Guida per l'utente

Amazon Detective

Amazon Detective: Guida per l'utente

Table of Contents

Cos'è Amazon Detective?

Amazon Detective consente di analizzare, esaminare e identificare rapidamente la causa principale degli esiti di sicurezza o delle attività sospette. Detective raccoglie automaticamente i dati di log dalle tue risorse AWS . Utilizza quindi il machine learning, l'analisi statistica e la teoria dei grafi per generare visualizzazioni che consentono di condurre indagini sulla sicurezza più rapide ed efficaci. Le aggregazioni di dati, i riepiloghi e il contesto predefiniti di Detective facilitano e velocizzano l'analisi e la determinazione della natura e dell'estensione dei possibili problemi di sicurezza.

Con Detective puoi accedere fino a un anno di dati storici degli eventi. Questi dati sono disponibili attraverso una serie di visualizzazioni che mostrano le variazioni del tipo e del volume di attività in una finestra temporale selezionata. Detective collega queste modifiche ai GuardDuty risultati. Per ulteriori informazioni sui dati di origine in Detective, consulta the section called “Dati di origine utilizzati in un grafico di comportamento”.

Aggregando automaticamente i dati e fornendo strumenti visivi, Amazon Detective ti consente di condurre indagini di sicurezza più rapide ed efficienti. Puoi analizzare rapidamente i potenziali problemi e determinare la portata delle minacce alla sicurezza.

Argomenti

Caratteristiche di Amazon Detective

Ecco alcuni dei modi principali in cui Amazon Detective è utile per indagare su attività sospette nel tuo AWS ambiente e analizzare le risorse per identificare la causa principale dei problemi di sicurezza.

Detective: gruppi di ricerca

I gruppi di ricerca investigativa consentono di esaminare più attività in relazione a un potenziale evento di sicurezza. È possibile analizzare la causa principale dei GuardDuty risultati di elevata gravità utilizzando i gruppi di ricerca. Se un autore della minaccia sta tentando di compromettere l' AWS ambiente, in genere esegue una sequenza di azioni che generano molteplici risultati di sicurezza e comportamenti insoliti.

La pagina dei gruppi di ricerca in Detective mostra tutti i gruppi di risultati correlati estratti dal grafico del comportamento. Per ulteriori informazioni su come sfruttare i gruppi di ricerca per analizzare la causa principale dei risultati di sicurezza, consulta Analisi dei gruppi di risultati in Detective.

Detective offre una visualizzazione interattiva di ogni gruppo di ricerca per aiutarti a indagare sui problemi di sicurezza in modo più rapido e approfondito. La visualizzazione è progettata per visualizzare le entità e i risultati coinvolti in un incidente di sicurezza, facilitando la comprensione delle connessioni e delle cause principali. Consente di analizzare i problemi in modo più rapido e approfondito con meno sforzo. Il pannello Finding group Visualization mostra i risultati e le entità coinvolte in un gruppo di ricerca.

Investigazione investigativa per valutare i risultati

Con Detective Investigation puoi indagare su IAM utenti e IAM ruoli utilizzando indicatori di compromissione, che possono aiutarti a determinare se una risorsa è coinvolta in un incidente di sicurezza. Un indicatore di compromissione (IOC) è un artefatto osservato in o su una rete, sistema o ambiente in grado (con un elevato livello di sicurezza) di identificare attività dannose o incidenti di sicurezza. Con le indagini Detective, puoi massimizzare l'efficienza, concentrarti sulle minacce alla sicurezza e rafforzare le capacità di risposta all'incidenza.

Detective Investigation utilizza modelli di apprendimento automatico e intelligence sulle minacce per far emergere solo i problemi più critici e sospetti, consentendoti di concentrarti su indagini di alto livello. Analizza automaticamente le risorse presenti nell' AWS ambiente per identificare potenziali indicatori di compromissione o attività sospette. Ciò consente di identificare modelli e comprendere quali risorse sono influenzate dagli eventi di sicurezza, offrendo un approccio proattivo all'identificazione e alla mitigazione delle minacce.

Puoi usare Avvia un'indagine investigativa dalla console Detective eseguendo un'indagine investigativa. Per condurre un'indagine in modo programmatico, usa l'StartInvestigationoperazione del Detective. API Per eseguire un'indagine utilizzando AWS Command Line Interface (AWS CLI), esegui il comando start-investigation.

Integrazione di Detective con Amazon Security Lake

Detective si integra con Amazon Security Lake, il che significa che puoi interrogare e recuperare i dati di registro non elaborati archiviati da Security Lake. Con questa integrazione, puoi raccogliere log ed eventi dalle seguenti fonti, supportate in modo nativo da Security Lake.

- AWS CloudTrail gestione degli eventi versione 1.0 e successive
- Amazon Virtual Private Cloud (AmazonVPC) Flow Logs versione 1.0 e successive
- Log di controllo di Amazon Elastic Kubernetes Service (EKSAmazon) versione 2.0

Dopo aver integrato Detective con Security Lake, Detective inizia a estrarre log non elaborati da Security Lake relativi agli eventi di AWS CloudTrail gestione e Amazon VPC Flow Logs. Puoi interrogare i log non elaborati per visualizzare i log e gli eventi in Detective.

Analizza VPC il volume del flusso

Con Detective puoi esaminare in modo interattivo i dettagli delle attività dei flussi di rete del cloud privato virtuale (VPC) delle tue istanze Amazon Elastic Compute Cloud (AmazonEC2) e dei pod Kubernetes. Detective raccoglie automaticamente i log di VPC flusso dagli account monitorati, li aggrega per EC2 istanza e presenta riepiloghi visivi e analisi su questi flussi di rete.

EC2Ad esempio, i dettagli dell'attività per Overall VPC flow Volume mostrano le interazioni tra l'EC2istanza e gli indirizzi IP durante un intervallo di tempo selezionato.

Per un pod Kubernetes, Overall VPC flow volume mostra il volume complessivo di byte in entrata e in uscita dall'indirizzo IP assegnato al pod Kubernetes per tutti gli indirizzi IP di destinazione.

Accesso ad Amazon Detective

Amazon Detective è disponibile nella maggior parte dei casi Regioni AWS. Per un elenco delle regioni in cui Detective è attualmente disponibile, consulta gli endpoint e le quote di Amazon Detective nel. Riferimenti generali di AWS Per informazioni sulla gestione Regioni AWS del tuo account Account AWS, consulta Specificare quali Regioni AWS account può utilizzare nella Gestione dell'account AWS Guida di riferimento.

In ogni Regione, puoi lavorare con Detective in uno dei seguenti modi.

AWS Management Console

AWS Management Console È un'interfaccia basata su browser che puoi utilizzare per creare e gestire AWS risorse. Come parte di tale console, la console Amazon Detective fornisce l'accesso al tuo account, ai dati e alle risorse di Amazon Detective. Puoi eseguire qualsiasi attività investigativa utilizzando la console Detective: esamina le potenziali minacce alla sicurezza e analizza, indaga e identifica la causa principale dei risultati di sicurezza.

AWS strumenti da riga di comando

Con gli strumenti da riga di AWS comando, puoi impartire comandi dalla riga di comando del tuo sistema per eseguire attività e AWS attività da Detective. L'utilizzo della riga di comando può essere più rapido e comodo rispetto all'utilizzo della console. Gli strumenti a riga di comando sono inoltre utili per creare script che eseguono le attività di .

AWS fornisce due set di strumenti da riga di comando: the AWS Command Line Interface (AWS CLI) e the AWS Strumenti per PowerShell. Per informazioni sull'installazione e l'utilizzo di AWS CLI, consulta la Guida AWS Command Line Interface per l'utente. Per informazioni sull'installazione e l'utilizzo degli strumenti per PowerShell, consultate la Guida per AWS Strumenti per PowerShell l'utente.

AWS SDKs

AWS fornisce SDKs che consistono in librerie e codice di esempio per vari linguaggi e piattaforme di programmazione, ad esempio Java, Go, Python, C++ e. NET. SDKsForniscono un accesso comodo e programmatico a Detective e ad altri Servizi AWS. Gestiscono anche attività come la firma crittografica delle richieste, la gestione degli errori e il ritentativo automatico delle richieste. Per informazioni sull'installazione e l'utilizzo di AWS SDKs, consulta Tools to Build on. AWS

Detective Amazon REST API

Amazon Detective ti REST API offre un accesso completo e programmatico al tuo account, ai dati e alle risorse di Detective. Con questoAPI, puoi inviare HTTPS richieste direttamente al Detective. Tuttavia, a differenza degli strumenti a riga di AWS comandoSDKs, il loro utilizzo API richiede che l'applicazione gestisca dettagli di basso livello, come la generazione di un hash per firmare una richiesta. Per informazioni al riguardoAPI, consulta il Detective API Reference.

Prezzi per Amazon Detective

Come per altri AWS prodotti, non ci sono contratti o impegni minimi per l'utilizzo di Amazon Detective.

I prezzi di Detective si basano su diverse dimensioni e addebita una tariffa fissa a più livelli per GB per tutti i dati indipendentemente dalla fonte. Per ulteriori informazioni, consulta i prezzi di Amazon Detective.

Per aiutarti a comprendere e prevedere i costi di utilizzo di Detective, Detective fornisce una stima dei costi di utilizzo del tuo account. Puoi rivedere queste stime sulla console Amazon Detective e accedervi con Amazon DetectiveAPI. A seconda di come utilizzi il servizio, potresti incorrere in costi aggiuntivi per l'utilizzo di altri Servizi AWS in combinazione con determinate funzionalità di Detective, come l'integrazione di Security Lake e Detective Investigations.

Quando attivi Detective per la prima volta, vieni Account AWS automaticamente iscritto alla versione di prova gratuita di 30 giorni di Detective. Sono inclusi i singoli account abilitati come parte di un'organizzazione in. AWS Organizations Durante la prova gratuita, non è previsto alcun costo per l'utilizzo di Detective nella versione applicabile Regione AWS.

Per aiutarti a comprendere e prevedere il costo dell'utilizzo di Detective al termine del periodo di prova gratuito, Detective fornisce una stima dei costi di utilizzo in base all'utilizzo di Detective durante il periodo di prova. I dati di utilizzo indicano anche il tempo che rimane prima della fine della prova gratuita. Puoi esaminare i dati relativi all'utilizzo del tuo account Detective sulla console Amazon Detective e accedervi con Amazon DetectiveAPI.

Come funziona Detective?

Detective estrae automaticamente eventi basati sul tempo come tentativi di accesso, API chiamate e traffico di rete dai log di VPC flusso di AWS CloudTrail Amazon. Inoltre, acquisisce i risultati rilevati da. GuardDuty

A partire da questi eventi, Detective utilizza il machine learning e la visualizzazione per creare una vista unificata, interattiva dei comportamenti delle risorse e delle interazioni tra di esse nel tempo. È possibile esplorare questo grafico comportamentale per esaminare diverse azioni, ad esempio tentativi di accesso falliti o chiamate sospette. API Puoi anche vedere come queste azioni influiscono su risorse come AWS account e EC2 istanze Amazon. Puoi modificare l'ambito e la tempistica del grafico di comportamento per una serie di attività:

- Esamina rapidamente qualsiasi attività che non rientri nella norma.
- Identifica gli schemi che possono indicare un problema di sicurezza.
- Scopri tutte le risorse interessate da un risultato.

Le visualizzazioni personalizzate di Detective forniscono una base e riepilogano le informazioni sull'account. Questi risultati possono aiutare a rispondere a domande come «È una API chiamata insolita per questo ruolo?» Oppure "È previsto questo picco di traffico da questa istanza?"

Con Detective, non è più necessario organizzare i dati o sviluppare, configurare o ottimizzare le query e i propri algoritmi. Non sono previsti costi anticipati, vengono addebitati solo gli eventi analizzati, senza software aggiuntivo da implementare o altri feed a cui abbonarsi.

Chi usa Detective?

Quando un account abilita Detective, diventa l'account amministratore per un grafico di comportamento. Un grafico comportamentale è un insieme collegato di dati estratti e analizzati da uno o più AWS account. Gli account amministratore invitano gli account membri a contribuire con i propri dati al grafico di comportamento dell'account amministratore.

Detective è anche integrato con AWS Organizations. L'account di gestione dell'organizzazione indica un account amministratore di Detective per l'organizzazione. L'account amministratore di Detective abilita gli account dell'organizzazione come account membri nel grafico di comportamento dell'organizzazione.

Per informazioni su come Detective utilizza i dati di origine degli account del grafico comportamentale, consulta the section called “Dati di origine utilizzati in un grafico di comportamento”.

Per informazioni su come gli account amministratore gestiscono i grafici del comportamento, consulta Gestione degli account. Per informazioni su come gli account membri gestiscono il grafico di comportamento, gli inviti e le iscrizioni, consulta the section called “Per gli account membri: gestione degli inviti e delle iscrizioni”.

L'account amministratore utilizza le analisi e le visualizzazioni generate dal grafico comportamentale per esaminare AWS risorse e GuardDuty risultati. Utilizzando le integrazioni di Detective con GuardDuty e AWS Security Hub, puoi passare da una GuardDuty scoperta in questi servizi direttamente alla console Detective.

Un'indagine di Detective si concentra sull'attività connessa alle risorse AWS coinvolte. Per una panoramica del processo di indagine in Detective, consulta Come viene usato Amazon Detective per le indagini nella Guida per l'utente di Detective.

Servizi correlati

Per proteggere ulteriormente dati, carichi di lavoro e applicazioni, prendi in AWS considerazione l'utilizzo di quanto segue Servizi AWS in combinazione con Amazon Detective.

AWS Security Hub

AWS Security Hub ti offre una visione completa dello stato di sicurezza delle tue AWS risorse e ti aiuta a controllare il tuo AWS ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza. Lo fa in parte consumando, aggregando, organizzando e dando priorità ai risultati di sicurezza provenienti da più prodotti (Servizi AWS incluso Detective) e AWS Partner Network (APN) supportati. Security Hub ti aiuta ad analizzare le tendenze della sicurezza e a identificare i problemi di sicurezza con la massima priorità in tutto l' AWS ambiente.

Per ulteriori informazioni su Security Hub, consulta la Guida AWS Security Hub per l'utente.

Amazon GuardDuty

Amazon GuardDuty è un servizio di monitoraggio della sicurezza che analizza ed elabora determinati tipi di AWS log, come i registri degli eventi di AWS CloudTrail dati per Amazon S3 e i registri degli eventi di gestione. CloudTrail Utilizza feed di intelligence sulle minacce, come elenchi di indirizzi IP e domini dannosi, e l'apprendimento automatico per identificare attività impreviste, potenzialmente non autorizzate e dannose all'interno dell'ambiente. AWS

Per ulteriori informazioni GuardDuty, consulta la Amazon GuardDuty User Guide.

Amazon Security Lake

Amazon Security Lake è un servizio di data lake di sicurezza completamente gestito. Puoi utilizzare Security Lake per centralizzare automaticamente i dati di sicurezza provenienti da AWS ambienti, provider SaaS, fonti locali, fonti cloud e fonti di terze parti in un data lake creato appositamente e archiviato nel tuo account. AWS Security Lake ti aiuta ad analizzare i dati di sicurezza in modo da ottenere un quadro più completo del tuo livello di sicurezza in tutta l'organizzazione. Con Security Lake, puoi anche migliorare la protezione di carichi di lavoro, applicazioni e dati.

Per ulteriori informazioni su Security Lake, consulta la Guida per l'utente di Amazon Security Lake. Per ulteriori informazioni sull'utilizzo congiunto di Detective e Security Lake, consultaIntegrazione tra Detective e Security Lake.

Per ulteriori informazioni sui servizi AWS di sicurezza aggiuntivi, consulta Sicurezza, identità e conformità su AWS.

Concetti e terminologia di Amazon Detective

I seguenti termini e concetti sono importanti per comprendere Amazon Detective e il relativo funzionamento.

Account amministratore

Il Account AWS che possiede un grafico comportamentale e che utilizza il grafico comportamentale per le indagini.

L'account amministratore invita gli account membri a contribuire con i propri dati al grafico di comportamento. Per ulteriori informazioni, consulta the section called “Gestione degli account membri invitati”.

Per il grafico di comportamento dell'organizzazione, l'account amministratore è l'account amministratore Detective designato dall'account di gestione dell'organizzazione. Per ulteriori informazioni, consulta the section called “Designazione dell'account amministratore di Detective”. L'account amministratore di Detective abilita qualsiasi account dell'organizzazione come account membro nel grafico di comportamento dell'organizzazione. Per ulteriori informazioni, consulta the section called “Gestione degli account membri dell'organizzazione”.

Gli account amministratore possono anche visualizzare l'utilizzo dei dati per il grafico di comportamento e rimuovere gli account membri dal grafico di comportamento.

Organizzazione autonoma del sistema (ASO)

L'organizzazione titolata a cui è assegnato un sistema autonomo. Questo sistema autonomo è una rete eterogenea o un insieme di reti che utilizzano logiche e policy di routing simili.

Grafico di comportamento

Un insieme collegato di dati generati dai dati di origine in entrata che è associato a uno o più Account AWS.

Ogni grafico di comportamento utilizza la stessa struttura di risultati, entità e relazioni.

Account amministratore delegato (AWS Organizations)

In Organizations, l'account amministratore delegato per un servizio è in grado di gestire l'utilizzo di un servizio per l'organizzazione.

In Detective, l'account amministratore di Detective è anche l'account amministratore delegato, a meno che l'account amministratore di Detective non sia l'account di gestione dell'organizzazione. L'account di gestione dell'organizzazione non può essere un account amministratore delegato.

In Detective, è consentita l'autodelega. Un account di gestione dell'organizzazione può delegare il proprio account come amministratore delegato di Detective, ma ciò verrebbe registrato o memorizzato solo nell'ambito di Detective e non delle organizzazioni.

Account amministratore Detective

Per il grafico del comportamento dell'organizzazione in una Regione, l'account designato dall'account di gestione dell'organizzazione come account amministratore. Per ulteriori informazioni, consulta the section called “Designazione dell'account amministratore di Detective”.

Detective consiglia all'account di gestione dell'organizzazione di scegliere un account diverso dal proprio account.

Se l'account non è l'account di gestione dell'organizzazione, l'account amministratore di Detective è anche l'account amministratore delegato di Detective in Organizations.

Dati di origine di Detective

Versioni elaborate e strutturate delle informazioni provenienti dai seguenti tipi di feed:

- Registri da AWS servizi, come AWS CloudTrail registri e Amazon VPC Flow Logs
- GuardDuty risultati

Detective utilizza i dati dell'origine di Detective per compilare il grafico di comportamento. Detective archivia anche copie dei dati di origine di Detective per supportarne l'analisi.

Entità

Un elemento estratto dai dati importati.

Ogni entità ha un tipo, che identifica il tipo di oggetto che rappresenta. Esempi di tipi di entità includono indirizzi IP, EC2 istanze Amazon e AWS utenti.

Le entità possono essere AWS risorse gestite dall'utente o indirizzi IP esterni che hanno interagito con le risorse dell'utente.

Per ogni entità, i dati di origine vengono utilizzati anche per compilare le proprietà dell'entità. I valori delle proprietà possono essere estratti direttamente dai record di origine o aggregati su più record.

Risultato

Un problema di sicurezza rilevato da Amazon GuardDuty.

Gruppo di risultati

Una raccolta di risultati, entità e prove che potrebbero essere correlate allo stesso evento o problema di sicurezza. Detective genera gruppi di risultati basati su un modello di machine learning integrato.

Prova di Detective

Detective identifica ulteriori prove relative a un gruppo di risultati sulla base dei dati del grafico di comportamento raccolti negli ultimi 45 giorni. Questa prova viene presentata come un risultato con il valore di gravità Informativo. Le prove forniscono informazioni di supporto che evidenziano un'attività insolita o un comportamento sconosciuto potenzialmente sospetto se osservati all'interno di un gruppo di risultati. Un esempio di ciò potrebbero essere le nuove geolocalizzazioni o le API chiamate rilevate nell'ambito di un rilevamento. Al momento, questi risultati sono visualizzabili solo in Detective e non vengono inviati alla Centrale di sicurezza.

Panoramica dei risultati

Una singola pagina che fornisce un riepilogo delle informazioni su un risultato.

Una panoramica dei risultati contiene l'elenco delle entità coinvolte nei risultati. Dall'elenco, è possibile passare al profilo di un'entità.

Una panoramica dei risultati contiene anche un pannello dei dettagli che contiene gli attributi dei risultati.

Entità ad alto volume

Un'entità che ha connessioni da o verso un gran numero di altre entità durante un intervallo di tempo. Ad esempio, un'EC2istanza potrebbe avere connessioni da milioni di indirizzi IP. Il numero di connessioni supera la soglia che può essere gestita da Detective.

Quando il periodo di validità corrente contiene un intervallo di tempo ad alto volume, Detective avvisa l'utente.

Per ulteriori informazioni, consulta Visualizzazione dei dettagli per entità con volumi elevati nella Guida per l'utente di Amazon Detective.

Indagine

Processo che consiste nell'individuare un'attività sospetta o interessante, determinarne l'ambito, individuarne la sorgente o la causa sottostante e quindi decidere come procedere.

Account membro

Un record Account AWS che un account amministratore ha invitato a fornire dati a un grafico comportamentale. Nel grafico del comportamento dell'organizzazione, un account membro può essere un account dell'organizzazione che l'account amministratore di Detective ha abilitato come account membro.

Gli account membri invitati possono rispondere all'invito del grafico di comportamento e rimuovere il proprio account dal grafico. Per ulteriori informazioni, consulta the section called “Per gli account membri: gestione degli inviti e delle iscrizioni”.

Gli account dell'organizzazione non possono modificare la loro appartenenza al grafico di comportamento dell'organizzazione.

Tutti gli account membri possono inoltre visualizzare le informazioni sull'utilizzo del proprio account attraverso i grafici del comportamento a cui contribuiscono con i dati.

Non hanno altro accesso al grafico di comportamento.

Grafico del comportamento dell'organizzazione

Il grafico di comportamento di proprietà dell'account amministratore di Detective. L'account di gestione dell'organizzazione indica un account amministratore di Detective. Per ulteriori informazioni, consulta the section called “Designazione dell'account amministratore di Detective”.

Nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective controlla se un account dell'organizzazione è un account membro. Gli account dell'organizzazione non possono auto-rimuoversi dal grafico di comportamento dell'organizzazione.

L'account amministratore di Detective può anche invitare altri account al grafico di comportamento dell'organizzazione.

Profilo

Una singola pagina che fornisce una raccolta di visualizzazioni di dati relative all'attività di un'entità.

Per quanto riguarda i risultati, i profili aiutano gli analisti a determinare se il risultato è fonte di reale preoccupazione o falso positivo.

I profili forniscono informazioni a supporto di un'indagine su un risultato o per una ricerca generale di attività sospette.

Pannello del profilo

Una singola visualizzazione su un profilo. Ogni pannello del profilo ha lo scopo di aiutare a rispondere a una o più domande specifiche per assistere un analista in un'indagine.

I pannelli del profilo possono contenere coppie chiave-valore, tabelle, sequenze temporali, grafici a barre o grafici di geolocalizzazione.

Relazione

Attività che si verifica tra singole entità. Le relazioni vengono estratte anche dai dati di origine in entrata.

Analogamente a un'entità, una relazione ha un tipo, che identifica i tipi di entità coinvolte e la direzione della connessione. Un esempio di tipo di relazione è un indirizzo IP che si connette a un'EC2istanza Amazon.

Periodo di validità

La finestra temporale utilizzata per definire l'ambito dei dati visualizzati sui profili.

Il periodo di validità predefinito per un risultato riflette la prima e l'ultima volta in cui è stata osservata l'attività sospetta.

Il periodo di validità predefinito per un profilo di entità è pari alle 24 ore precedenti.

Guida introduttiva ad Amazon Detective

Questo tutorial fornisce un'introduzione ad Amazon Detective. Imparerai come abilitare Detective per il tuo AWS account. Imparerai anche come verificare che il Detective abbia iniziato a inserire ed estrarre dati dal tuo AWS account nel tuo grafico comportamentale.

Quando abiliti Amazon Detective, Detective crea un grafico di comportamento specifico per Regione con il tuo account come account amministratore. Inizialmente questo è l'unico account nel grafico di comportamento. L'account amministratore può quindi invitare altri AWS account a contribuire con i propri dati al grafico del comportamento. Consultare Gestione degli account.

L'abilitazione di Detective in una Regione per la prima volta dà inizio anche a una prova gratuita di 30 giorni per il grafico di comportamento. Se l'account disabilita Detective e poi lo abilita di nuovo, non sarà disponibile alcuna prova gratuita. Consultare the section called “Informazioni sulla versione di prova gratuita per i grafici di comportamento”.

Dopo la prova gratuita, a ogni account indicato nel grafico di comportamento vengono fatturati i dati con cui contribuisce. L'account amministratore può tenere traccia dell'uso e visualizzare il costo totale previsto per un periodo tipico di 30 giorni per l'intero grafico di comportamento. Per ulteriori informazioni, consulta the section called “Utilizzo e costi dell'account amministratore”. Gli account membri possono tenere traccia dell'utilizzo e dei costi previsti per i grafici di comportamento a cui appartengono. Per ulteriori informazioni, consulta the section called “Monitoraggio dell'utilizzo dell'account membro”.

Argomenti

- Configurazione AWS dell'account
- Prerequisiti per abilitare Detective
- Consigli per abilitare Detective
- Abilitazione di Detective

Configurazione AWS dell'account

Per poter abilitare Amazon Detective, assicurati di disporre di un Account AWS. Se non disponi di un AWS account, completa i seguenti passaggi per crearne uno.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Prerequisiti per abilitare Detective

Assicurati che siano soddisfatti i seguenti requisiti prima di abilitare Detective.

Concessione delle autorizzazioni necessarie per Detective

Prima di poter abilitare Detective, devi assicurarti che il tuo principale IAM disponga delle autorizzazioni di Detective richieste. Il principale può essere un utente o un ruolo esistente in uso oppure puoi crearne uno nuovo da utilizzare per Detective.

Quando ti registri ad Amazon Web Services (AWS), il tuo account viene automaticamente registrato per tutti i Servizi AWS, incluso Amazon Detective. Tuttavia, per abilitare e utilizzare Detective è necessario prima impostare le autorizzazioni che consentono l'accesso alla console Amazon Detective e alle operazioni API. Tu o il tuo amministratore potete farlo utilizzando AWS Identity and Access Management (IAM) per allegare la policy `AmazonDetectiveFullAccess` gestita al vostro principale IAM, che concede l'accesso a tutte le azioni del Detective. Senza queste autorizzazioni IAM, potresti visualizzare la pagina Guida introduttiva a Detective nella AWS console. Di conseguenza, la console non mostrerà alcun grafico attivo finché non verranno aggiunte queste autorizzazioni, anche se il servizio è abilitato.

Versione supportata AWS Command Line Interface

Per utilizzarlo AWS CLI per eseguire attività di Detective, la versione minima richiesta è 1.16.303.

Consigli per abilitare Detective

Valuta la possibilità di seguire questi consigli prima di abilitare Detective

Allineamento consigliato con e GuardDuty AWS Security Hub

Se sei registrato GuardDuty e AWS Security Hub, ti consigliamo di utilizzare un account amministratore per tali servizi. Se gli account amministratore sono gli stessi per tutti e tre i servizi, i seguenti punti di integrazione funzionano perfettamente.

- Nel GuardDuty nostro Security Hub, quando visualizzi i dettagli di una GuardDuty scoperta, puoi passare dai dettagli del ritrovamento al profilo di ricerca del Detective.
- In Detective, quando indaghi su un GuardDuty ritrovamento, puoi scegliere l'opzione per archiviarlo.

Se disponi di account amministratore diversi per GuardDuty Security Hub, ti consigliamo di allineare gli account amministratore in base al servizio che utilizzi più frequentemente.

- Se lo usi GuardDuty più frequentemente, abilita Detective utilizzando l'account GuardDuty amministratore.

  Se lo utilizzi AWS Organizations per gestire gli account, designa l'account GuardDuty amministratore come account amministratore Detective per l'organizzazione.
- Se usi Centrale di sicurezza più frequentemente, abilita Detective utilizzando l'account amministratore di Centrale di sicurezza.

  Se utilizzi Organizations per gestire gli account, designa l'account amministratore di Centrale di sicurezza come account amministratore di Detective per l'organizzazione.

Se non puoi utilizzare gli stessi account amministratore in tutti i servizi, dopo aver abilitato Detective, puoi facoltativamente creare un ruolo per più account. Questo ruolo consente a un account amministratore di accedere ad altri account.

Per informazioni su come IAM supporta questo tipo di ruolo, consulta Fornire l'accesso a un utente IAM in un altro AWS account di tua proprietà nella Guida per l'utente IAM.

Aggiornamento consigliato della frequenza GuardDuty CloudWatch di notifica

Nel GuardDuty, i rilevatori sono configurati con una frequenza di CloudWatch notifica Amazon per segnalare le occorrenze successive di un risultato. Ciò include l'invio di notifiche a Detective.

Per impostazione predefinita, la frequenza è di sei ore. Ciò significa che anche se un risultato si ripete più volte, le nuove ricorrenze non si rifletteranno in Detective se non sei ore dopo.

Per ridurre il tempo necessario a Detective per ricevere questi aggiornamenti, consigliamo GuardDuty all'account amministratore di modificare l'impostazione dei rilevatori a 15 minuti. Tieni presente che la modifica della configurazione non ha alcun effetto sul costo di utilizzo GuardDuty.

Per informazioni sull'impostazione della frequenza di notifica, consulta Monitoring GuardDuty Findings with Amazon CloudWatch Events nella Amazon GuardDuty User Guide.

Abilitazione di Detective

Puoi abilitare Detective dalla console Detective, dall'API Detective o dalla AWS Command Line Interface.

Puoi abilitare Detective solo una volta in ogni Regione. Se sei già l'account amministratore di un grafico di comportamento nella Regione, non puoi abilitare nuovamente Detective in quella Regione.

Console

Abilitare Detective (console)

1. Accedi alla AWS Management Console. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Scegli Avvia.
3. Nella pagina Abilita Amazon Detective, Align administrator accounts (consigliato) spiega la raccomandazione per allineare gli account amministratore tra Detective e Amazon GuardDuty and. AWS Security Hub Consultare the section called “Allineamento consigliato con e GuardDuty AWS Security Hub”.
4. Il pulsante Allega policy IAM ti porta direttamente alla console IAM e apre la policy consigliata. Hai la possibilità di allegare la policy consigliata al principale che usi per Detective. Se non disponi delle autorizzazioni per operare nella console IAM, in Autorizzazioni richieste puoi copiare il nome della risorsa Amazon (ARN) della policy da fornire al tuo amministratore IAM. L'amministratore può quindi collegare la policy per tuo conto.

   Verifica che la policy IAM richiesta sia in vigore.
5. La sezione Aggiungi tag consente di aggiungere tag al grafico di comportamento.

   Per aggiungere un tag, procedere come segue:

   a. Scegli Aggiungi nuovo tag.
   b. Per Chiave, inserisci il nome del tag.
   c. In Valore, immetti il valore del tag.

   Per rimuovere un tag, seleziona l'opzione Rimuovi per quel tag.
6. Scegli Abilita Amazon Detective.
7. Dopo aver abilitato Detective, puoi invitare gli account membri al tuo grafico di comportamento.

Per accedere alla pagina di Gestione dell'account, scegli Aggiungi membri adesso. Per informazioni su come invitare gli account membri, consulta the section called “Gestione degli account membri invitati”.

Detective API, AWS CLI

Puoi abilitare Amazon Detective dall'API Detective o dalla AWS Command Line Interface.

Per abilitare Detective (Detective API, AWS CLI)

- API Detective: usa l'operazione `CreateGraph`.
- AWS CLI: alla riga di comando, esegui il comando `create-graph`.

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

Il comando seguente abilita Detective e imposta il valore del tag `Department` su `Security`.

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

Python script on GitHub

Puoi abilitare Detective in tutte le regioni utilizzando lo script Detective Python GitHub su .Detective fornisce uno script open source che esegue le seguenti GitHub operazioni:

- Abilita Detective per un account amministratore in un elenco specificato di Regioni
- Aggiunge un elenco fornito di account membri a ciascuno dei grafici di comportamento risultanti
- Invia le e-mail di invito agli account membri
- Accetta automaticamente gli inviti per gli account membri

Per informazioni su come configurare e utilizzare gli script, consulta GitHub . the section called “Script di Amazon Detective Python”

Verifica che il Detective stia acquisendo dati dal tuo account AWS

Dopo aver abilitato Detective, inizia a inserire ed estrarre i dati dal tuo AWS account nel tuo grafico comportamentale.

Per l'estrazione iniziale, i dati di solito diventano disponibili nel grafico comportamentale entro 2 ore.

Un modo per verificare che Detective stia estraendo dati è cercare valori di esempio nella pagina Cerca di Detective.

Controllare i valori di esempio nella pagina Cerca

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione selezionare Search (Cerca).
3. Dal menu Seleziona tipo, scegli un tipo di elemento.

   La sezione Esempi dai dati contiene un set di identificatori del tipo selezionato presenti nei dati del grafico di comportamento.

   Se riesci a vedere valori di esempio, allora sai che i dati vengono inseriti ed estratti nel tuo grafico di comportamento.

Dati in un grafico del comportamento del Detective

In Amazon Detective, conduci indagini utilizzando i dati di un grafico di comportamento di Detective. In questa sezione puoi scoprire le principali fonti di dati utilizzate in un grafico del comportamento di un Detective e come Detective utilizza i dati di origine per compilarlo.

Un grafico di comportamento è un insieme collegato di dati generati dai dati di origine di Detective che vengono importati da uno o più account Amazon Web Services (AWS).

Il grafico del comportamento utilizza i dati di origine per eseguire le seguenti operazioni.

- Genera un quadro generale dei tuoi sistemi, degli utenti e delle interazioni tra loro nel tempo
- Esegui un'analisi più dettagliata di attività specifiche per rispondere alle domande che sorgono durante le indagini
- Metti in correlazione raccolte di risultati, entità e prove che potrebbero essere correlate allo stesso evento o problema di sicurezza.

Tieni presente che tutta l'estrazione, la modellazione e l'analisi dei dati del grafico di comportamento avvengono nel contesto di ogni singolo grafico.

Ogni grafico di comportamento contiene i dati di uno o più account. Quando un account abilita Detective, diventa l'account amministratore per il grafico di comportamento e sceglie gli account membri per il grafico. Un grafico di comportamento può contenere fino a 1.200 account membri. Per informazioni su come un account amministratore gestisce gli account dei membri in un grafico comportamentale, vedi Gestione degli account in Detective.

Indice

Come Detective compila un grafico del comportamento

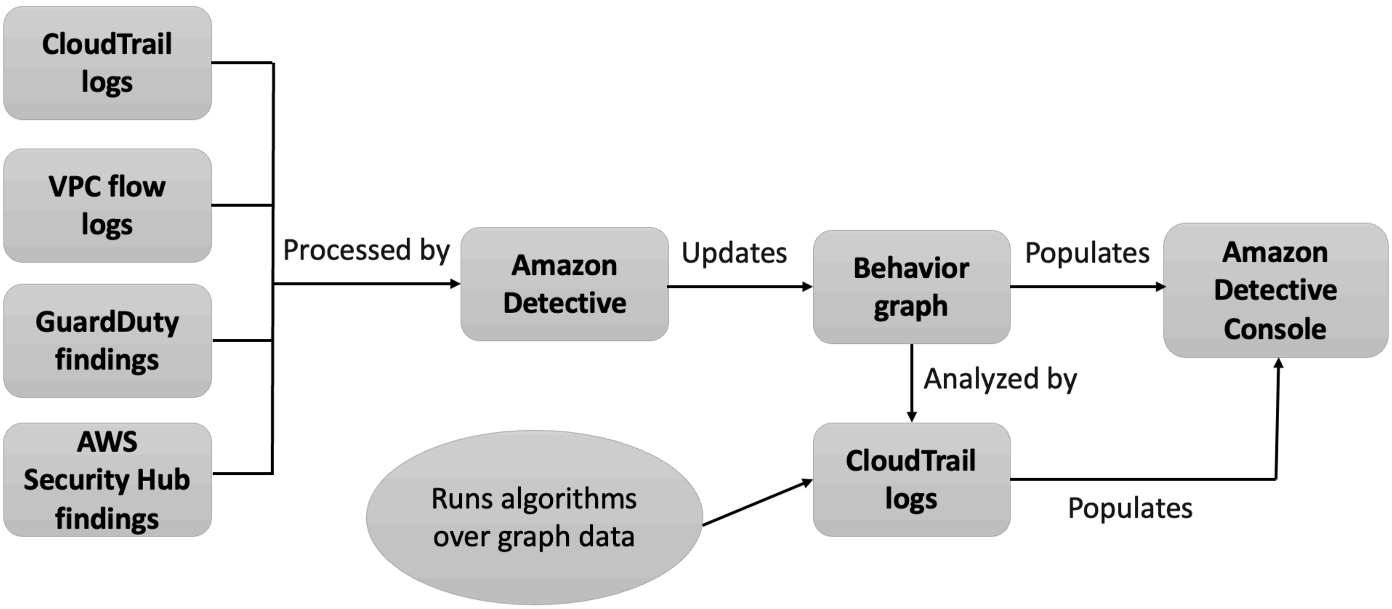
Per fornire i dati non elaborati per le indagini, Detective riunisce i dati provenienti da tutto l'ambiente AWS e non solo, tra cui:

- Dati di log, tra cui Amazon Virtual Private Cloud (AmazonVPC) e AWS CloudTrail
- I risultati di Amazon GuardDuty
- Risultati di AWS Security Hub

Per ulteriori informazioni sui dati di origine utilizzati in un grafico comportamentale, consulta Dati di origine utilizzati in un grafico comportamentale.

Come Detective elabora i dati di origine

Man mano che arrivano nuovi dati, Detective utilizza una combinazione di estrazione e analisi per compilare il grafico di comportamento.



Estrazione di Detective

L'estrazione si basa su regole di mappatura configurate. Una regola di mappatura fondamentalmente indica: "Ogni volta che vedi questo dato, usalo in questo modo specifico per aggiornare i dati del grafico di comportamento".

Ad esempio, un record di dati di origine di Detective in entrata potrebbe includere un indirizzo IP. In caso affermativo, Detective utilizza le informazioni in quel record per creare una nuova entità di indirizzo IP o aggiornare un'entità di indirizzo IP esistente.

Analisi di Detective

Le analisi sono algoritmi più complessi che analizzano i dati per fornire informazioni sulle attività associate alle entità.

Ad esempio, un tipo di analisi di Detective analizza la frequenza con cui si verifica l'attività eseguendo algoritmi. Per le entità che effettuano API chiamate, l'algoritmo cerca API le chiamate che l'entità normalmente non utilizza. L'algoritmo cerca anche un forte picco nel numero di API chiamate.

Le informazioni analitiche supportano le indagini fornendo risposte alle domande chiave degli analisti e vengono spesso utilizzate per compilare i pannelli dei risultati e dei profili delle entità.

Periodo di formazione per nuovi grafici comportamentali dei Detective

Un modo per indagare su un risultato consiste nel confrontare l'attività svolta durante il periodo di validità del risultato con l'attività che si è verificata prima che il risultato venisse rilevato. L'attività che non è mai stata osservata prima potrebbe avere maggiori probabilità di essere sospetta.

Alcuni pannelli di profilo di Amazon Detective evidenziano attività che non sono state osservate nel periodo precedente al risultato. Diversi pannelli di profilo mostrano anche un valore di base per mostrare l'attività media nei 45 giorni precedenti al periodo di validità. Scope time è il riepilogo dell'attività di un'entità nel tempo.

Man mano che vengono estratti più dati nel grafico di comportamento, Detective sviluppa un quadro più accurato di quali attività sono normali nell'organizzazione e quali attività sono insolite.

Tuttavia, per creare questa immagine, Detective deve accedere ad almeno due settimane di dati. La maturità dell'analisi di Detective aumenta anche con il numero di account nel grafico di comportamento.

Le prime due settimane dopo l'attivazione di Detective sono considerate un periodo di addestramento. Durante questo periodo, i pannelli del profilo che confrontano l'attività del periodo di validità con l'attività precedente visualizzano un messaggio che indica che Detective è in un periodo di addestramento.

Durante il periodo di prova, Detective consiglia di aggiungere il maggior numero possibile di account membri al grafico del comportamento. Ciò fornisce a Detective un pool di dati più ampio, che gli consente di generare un quadro più accurato della normale attività dell'organizzazione.

Panoramica della struttura dei dati del grafico di comportamento

La struttura dei dati del grafico di comportamento definisce la struttura dei dati estratti e analizzati. Definisce inoltre come i dati di origine vengono mappati al grafico di comportamento.

Tipi di elementi nella struttura dei dati del grafico di comportamento

La struttura dei dati del grafico di comportamento è costituita dai seguenti elementi di informazione.

Entità

Un'entità rappresenta un elemento estratto dai dati di origine di Detective.

Ogni entità ha un tipo, che identifica il tipo di oggetto che rappresenta. Esempi di tipi di entità includono indirizzi IP, EC2 istanze Amazon e AWS utenti.

Per ogni entità, i dati di origine vengono utilizzati anche per compilare le proprietà dell'entità. I valori delle proprietà possono essere estratti direttamente dai record di origine o aggregati su più record.

Alcune proprietà sono costituite da un singolo valore scalare o aggregato. Ad EC2 esempio, Detective tiene traccia del tipo di istanza e del numero totale di byte elaborati.

Le proprietà delle serie temporali tengono traccia dell'attività nel tempo. Ad EC2 esempio, Detective tiene traccia nel tempo delle porte uniche utilizzate.

Relazioni

Una relazione rappresenta l'attività che si verifica tra singole entità. Le relazioni vengono estratte anche dai dati di origine di Detective.

Analogamente a un'entità, una relazione ha un tipo, che identifica i tipi di entità coinvolte e la direzione della connessione. Un esempio di tipo di relazione sono gli indirizzi IP che si connettono alle EC2 istanze.

Per ogni singola relazione, ad esempio un indirizzo IP specifico che si connette a un'istanza specifica, Detective tiene traccia delle ricorrenze nel tempo.

Tipi di entità nella struttura dei dati del grafico di comportamento

La struttura dei dati del grafico di comportamento è costituita da tipi di entità e relazioni che eseguono le seguenti operazioni:

- Traccia dei server, degli indirizzi IP e degli agenti utente utilizzati
- Tieni traccia degli AWS utenti, dei ruoli e degli account utilizzati
- Traccia delle connessioni di rete e delle autorizzazioni che si verificano nel tuo ambiente AWS

La struttura dei dati del grafico di comportamento contiene i seguenti tipi di entità.

AWS account

AWS account presenti nei dati di origine del Detective.

Per ogni account, Detective risponde a diverse domande:

- Quali API chiamate ha utilizzato l'account?
- Quali agenti utente ha utilizzato l'account?
- Quali organizzazioni di sistema autonome (ASOs) ha utilizzato l'account?
- In quali aree geografiche l'account è stato attivo?

AWS ruolo

AWS ruoli presenti nei dati di origine del Detective.

Per ogni ruolo, Detective risponde a diverse domande:

- Quali API chiamate ha utilizzato il ruolo?
- Quali agenti utente ha utilizzato il ruolo?
- Qual ASOs è stato il ruolo utilizzato?
- In quali aree geografiche il ruolo è stato attivo?
- Quali risorse hanno assunto questo ruolo?
- Quali ruoli ha assunto questo ruolo?
- Quali sessioni di ruolo hanno coinvolto questo ruolo?

AWS utente

AWS utenti presenti nei dati di origine del Detective.

Per ogni utente, Detective risponde a diverse domande:

- Quali API chiamate ha utilizzato l'utente?
- Quali agenti utente ha utilizzato l'utente?

- In quali aree geografiche l'utente è stato attivo?
- Quali ruoli ha assunto questo utente?
- Quali sessioni di ruolo hanno coinvolto questo utente?

Utente federato

Istanze di un utente federato. Di seguito sono riportati alcuni esempi di utenti federati:

- Un'identità che accede utilizzando Security Assertion Markup Language () SAML
- Un'identità che accede tramite la federazione delle identità Web

Per ogni utente federato, Detective risponde a queste domande:

- Con quale provider di identità si è autenticato l'utente federato?
- Qual era il pubblico dell'utente federato? Il pubblico identifica l'applicazione che ha richiesto il token di identità Web dell'utente federato.
- In quali aree geografiche è stato attivo l'utente federato?
- Quali agenti utente ha utilizzato l'utente federato?
- Cosa ASOs ha usato l'utente federato?
- Quali ruoli ha assunto questo utente federato?
- Quali sessioni di ruolo hanno coinvolto questo utente federato?

EC2istanza

EC2istanze presenti nei dati di origine del Detective.

EC2Ad esempio, il Detective risponde a diverse domande:

- Quali indirizzi IP hanno comunicato con l'istanza?
- Quali porte sono state utilizzate per comunicare con l'istanza?
- Quale volume di dati è stato inviato da e verso l'istanza?
- Cosa VPC contiene l'istanza?
- Quali API chiamate ha utilizzato l'EC2istanza?
- Quali user agent ha utilizzato l'EC2istanza?
- Che cosa ASOs è stata utilizzata dall'EC2istanza?
- In quali aree geografiche l'EC2istanza è stata attiva?
- Quali ruoli ha assunto l'EC2istanza?

Sessioni dei ruoli

Istanze di una risorsa che sta assumendo un ruolo. Ogni sessione di ruolo è identificata dall'identificatore del ruolo e un nome della sessione.

Per ogni ruolo, Detective risponde a diverse domande:

- Quali risorse sono state coinvolte in questa sessione di ruolo? In altre parole, quale ruolo è stato assunto e quale risorsa ha assunto il ruolo?

  Tieni presente che per l'assunzione del ruolo tra account, Detective non può identificare la risorsa che ha assunto il ruolo.
- Quali API chiamate ha utilizzato la sessione di ruolo?
- Quali agenti utente ha utilizzato la sessione di ruolo?
- Cosa ASOs è stata utilizzata la sessione di ruolo?
- In quali aree geografiche la sessione di ruolo è stata attiva?
- Quale utente o ruolo ha avviato questa sessione di ruolo?
- Quali sessioni di ruolo sono state avviate da questa sessione di ruolo?

Risultato

Risultati scoperti da Amazon GuardDuty che vengono inseriti nei dati di origine del Detective.

Per ogni risultato, Detective tiene traccia del tipo di risultato, dell'origine e della finestra temporale dell'attività del risultato.

Memorizza inoltre informazioni specifiche sul risultato, come i ruoli o gli indirizzi IP coinvolti nell'attività rilevata.

Indirizzo IP

Gli indirizzi IP presenti nei dati di origine di Detective.

Per ogni indirizzo IP, Detective risponde a diverse domande:

- Quali API chiamate ha utilizzato l'indirizzo?
- Quali porte ha utilizzato l'indirizzo?
- Quali utenti e agenti utente hanno utilizzato l'indirizzo IP?
- In quali aree geografiche l'indirizzo IP è stato attivo?
- A quali EC2 istanze è stato assegnato e con quali comunicazioni è stato assegnato questo indirizzo IP?

Bucket S3

I bucket S3 presenti nei dati di origine di Detective.

Per ogni bucket S3, Detective risponde a queste domande:

- Quali principali hanno interagito con il bucket S3?
- Quali API chiamate sono state effettuate al bucket S3?
- Da quali località geografiche i gestori hanno effettuato API chiamate verso il bucket S3?
- Quali agenti utente sono stati utilizzati per interagire con il bucket S3?
- Cosa ASOs sono stati utilizzati per interagire con il bucket S3?

Puoi eliminare un bucket S3 e quindi crearne uno nuovo con lo stesso nome. Poiché Detective utilizza il nome del bucket S3 per identificare il bucket S3, tratta questi nomi come un'unica entità di bucket S3. Nel profilo dell'entità, Ora di creazione è l'ora della prima creazione. Ora di eliminazione è l'ora di eliminazione più recente.

Per visualizzare tutti gli eventi di creazione ed eliminazione, imposta il periodo di validità in modo che inizi con l'ora di creazione e termini con l'ora di eliminazione. Nel pannello del profilo relativo al volume complessivo delle API chiamate, visualizza i dettagli dell'attività per il periodo di riferimento. Filtra i API metodi da mostrare `Create` e `Delete` i metodi. Per informazioni, consulta the section called “Volume complessivo delle API chiamate”.

Agente utente

Gli agenti utente presenti nei dati di origine di Detective.

Per ogni agente utente, Detective risponde a domande come le seguenti:

- Quali API chiamate ha utilizzato l'agente utente?
- Quali utenti e ruoli hanno utilizzato l'agente utente?
- Quali indirizzi IP hanno utilizzato l'agente utente?

EKSCluster

EKScluster presenti nei dati di origine del Detective.

> **Note**
>
> Per visualizzare i dettagli completi per questo tipo di entità, è necessario abilitare l'origine dati opzionale dei log di EKS controllo. Per maggiori informazioni, consulta Origini dati facoltative

Per ogni EKS cluster, Detective risponde a domande come le seguenti:

- Quali API chiamate Kubernetes sono state eseguite in questo cluster?
- Quali utenti e account di servizio (soggetti) di Kubernetes sono attivi in questo cluster?
- Quali container sono stati avviati in questo cluster?
- Quali immagini vengono utilizzate per avviare i container in questo cluster?

Pod Kubernetes

I pod Kubernetes presenti nei dati di origine di Detective.

> **Note**
>
> Per visualizzare i dettagli completi per questo tipo di entità, è necessario abilitare l'origine dati opzionale dei log di EKS controllo. Per maggiori informazioni, consulta Origini dati facoltative

Per ogni pod, Detective risponde a domande come le seguenti:

- Quali immagini di container in questo pod sono comuni nei miei account?
- Quali attività sono state indirizzate a questo pod?
- Quali container vengono eseguiti in questo pod?
- I registri dei container in questo pod sono comuni nei miei account?
- Quali altri container sono in esecuzione negli altri pod del carico di lavoro?
- Ci sono container anomali in questo pod che non si trovano negli altri pod del carico di lavoro?

Immagine di container

Le immagini di container presenti nei dati di origine di Detective.

> **Note**
>
> Per visualizzare i dettagli completi per questo tipo di entità, è necessario abilitare l'origine dati opzionale dei log di EKS controllo. Per maggiori informazioni, consulta Origini dati facoltative

Per ogni immagine di container, Detective risponde a domande come le seguenti:

- Quali altre immagini del mio ambiente condividono lo stesso repository o registro con questa immagine?
- Quante copie di questa immagine sono in esecuzione nel mio ambiente?

Soggetto Kubernetes

I soggetti Kubernetes presenti nei dati di origine di Detective. Un soggetto Kubernetes è un account utente o di servizio.

> **Note**
>
> Per visualizzare i dettagli completi per questo tipo di entità, è necessario abilitare l'origine dati opzionale dei log di EKS controllo. Per maggiori informazioni, consulta Origini dati facoltative

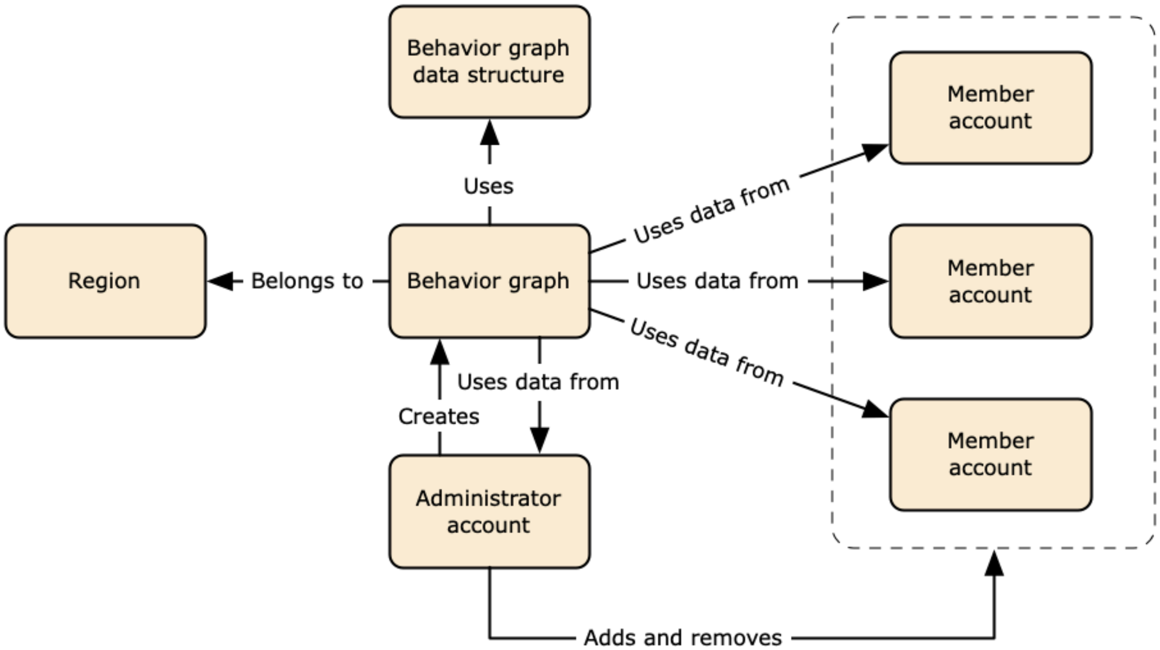
Per ogni soggetto, Detective risponde a domande come le seguenti:

- Quali IAM soggetti si sono autenticati come tale?
- Quali risultati sono associati a questo soggetto?
- Quali indirizzi IP utilizza il soggetto?

Dati di origine utilizzati in un grafico del comportamento del Detective

Per compilare un grafico di comportamento, Amazon Detective utilizza i dati di origine dell'account amministratore e degli account dei membri del grafico di comportamento.

Con Detective puoi accedere fino a un anno di dati storici degli eventi. Questi dati sono disponibili attraverso una serie di visualizzazioni che mostrano le variazioni del tipo e del volume di attività in una finestra temporale selezionata. Detective collega queste modifiche ai GuardDuty risultati.



Per i dettagli sulla struttura dei dati del grafico di comportamento, consulta [Panoramica della struttura dei dati del grafico di comportamento] nella Guida per l'utente di Detective.

Tipi di origini dati principali in Detective

Detective acquisisce i dati da questi tipi di AWS log:

- AWS CloudTrail registri
- Registri di flusso di Amazon Virtual Private Cloud (AmazonVPC)
  - Acquisisce entrambi IPv4 e IPv6 registra, ma non i MAC record prodotti da Elastic Fabric Adapters.
  - Inserisce i record di registro quando il valore del `log-status` campo è attivo. `OK` Per ulteriori informazioni, consulta i [record di log di flusso] nella Amazon VPC User Guide.
  - Acquisisce i log di flusso prodotti dalle istanze di Amazon Elastic Compute Cloud in esecuzione solo in quelle istanze. VPCs Non vengono utilizzate altre risorse, come NAT gateway, RDS istanze o cluster Fargate.
  - Acquisisce sia il traffico accettato che quello rifiutato.
- Per gli account registrati GuardDuty, il Detective acquisisce anche i risultati. GuardDuty

Detective consuma CloudTrail e registra gli eventi utilizzando flussi e log di VPC flusso indipendenti CloudTrail e VPC duplicati. Questi processi non influiscono né utilizzano le configurazioni esistenti

CloudTrail e VPC dei log di flusso. Inoltre, non influiscono sulle prestazioni né aumentano i costi di questi servizi.

Tipi di origini dati facoltativi in Detective

Detective offre pacchetti sorgente opzionali oltre alle tre fonti di dati offerte nel pacchetto principale Detective (il pacchetto principale include AWS CloudTrail log, log di VPC flusso e GuardDuty risultati). Un pacchetto di origini dati facoltativo può essere avviato o interrotto per un grafico di comportamento in qualsiasi momento.

Detective offre una prova gratuita di 30 giorni per tutti i pacchetti di origini principali e facoltativi per Regione.

> **Note**
>
> Detective conserva tutti i dati ricevuti da ciascun pacchetto di origini dati per un massimo di 1 anno.

Attualmente sono disponibili i seguenti pacchetti di origini facoltative:

- Log di verifica EKS

  Questo pacchetto opzionale di sorgenti dati consente a Detective di inserire informazioni dettagliate sui EKS cluster presenti nell'ambiente e di aggiungere tali dati al grafico del comportamento. Detective mette in correlazione le attività degli utenti con gli eventi di AWS CloudTrail gestione e le attività di rete con Amazon VPC Flow Logs senza che tu debba abilitare o archiviare questi log manualmente. Per informazioni dettagliate, vedi Registri EKS di controllo di Amazon.
- AWS risultati di sicurezza

  Questo pacchetto di origini dati facoltativi consente a Detective di importare dati da Centrale di sicurezza e di aggiungerli al grafico di comportamento. Per informazioni dettagliate, vedi AWS risultati di sicurezza.

Avvio o arresto di un'origine dati facoltativa:

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, in Impostazioni, scegli Generale.

3. In Pacchetti sorgente opzionali, seleziona Aggiorna. Quindi seleziona l'origine dati che desideri abilitare o deseleziona una casella per un'origine dati già abilitata e scegli Aggiorna per modificare i pacchetti di origini dati abilitati.

> **Note**
>
> Se arresti e poi riavvii un'origine dati facoltativa, vedrai una lacuna nei dati visualizzati su alcuni profili di entità. Questa lacuna verrà rilevata sul display della console e rappresenterà il periodo di tempo in cui l'origine dati è stata arrestata. Quando un'origine dati viene riavviata, Detective non importa i dati in modo retroattivo.

Registri EKS di controllo di Amazon

Amazon EKS audit logs è un pacchetto di sorgenti dati opzionale che può essere aggiunto al grafico comportamentale del Detective. Puoi visualizzare i pacchetti sorgente opzionali disponibili e il loro stato nel tuo account, dalla pagina Impostazioni della console o tramite il DetectiveAPI.

È disponibile una prova gratuita di 30 giorni per questa origini dati. Per ulteriori informazioni, consulta Versione di prova gratuita per origini dati facoltative.

L'abilitazione EKS dei log di controllo di Amazon consente a Detective di aggiungere informazioni approfondite sulle risorse create con Amazon EKS al tuo grafico comportamentale. Questa fonte di dati migliora le informazioni fornite sui seguenti tipi di entità: EKS Cluster, Kubernetes Pod, Container Image e Kubernetes subject.

Inoltre, se hai abilitato i log di EKS controllo come fonte di dati in Amazon, GuardDuty potrai vedere i dettagli dei risultati di Kubernetes da. GuardDuty Per maggiori informazioni sull'attivazione di questa fonte di dati, GuardDuty consulta la protezione di Kubernetes in Amazon. GuardDuty

> **Note**
>
> Questa origine dati è abilitata per impostazione predefinita per i nuovi grafici di comportamento creati dopo il 26 luglio 2022. Per i grafici di comportamento creati prima del 26 luglio 2022, deve essere abilitata manualmente.

Aggiungere o rimuovere i log EKS di controllo di Amazon come origine dati opzionale:

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, in Impostazioni, scegli Generale.
3. In Pacchetti sorgente, seleziona i log di EKS controllo per abilitare questa fonte di dati. Se è già abilitato, selezionalo nuovamente per interrompere l'inserimento dei log di EKS controllo nel tuo grafico comportamentale.

AWS risultati di sicurezza

AWS security findings è un pacchetto di sorgenti dati opzionale che può essere aggiunto al grafico del comportamento del Detective.

Puoi visualizzare i pacchetti sorgente opzionali disponibili e il loro stato nel tuo account, dalla pagina Impostazioni della console o tramite il DetectiveAPI.

È disponibile una prova gratuita di 30 giorni per questa origini dati. Per ulteriori informazioni, consulta Versione di prova gratuita per origini dati facoltative.

L'abilitazione dei risultati di AWS sicurezza consente a Detective di utilizzare i risultati di Security Hub aggregati da Security Hub dai servizi upstream in un formato di risultati standard chiamato AWS Security Format (ASFF), che elimina la necessità di lunghe conversioni dei dati. Quindi, correla i risultati acquisiti tra i prodotti per definire la priorità di quelli più importanti.

Aggiungere o rimuovere i risultati AWS di sicurezza come fonte di dati opzionale:

> **Note**
>
> L'origine dati sui risultati di AWS sicurezza è abilitata per impostazione predefinita per i nuovi grafici comportamentali creati dopo il 16 maggio 2023. Per i grafici del comportamento creati prima del 16 maggio 2023, deve essere abilitata manualmente.

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, in Impostazioni, scegli Generale.
3. In Pacchetti sorgente, seleziona i risultati AWS di sicurezza per abilitare questa fonte di dati. Se è già abilitato, selezionalo nuovamente per interrompere l'inserimento dei risultati di AWS Security Finding Format (ASFF) nel grafico comportamentale.

Risultati correntemente supportati

Detective acquisisce tutti i ASFF risultati in Security Hub dai servizi di proprietà di Amazon o AWS.

- Per visualizzare l'elenco delle integrazioni di servizi supportate, consulta Integrazioni di AWS servizi disponibili nella Guida per l' AWS Security Hub utente.
- Per l'elenco delle risorse supportate, consulta Risorse nella Guida per l'utente di AWS Security Hub .
- AWS I risultati dei servizi con uno stato di conformità non impostato su `FAILED` e i risultati aggregati interregionali non vengono inseriti.

Come Detective importa e archivia i dati di origine

Quando Detective è abilitato, Detective inizia a importare i dati di origine dall'account amministratore del grafico di comportamento. Man mano che gli account dei membri vengono aggiunti al grafico di comportamento, Detective inizia anche a utilizzare i dati di tali account membro.

I dati di origine di Detective sono costituiti da versioni strutturate ed elaborate dei feed originali. Per supportare l'analisi dei dati di Detective, archivia anche copie dei dati di origine di Detective.

Il processo di importazione di Detective inserisce i dati nei bucket Amazon Simple Storage Service (Amazon S3) dal datastore di origine di Detective. Con l'arrivo di nuovi dati di origine, altri componenti di Detective raccolgono i dati e avviano i processi di estrazione e analisi. Per ulteriori informazioni, consulta Come Detective utilizza i dati di origine per compilare un grafico di comportamento nella Guida per l'utente di Detective.

Come Detective applica la quota di volume di dati per i grafici del comportamento

Detective ha quote rigorose sul volume di dati che consente in ogni grafico di comportamento. Il volume di dati è la quantità di dati al giorno che confluisce nel grafico di comportamento di Detective.

Detective applica queste quote quando un account amministratore abilita Detective e quando un account membro accetta un invito a contribuire a un grafico di comportamento.

- Se il volume di dati per un account amministratore supera i 10 TB al giorno, l'account amministratore non può abilitare Detective.

- Se il volume di dati aggiunto proveniente da un account membro fa sì che il grafico di comportamento superi i 10 TB al giorno, l'account membro non può essere abilitato.

Il volume di dati per un grafico di comportamento può inoltre crescere naturalmente nel tempo. Detective controlla ogni giorno il volume dei dati del grafico di comportamento per assicurarsi che non superi la quota.

Se il volume di dati del grafico di comportamento si avvicina alla quota, Detective visualizza un messaggio di avviso sulla console. Per evitare di superare la quota, è possibile rimuovere gli account membri.

Se il volume di dati del grafico di comportamento supera i 10 TB al giorno, non è possibile aggiungere un nuovo account membro al grafico di comportamento.

Se il volume di dati del grafico di comportamento supera i 15 TB al giorno, Detective interrompe l'importazione dei dati nel grafico di comportamento. La quota di 15 TB al giorno riflette sia il normale volume di dati che i picchi del volume di dati. Quando viene raggiunta questa quota, non vengono inseriti nuovi dati nel grafico di comportamento, ma i dati esistenti non vengono rimossi. È comunque possibile utilizzare tali dati storici per le indagini. La console visualizza un messaggio per indicare che l'importazione dei dati è sospesa per il grafico di comportamento.

Se l'acquisizione dei dati è sospesa, è necessario intervenire per riattivarla. Supporto Se possibile, prima di contattare Supporto, prova a rimuovere gli account dei membri per portare il volume di dati al di sotto della quota. Ciò semplifica la riabilitazione dell'importazione dei dati per il grafico di comportamento.

Utilizzo della dashboard di riepilogo del Detective

Utilizza la dashboard di riepilogo in Amazon Detective per identificare le entità per indagare sull'origine dell'attività nelle 24 ore precedenti. La dashboard di Amazon Detective Summary ti aiuta a identificare le entità associate a tipi specifici di attività insolite. È uno dei tanti possibili punti di partenza per un'indagine.

Per visualizzare la dashboard Riepilogo, nel riquadro di navigazione Detective, scegli Riepilogo. La dashboard Riepilogo viene visualizzata anche per impostazione predefinita quando si apre per la prima volta la console Detective.

Dalla dashboard di riepilogo, puoi identificare le entità che soddisfano i seguenti criteri:

- Indagini che mostrano potenziali eventi di sicurezza identificati da Detective
- Entità coinvolte in attività che si sono verificate in geolocalizzazioni appena osservate
- Entità che hanno effettuato il maggior numero di API chiamate
- EC2istanze con il maggior volume di traffico
- Cluster di container con il maggior numero di container

Da ogni pannello della dashboard di riepilogo, puoi passare al profilo di un'entità selezionata.

Mentre esamini la dashboard di riepilogo, puoi modificare l'orario di Scope in modo da visualizzare l'attività per qualsiasi periodo di 24 ore nei 365 giorni precedenti. Quando modifichi la data e l'ora di inizio, la data e l'ora di fine vengono aggiornate automaticamente a 24 ore dall'ora di inizio scelta.

Con Detective puoi accedere fino a un anno di dati storici degli eventi. Questi dati sono disponibili attraverso una serie di visualizzazioni che mostrano le variazioni del tipo e del volume di attività in una finestra temporale selezionata. Detective collega queste modifiche ai GuardDuty risultati.

Per ulteriori informazioni sui dati di origine in Detective, consulta Dati di origine utilizzati in un grafico comportamentale.

Indagini

Il pannello Indagini riporta i potenziali eventi di sicurezza identificati da Detective. Nel pannello Indagini, è possibile visualizzare le indagini critiche e i ruoli e utenti AWS corrispondenti che sono stati interessati dagli eventi di sicurezza in un determinato periodo di tempo. Le indagini raggruppano gli indicatori di compromissione per aiutare a determinare se una AWS risorsa è coinvolta in attività insolite che potrebbero indicare un comportamento dannoso e il relativo impatto.

Seleziona Visualizza tutte le indagini per esaminare i risultati, valutare i gruppi di risultati e i dettagli delle risorse per accelerare le indagini di sicurezza. Le indagini vengono visualizzate in base al periodo di validità selezionato. È possibile modificare il periodo di validità per visualizzare le indagini in un intervallo di tempo di 24 ore nei 365 giorni precedenti. Puoi passare direttamente a Indagini critiche per visualizzare un rapporto di indagine dettagliato.

Se identificate un AWS ruolo o un utente che sembra avere attività sospette, potete passare direttamente dal pannello Investigazioni al ruolo o all'utente per continuare l'indagine. Passa a un ruolo o un utente e fai clic su Esegui indagine per generare un rapporto sulle indagini. Dopo aver eseguito un'indagine su un ruolo o un utente, il ruolo o l'utente viene spostato nella scheda Indagine eseguita.

Geolocalizzazioni appena osservate

Le geolocalizzazioni appena osservate evidenziano le località geografiche che sono state all'origine dell'attività nelle 24 ore precedenti, ma che non erano state rilevate durante il periodo di riferimento precedente.

Il pannello include fino a 100 geolocalizzazioni. Le posizioni sono contrassegnate sulla mappa ed elencate nella tabella sotto la mappa.

Per ogni geolocalizzazione, la tabella mostra il numero di API chiamate fallite e riuscite effettuate da tale geolocalizzazione nelle 24 ore precedenti.

Puoi espandere ogni geolocalizzazione per visualizzare l'elenco degli utenti e dei ruoli che hanno effettuato chiamate da quella geolocalizzazione. API Per ogni principale, la tabella elenca il tipo e l' Account AWS associato.

Se identifichi un ruolo o un utente che sembra sospetto, puoi passare direttamente dal pannello al profilo del ruolo o dell'utente per continuare l'indagine. Per passare a un profilo, scegli l'identificatore dell'utente o del ruolo.

Detective determina la posizione delle richieste utilizzando i database MaxMind GeoIP. MaxMind riporta un'accuratezza molto elevata dei propri dati a livello nazionale, sebbene la precisione vari in base a fattori quali il paese e il tipo di IP. Per ulteriori informazioni su MaxMind, consulta Geolocalizzazione MaxMind IP. Se ritieni che uno qualsiasi dei dati GeoIP sia errato, puoi inviare una richiesta di correzione a Maxmind all'indirizzo MaxMind Correct Geo Data. IP2

Gruppi di risultati attivi negli ultimi 7 giorni

La sezione Gruppi di risultati attivi negli ultimi 7 giorni mostra raggruppamenti correlati di risultati, entità e prove di Detective che si sono verificati nel tuo ambiente in un determinato periodo di tempo. Questi raggruppamenti mettono in correlazione attività insolite che potrebbero indicare un comportamento dannoso. La dashboard riassuntiva mostra fino a cinque gruppi ordinati in base ai gruppi contenenti i risultati più critici che sono stati attivi nell'ultima settimana.

Puoi selezionare i valori nei contenuti Tattica, Account, Risorse e Risultati per visualizzare maggiori dettagli.

I gruppi di risultati vengono generati su base giornaliera. Se identifichi un gruppo di risultati che ti interessa, puoi selezionare il titolo per passare alla visualizzazione dettagliata del profilo di un gruppo e continuare l'indagine.

Ruoli e utenti con il maggior volume di API chiamate

Ruoli e utenti con il maggior volume di API chiamate identificano gli utenti e i ruoli che hanno effettuato il maggior numero di API chiamate nelle 24 ore precedenti.

Il pannello può includere fino a 100 utenti e ruoli. Per ogni utente o ruolo, puoi vedere il tipo (utente o ruolo) e l'account associato. Puoi anche visualizzare il numero di API chiamate emesse da quell'utente o ruolo nelle 24 ore precedenti.

Per impostazione predefinita, vengono visualizzati i ruoli collegati ai servizi. I ruoli collegati ai servizi possono generare grandi volumi di AWS CloudTrail attività, il che sostituisce i principali che desideri approfondire. Puoi scegliere di disattivare Mostra ruoli collegati ai servizi, per filtrare i ruoli collegati al servizio dalla visualizzazione riassuntiva del dashboard.

Puoi esportare un file con valori separati da virgole (.csv) che contiene i dati in questo pannello.

È inoltre disponibile una cronologia del volume delle API chiamate dei 7 giorni precedenti. La cronologia può aiutarti a determinare se il volume delle API chiamate è insolito per quel preside.

Se identifichi un utente o un ruolo per il quale il volume delle API chiamate sembra sospetto, puoi passare direttamente dal pannello al profilo dell'utente o del ruolo per continuare l'indagine. Puoi anche visualizzare il profilo dell'account associato all'utente o al ruolo. Per visualizzare un profilo, scegli l'utente, il ruolo o l'identificatore dell'account.

EC2istanze con il maggior volume di traffico

EC2le istanze con il maggior volume di traffico identificano le EC2 istanze che hanno registrato il maggior volume totale di traffico nelle 24 ore precedenti.

Il pannello può includere fino a 100 istanze. EC2 Per ogni EC2 istanza, puoi visualizzare l'account associato e il numero di byte in entrata, di byte in uscita e di byte totali delle 24 ore precedenti.

È possibile esportare un file di valori separati da virgole (.csv) che contiene i dati in questo pannello.

Puoi anche visualizzare una sequenza temporale che mostra il traffico in entrata e in uscita nei 7 giorni precedenti. La cronologia può aiutare a determinare se il volume di traffico è insolito per quel caso. EC2

Se identifichi un'EC2istanza con un volume di traffico sospetto, puoi passare direttamente dal pannello al profilo dell'EC2istanza per continuare l'indagine. Puoi anche visualizzare il profilo dell'account proprietario dell'EC2istanza. Per visualizzare un profilo, scegli l'identificatore dell'EC2istanza o dell'account.

Cluster di container con il maggior numero di pod Kubernetes

La sezione Cluster di container con il maggior numero di pod Kubernetes identifica i cluster con il maggior numero di container in esecuzione nelle 24 ore precedenti.

Questo pannello include fino a 100 cluster organizzati in base ai quali ai cluster era associato il maggior numero di risultati. Per ogni cluster è possibile visualizzare l'account associato, il numero corrente di container in quel cluster e il numero di risultati associati al cluster nelle ultime 24 ore. È possibile esportare un file di valori separati da virgole (.csv) che contiene i dati in questo pannello.

Se identifichi un cluster con risultati recenti, potete passare direttamente dal pannello al profilo del cluster per continuare l'indagine. Puoi anche passare al profilo dell'account proprietario del cluster. Per passare a un profilo, scegli il nome del cluster o l'identificatore dell'account.

Notifica del valore approssimativo

In Ruoli e utenti con il maggior volume di API chiamate e EC2istanze con il maggior volume di traffico, se un valore è seguito da un asterisco (*), significa che il valore è un'approssimazione. Il valore vero è uguale o maggiore del valore visualizzato.

Ciò si verifica a causa del metodo utilizzato da Detective per calcolare il volume per ogni intervallo di tempo. Nella pagina Riepilogo, l'intervallo di tempo è di un'ora.

Per ogni ora, Detective calcola il volume totale per i 1.000 utenti, ruoli o EC2 istanze con il volume maggiore. Esclude i dati per gli utenti, i ruoli o le istanze rimanenti. EC2

Se una risorsa a volte si trovava tra le prime 1.000 e a volte no, il volume calcolato per quella risorsa potrebbe non includere tutti i dati. Vengono esclusi i dati relativi agli intervalli di tempo in cui non era tra i primi 1.000.

Tieni presente che questo vale solo per la pagina Riepilogo. Il profilo dell'utente, del ruolo o dell'EC2istanza fornisce dettagli precisi.

Come viene utilizzato Detective per le indagini

Amazon Detective consente di analizzare, esaminare e identificare rapidamente la causa principale dei risultati di sicurezza o delle attività sospette. Detective fornisce strumenti a supporto dell'intero processo di indagine. Un'indagine in Detective può iniziare da un risultato, un gruppo di risultati o un'entità.

Fasi investigative in Detective

Qualsiasi processo investigativo da Detective prevede le seguenti fasi:

Triage

Il processo di indagine inizia quando si riceve una notifica relativa a un caso sospetto di attività dannosa o ad alto rischio. Ad esempio, ti viene assegnato il compito di esaminare i risultati o gli avvisi rilevati da servizi come Amazon GuardDuty e Amazon Inspector.

Nella fase di triage, stabilisci se ritieni che l'attività sia un vero positivo (una reale attività dannosa) o un falso positivo (attività non dannosa o ad alto rischio). I profili Detective supportano il processo di triage fornendo informazioni sull'attività dell'entità coinvolta.

Per i casi di vero positivo, si passa alla fase successiva.

Analisi dell'ambito

Durante la fase di analisi dell'ambito, gli analisti determinano l'entità dell'attività dannosa o ad alto rischio e la causa sottostante.

L'analisi dell'ambito risponde ai seguenti tipi di domande:

- Quali sistemi e utenti sono stati compromessi?
- Da dove ha avuto origine l'attacco?
- Da quanto tempo è in corso l'attacco?
- Ci sono altre attività correlate da considerare? Ad esempio, se un utente malintenzionato sta estraendo dati dal sistema, come li ha ottenuti?

Le visualizzazioni di Detective possono aiutarti a identificare altre entità coinvolte o interessate.

Risposta

Il passaggio finale consiste nel rispondere all'attacco per fermarlo, minimizzare i danni ed evitare che un attacco simile si ripeta.

Punti di partenza per un'indagine investigativa

Ogni indagine in Detective ha un punto di partenza essenziale. Ad esempio, ti potrebbe essere assegnato un Amazon GuardDuty o un AWS Security Hub risultato su cui indagare. Oppure potresti essere preoccupato per le attività insolite relative a un indirizzo IP specifico.

I punti di partenza tipici di un'indagine includono i risultati rilevati dai dati di origine del Detective GuardDuty e le entità estratte dai dati di origine.

Risultati rilevati da GuardDuty

GuardDuty utilizza i dati di registro per scoprire casi sospetti di attività dannose o ad alto rischio. Detective fornisce risorse che ti aiutano a indagare su questi risultati.

Per ogni risultato, Detective fornisce i relativi dettagli. Detective mostra anche le entità, come gli indirizzi IP e AWS gli account, collegate alla scoperta.

È quindi possibile esaminare l'attività delle entità coinvolte per determinare se l'attività rilevata dal risultato sia davvero motivo di preoccupazione.

Per ulteriori informazioni, consulta the section called “Panoramica degli esiti”.

AWS risultati di sicurezza aggregati da Security Hub

AWS Security Hub aggrega i risultati di sicurezza di vari fornitori di risultati in un unico posto e offre una visione completa dello stato di sicurezza in. AWS Centrale di sicurezza elimina la complessità di indirizzare grandi volumi di risultati provenienti da più provider. Riduce lo sforzo richiesto per gestire e migliorare la sicurezza di tutti gli AWS account, le risorse e i carichi di lavoro. Detective fornisce risorse che ti aiutano a indagare su questi risultati.

Per ogni risultato, Detective fornisce i relativi dettagli. Detective mostra anche le entità, come gli indirizzi IP e AWS gli account, collegate alla scoperta.

Per ulteriori informazioni, consulta the section called “Panoramica degli esiti”.

Entità estratte dai dati di origine di Detective

Dai dati di origine di Detective importati, Detective estrae entità come indirizzi IP e utenti AWS . Puoi usare una di queste entità come punto di partenza per l'indagine.

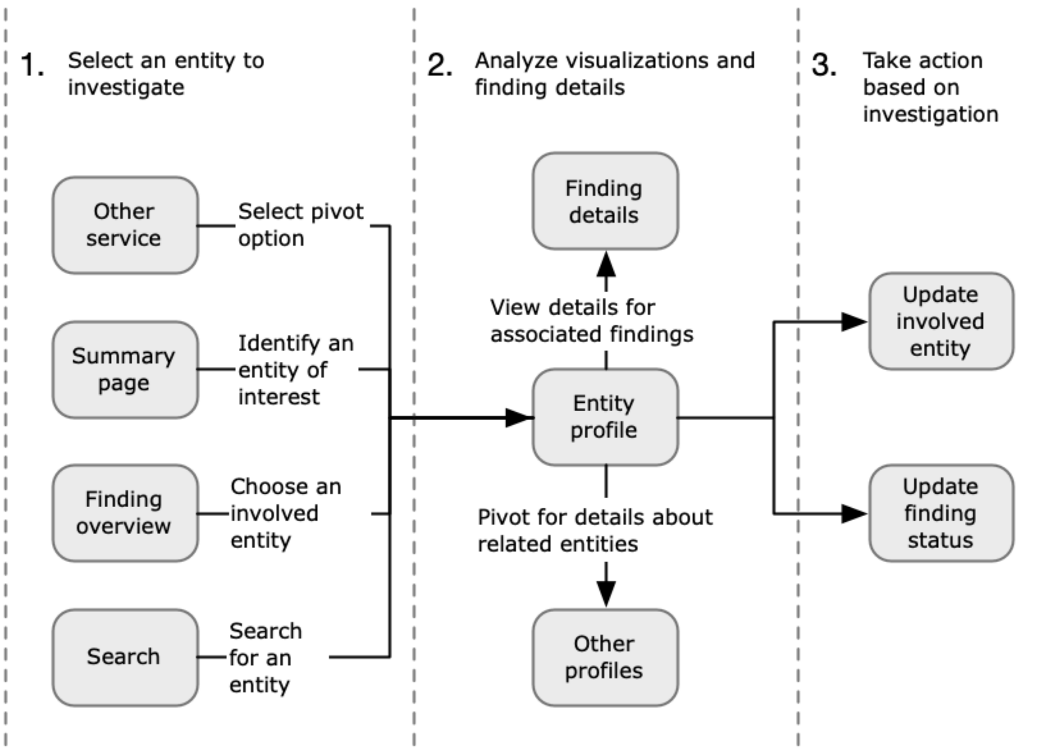
Detective fornisce dettagli generali sull'entità, come l'indirizzo IP o il nome utente. Fornisce anche i dettagli sulla cronologia delle attività. Ad esempio, Detective può segnalare a quali altri indirizzi IP un'entità si è connessa, è stata connessa o ha utilizzato.

Per ulteriori informazioni, consulta Analisi delle entità.

Flusso investigativo investigativo

Puoi usare Amazon Detective per indagare su un'entità come un'EC2istanza o un AWS utente. Puoi anche esaminare i risultati di sicurezza.

A un livello elevato, l'immagine seguente mostra il processo di un'Indagine Detective.



Fase 1: Selezione dell'entità da esaminare

Quando esaminano un reperto GuardDuty, gli analisti possono scegliere di indagare su un'entità associata in Detective. Per informazioni, consulta the section called “Passaggio da un'altra console”.

Selezionando l'entità si accede al profilo dell'entità in Detective.

Fase 2: Analisi delle visualizzazioni sui profili

Ogni profilo di entità contiene una serie di visualizzazioni generate dal grafico di comportamento. Il grafico di comportamento viene creato dai file di log e da altri dati che vengono inseriti in Detective.

Le visualizzazioni mostrano attività correlate a un'entità. Queste visualizzazioni vengono utilizzate per rispondere a domande volte a determinare se l'attività dell'entità è insolita. Per informazioni, consulta Analisi delle entità.

Per condurre un'indagine, puoi utilizzare la guida di Detective fornita per ogni visualizzazione. Questa guida delinea le informazioni visualizzate, suggerisce domande da porre e propone i passaggi successivi in base alle risposte. Per informazioni, consulta the section called “Utilizzo della guida del pannello del profilo”.

Ogni profilo contiene un elenco di risultati associati. È possibile visualizzare i dettagli di un risultato e visualizzare la panoramica dei risultati. Per informazioni, consulta the section called “Visualizzazione dei risultati per un'entità”.

Da un profilo di entità, puoi passare ad altri profili di entità e di risultati per approfondire le attività relative alle risorse correlate.

Fase 3: Operazioni

In base ai risultati dell'indagine, intraprendi le azioni appropriate.

Se il risultato è un falso positivo, puoi archiviarlo. Da Detective, puoi archiviare GuardDuty i risultati. Per maggiori dettagli, consulta Archiviazione di un GuardDuty risultato Amazon.

Altrimenti, intraprendi le azioni appropriate per risolvere la vulnerabilità e mitigare i danni. Ad esempio, potrebbe essere necessario aggiornare la configurazione di una risorsa.

Indagine Detective

Puoi utilizzare Amazon Detective Investigation per indagare su IAM utenti e IAM ruoli utilizzando indicatori di compromissione, che possono aiutarti a determinare se una risorsa è coinvolta in un incidente di sicurezza. Un indicatore di compromissione (IOC) è un artefatto osservato in o su una rete, sistema o ambiente che può (con un alto livello di sicurezza) identificare attività dannose o incidenti di sicurezza. Con Detective Investigations puoi massimizzare l'efficienza, concentrarti sulle minacce alla sicurezza e rafforzare le capacità di risposta all'incidenza.

Detective Investigation utilizza modelli di apprendimento automatico e intelligence sulle minacce per analizzare automaticamente le risorse nell' AWS ambiente e identificare potenziali incidenti di sicurezza. Consente di utilizzare in modo proattivo, efficace ed efficiente l'automazione basata sul grafico di comportamento di Detective per migliorare le operazioni di sicurezza. Usando Detective Investigation puoi indagare sulle tattiche di attacco, sui viaggi impossibili, sugli indirizzi IP contrassegnati e sulla ricerca di gruppi. Esegue le fasi iniziali di indagine sulla sicurezza e genera un report che evidenzia i rischi identificati da Detective, per aiutarti a comprendere gli eventi di sicurezza e rispondere a potenziali incidenti.

Argomenti

- Esecuzione di un'indagine investigativa
- Revisione dei rapporti delle Indagini Detective
- Comprensione di un rapporto di Investigazioni Detective
- Riepilogo del rapporto Detective Investigations
- Scaricamento di un rapporto sulle Indagini Detective
- Archiviazione di un rapporto di Investigazioni Detective

Esecuzione di un'indagine investigativa

Usa Esegui indagine per analizzare risorse come IAM utenti e IAM ruoli e per generare un rapporto di indagine. Il rapporto generato descrive in dettaglio il comportamento anomalo che indica un potenziale compromesso.

Console

Segui questi passaggi per eseguire un'indagine investigativa dalla pagina Investigazioni utilizzando la console Amazon Detective.

1. Accedi alla console di AWS gestione. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione scegli Indagini
3. Nella pagina Investigazioni, scegli Esegui indagine nell'angolo in alto a destra.

4. Nella sezione Seleziona risorsa, hai tre modi per condurre un'indagine. Puoi scegliere di condurre l'indagine su una risorsa consigliata dal Detective. Puoi eseguire l'indagine per una risorsa specifica. Puoi anche esaminare una risorsa dalla pagina Ricerca di Detective.

    1. `Choose a recommended resource`— Detective consiglia le risorse in base alla sua attività nei risultati e nei gruppi di ricerca. Per eseguire l'indagine su una risorsa consigliata dal Detective, nella tabella Risorse consigliate, selezionare una risorsa da esaminare.

        La tabella Risorse consigliate fornisce i seguenti dettagli:

        - Risorsa ARN: il nome della risorsa Amazon (ARN) della AWS risorsa.
        - Motivo dell'indagine: visualizza i motivi principali per esaminare la risorsa. I motivi per cui Detective suggerisce di esaminare una risorsa sono i seguenti:
            - Se una risorsa è stata coinvolta in un esito di elevata gravità nelle ultime 24 ore.
            - Se una risorsa è stata coinvolta in un gruppo di risultati osservati negli ultimi sette giorni. I gruppi di risultati di Detective ti consentono di esaminare più attività in relazione a un potenziale evento di sicurezza. Per ulteriori dettagli, consulta the section called “Ricerca di gruppi”.
            - Se una risorsa è stata coinvolta in un esito negli ultimi sette giorni.
        - Risultati più recenti: i risultati più recenti hanno la priorità all'inizio dell'elenco.
        - Tipo di risorsa: identifica il tipo di risorsa. Ad esempio, un AWS utente o un AWS ruolo.
    2. `Specify an AWS role or user with an ARN`— È possibile selezionare un AWS ruolo o un AWS utente ed eseguire un'indagine per la risorsa specifica.

        Segui questi passaggi per esaminare un tipo di risorsa specifico.

        a. Dall'elenco a discesa Seleziona il tipo di risorsa, scegli AWS ruolo o AWS utente.

        b. Inserisci la risorsa ARN della risorsa. IAM Per maggiori dettagli su ResourceARNs, consulta Amazon Resource Names (ARNs) nella Guida IAM per l'utente.
    3. `Find a resource to investigate from the Search page`— Puoi cercare tutte le tue IAM risorse dalla pagina Detective Search.

        Segui questi passaggi per esaminare una risorsa dalla pagina di ricerca.

        a. Nel riquadro di navigazione selezionare Search (Cerca).

        b. Nella pagina di ricerca, cerca una IAM risorsa.

        c. Vai alla pagina del profilo della risorsa ed esegui l'indagine da lì.

5. Nella sezione Ambito temporale dell'indagine, scegli l'intervallo temporale dell'indagine per valutare l'attività della risorsa selezionata. Puoi selezionare una data di inizio e un'ora di inizio; e data di fine e ora di fine nel UTC formato. Il periodo di validità selezionato può essere compreso tra un minimo di 3 ore e un massimo di 30 giorni.
6. Scegli Esegui indagine.

API

Per condurre un'indagine in modo programmatico, usa l'StartInvestigationoperazione del Detective. API Per eseguire un'indagine utilizzando AWS Command Line Interface (AWS CLI), esegui il comando start-investigation.

Nella richiesta, utilizza questi parametri per eseguire un'indagine in Detective:

- `GraphArn`— Specificare l'Amazon Resource Name (ARN) del grafico comportamentale.
- `EntityArn`— Specificare l'unico Amazon Resource Name (ARN) dell'IAMutente e del IAM ruolo.
- `ScopeStartTime`: facoltativamente, specifica la data e l'ora a partire dalle quali deve iniziare l'indagine. Il valore è una stringa in formato UTC ISO86 01. Ad esempio, `2021-08-18T16:35:56.284Z`.
- `ScopeEndTime`: facoltativamente, specifica la data e l'ora in cui deve terminare l'indagine. Il valore è una stringa in formato UTC ISO86 01. Ad esempio, `2021-08-18T16:35:56.284Z`.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
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
```

Puoi anche eseguire un'indagine dalle seguenti pagine di Detective:

- Una pagina del profilo IAM utente o del IAM ruolo in Detective.
- Il pannello di visualizzazione grafica di un gruppo di ricerca.

- La colonna Operazioni di una risorsa coinvolta.
- IAMutente o IAM ruolo in una pagina di ricerca.

Dopo che Detective ha eseguito l'indagine su una risorsa, viene generato un report di indagini. Per accedere al rapporto, vai a Indagini dal riquadro di navigazione.

Revisione dei rapporti delle Indagini Detective

I report di indagini ti consentono di esaminare i report generati per le indagini che hai eseguito in precedenza in Detective.

Esaminare i report di indagini

1. Accedi alla console di AWS gestione. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione scegli Indagini

Prendi nota dei seguenti attributi tratti da un report di indagini.

- ID: l'identificatore generato del report sulle indagini. Puoi scegliere questo ID per leggere un riepilogo del report di indagine, che contiene i dettagli dell'indagine.
- Stato: a ogni indagine è associato uno stato basato sullo stato di completamento dell'indagine. I valori dello stato possono essere In corso, Completata o Non riuscita.
- Gravità: a ogni indagine viene assegnata una gravità. Detective assegna automaticamente una gravità al risultato.

  Una gravità rappresenta la disposizione analizzata dall'indagine su una singola risorsa in un determinato periodo di validità. Una gravità segnalata da un'indagine non implica né indica in altro modo la criticità o l'importanza che una risorsa interessata potrebbe avere per l'organizzazione.

  I valori di gravità delle indagini possono essere Critico, Alto, Medio, Basso o Informativo, dal più grave al meno grave.

  Le indagini a cui viene assegnato un valore di gravità Critico o Alto devono avere la priorità per ulteriori ispezioni, poiché è più probabile che rappresentino problemi di sicurezza ad alto impatto identificati da Detective.
- Entità: la colonna Entità contiene dettagli sulle entità specifiche rilevate nell'indagine. Alcune entità sono AWS account, come utente e ruolo.

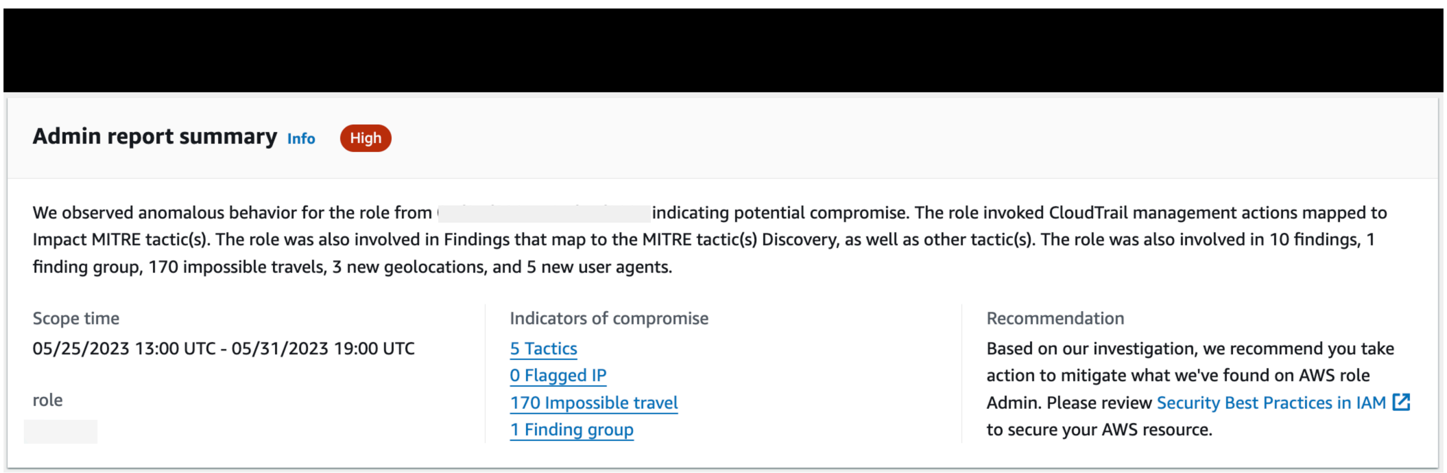
- Stato: la colonna Data di creazione contiene dettagli sulla data e l'ora in cui il report di indagine è stato creato per la prima volta.

Comprensione di un rapporto di Investigazioni Detective

Un rapporto di Investigazioni Detective elenca un riepilogo dei comportamenti non comuni o delle attività dannose che indicano una compromissione. Elenca inoltre le raccomandazioni suggerite da Detective per mitigare il rischio per la sicurezza.

Visualizzare un report di indagini relativo a un ID di indagine specifico.

1. Accedi alla console di AWS gestione. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione scegli Indagini
3. Nella tabella Report, seleziona un ID dell'indagine.



Detective genera il report per il periodo di validità e l'utente selezionati. Il report contiene una sezione Indicatori di compromesso che include dettagli su uno o più degli indicatori di compromesso elencati di seguito. Quando esamini ogni indicatore di compromesso, facoltativamente scegli un elemento di cui approfondire ed esaminarne i dettagli.

- Tattiche. Tecniche e procedure: identifica tattiche, tecniche e procedure (TTPs) utilizzate in un potenziale evento di sicurezza. Il framework MITRE ATT &CK viene utilizzato per comprendere il. TTPs Le tattiche si basano sulla [matrice MITRE ATT &CK for Enterprise](https://attack.mitre.org/matrices/enterprise/).
- Indirizzi IP segnalati da intelligence delle minacce: gli indirizzi IP sospetti vengono contrassegnati e identificati come minacce critiche o gravi sulla base dell'intelligence delle minacce di Detective.

- Impossible Travel: rileva e identifica attività utente insolite e impossibili per un account. Ad esempio, questo indicatore riporta un cambiamento drastico tra la posizione di origine e quella di destinazione di un utente in un breve lasso di tempo.
- Gruppo di risultati correlato: mostra più attività correlate a un potenziale evento di sicurezza. Detective utilizza tecniche di analisi dei grafici che deducono le relazioni tra risultati ed entità e li raggruppa in un gruppo di risultati.
- Risultati correlati: le attività correlate associate a un potenziale evento di sicurezza. Elenca tutte le categorie distinte di prove collegate alla risorsa o al gruppo di risultati.
- Nuove geolocalizzazioni: identifica le nuove geolocalizzazioni utilizzate a livello di risorsa o di account. Ad esempio, questo indicatore elenca una geolocalizzazione osservata che è una posizione poco frequente o inutilizzata in base all'attività precedente dell'utente.
- Nuovi agenti utente: identifica i nuovi agenti utente utilizzati a livello di risorsa o di account.
- Nuovo ASOs: identifica le nuove Organizzazioni di sistema autonome (ASOs) utilizzate a livello di risorsa o di account. Ad esempio, questo indicatore elenca una nuova organizzazione assegnata comeASO.

Riepilogo del rapporto Detective Investigations

Il riepilogo delle indagini evidenzia gli indicatori anomali che richiedono attenzione, per il periodo di tempo selezionato. Utilizzando il riepilogo, è possibile identificare più rapidamente la causa principale dei potenziali problemi di sicurezza, identificare i modelli e comprendere le risorse interessate dagli eventi di sicurezza.

Nel riepilogo dettagliato del report di indagini puoi visualizzare i dettagli seguenti.

Panoramica delle indagini

Nel pannello Panoramica, puoi vedere una visualizzazione delle attività IPs con elevata gravità, che può fornire maggiori informazioni sul percorso di un aggressore.

Il Detective evidenzia Attività insolite nelle indagini, ad esempio l'impossibilità dell'IAMutente di viaggiare da una fonte a una destinazione lontana.

Detective mappa le indagini in base a tattiche, tecniche e procedure (TTPs) utilizzate in un potenziale evento di sicurezza. Il framework MITRE ATT &CK viene utilizzato per comprendere il. TTPs Le tattiche si basano sulla matrice MITRE ATT &CK for Enterprise.

Indicatori delle indagini

È possibile utilizzare le informazioni nel riquadro Indicatori per determinare se una risorsa AWS è coinvolta in attività insolite che potrebbero indicare un comportamento dannoso e il relativo impatto. Un indicatore di compromissione (IOC) è un artefatto osservato in o su una rete, sistema o ambiente in grado (con un elevato livello di sicurezza) di identificare attività dannose o incidenti di sicurezza.

Scaricamento di un rapporto sulle Indagini Detective

Puoi scaricare il rapporto Detective Investigations in JSON formato, per analizzarlo ulteriormente o archiviarlo nella tua soluzione di archiviazione preferita, come un bucket Amazon S3.

Download di un report di indagini dalla tabella Report.

1. Accedi alla console di gestione. AWS Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione scegli Indagini
3. Seleziona un'indagine dalla tabella Report, quindi scegli Scarica.

Download di un report di indagini dalla pagina di riepilogo.

1. Accedi alla console AWS di gestione. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione scegli Indagini
3. Seleziona un'indagine dalla tabella Report.
4. Nella pagina di riepilogo delle indagini, scegli Scarica.

Archiviazione di un rapporto di Investigazioni Detective

Una volta completata l'indagine in Amazon Detective, puoi archiviare il report di indagini. Un'indagine archiviata indica che hai completato la revisione dell'indagine.

Puoi archiviare o annullare l'archiviazione di un'indagine solo se sei un amministratore di Detective. Detective conserverà le indagini archiviate per 90 giorni.

Per archiviare un rapporto di indagine dalla tabella Report.

1. Accedi alla console di AWS gestione. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.

2. Nel riquadro di navigazione scegli Indagini
3. Seleziona un'indagine dalla tabella Rapporti, quindi scegli Archivia.

Archiviare un report di indagine dalla pagina di riepilogo.

1. Accedi alla console AWS di gestione. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione scegli Indagini
3. Seleziona un'indagine dalla tabella Report.
4. Nella pagina di riepilogo delle indagini, scegli Archivia.

Analisi dei risultati in Amazon Detective

Un risultato è un'istanza di un'attività potenzialmente dannosa o di altro rischio rilevato. Amazon GuardDuty e i risultati AWS di sicurezza vengono caricati in Amazon Detective in modo che tu possa utilizzare Detective per indagare sulle attività associate alle entità coinvolte. GuardDuty i risultati fanno parte del pacchetto principale di Detective e vengono inseriti di default. Tutti gli altri risultati AWS di sicurezza aggregati da Security Hub vengono inseriti come fonte di dati opzionale. Per maggiori dettagli, consulta Dati di origine utilizzati in un grafico di comportamento.

Una panoramica dei risultati di Detective fornisce informazioni dettagliate sul risultato. Visualizza anche un riepilogo delle entità coinvolte, con collegamenti ai profili delle entità associate.

Se un risultato è correlato a un'attività più ampia, Detective avvisa di passare al gruppo di risultati. Consigliamo di utilizzare i gruppi di risultati per continuare l'indagine in quanto questi gruppi consentono di esaminare più attività relative a un potenziale evento di sicurezza. Per informazioni, consulta the section called “Ricerca di gruppi”.

Amazon Detective offre una visualizzazione interattiva dei gruppi di risultati. Questa visualizzazione è progettata per aiutarti a esaminare i problemi in modo più rapido e approfondito con meno sforzo. Il pannello Visualizzazione del gruppo di risultati mostra i risultati e le entità coinvolte in un gruppo di risultati. È possibile utilizzare questa visualizzazione interattiva per analizzare, comprendere e valutare l'impatto del gruppo di risultati. Questo pannello consente di visualizzare le informazioni presentate nella tabella Entità coinvolte e Risultati coinvolti. Dalla presentazione visiva, è possibile selezionare i risultati o le entità per ulteriori analisi. Vedi Finding group visualization.

Indice

Analisi di una panoramica dei risultati in Detective

Una panoramica dei risultati di Detective fornisce informazioni dettagliate sul risultato. Visualizza anche un riepilogo delle entità coinvolte, con collegamenti ai profili delle entità associate.

Periodo di validità utilizzato per la panoramica dei risultati

Il periodo di validità per una panoramica dei risultati è impostato sulla finestra dell'ora del risultato. La finestra dell'ora del risultato riporta la prima e l'ultima volta in cui l'attività del risultato è stata osservata.

Dettagli degli esiti

Il pannello a destra contiene i dettagli del risultato. Questi sono i dettagli forniti dal provider dei risultati.

Dai dettagli del risultato, puoi anche archiviare il risultato. Per maggiori dettagli, consulta Archiviazione di un GuardDuty risultato Amazon.

Entità correlate

Una panoramica dei risultati contiene un elenco delle entità coinvolte nel risultato. Per ogni entità, l'elenco fornisce informazioni generali sull'entità. Queste informazioni riflettono le informazioni sul pannello del profilo dei dettagli dell'entità sul profilo dell'entità corrispondente.

Puoi filtrare l'elenco in base al tipo di entità. È possibile inoltre filtrare l'elenco in base al testo dell'identificatore di entità.

Per passare al profilo di un'entità, scegli Vedi profilo. Quando si passa al profilo dell'entità, si verifica quanto segue:

- Il periodo di validità è impostato sulla finestra dell'ora del risultato.
- Nel pannello Risultati associati per l'entità, il risultato è selezionato. I dettagli del risultato rimangono visualizzati sulla destra del profilo dell'entità.

Risoluzione dei problemi relativi a "Pagina non trovata"

Quando accedi a un'entità o a un esito in Detective, potresti visualizzare un messaggio di errore Pagina non trovata.

Per risolvere il problema, procedi in uno dei seguenti modi:

- Assicurati che l'entità o l'esito appartenga a uno dei tuoi account membro. Per informazioni su come esaminare gli account dei membri, consulta Visualizzazione dell'elenco degli account.

- Assicurati che il tuo account amministratore sia allineato a GuardDuty e/o Security Hub per passare a Detective da questi servizi. Per i consigli, consulta Allineamento consigliato con GuardDuty e Security Hub.
- Verifica che l'esito si sia verificato dopo che l'account membro ha accettato l'invito.
- Verifica che il grafico del comportamento di Detective stia importando dati da un pacchetto di origine dati opzionale. Per ulteriori informazioni sui dati di origine utilizzati nei grafici comportamentali del Detective, consulta Dati di origine utilizzati in un grafico comportamentale.
- Per consentire a Detective di importare dati da Security Hub e aggiungerli al grafico del comportamento, devi abilitare Detective for AWS security findings come pacchetto di origine dati. Per ulteriori informazioni, consulta i risultati AWS di sicurezza.
- Se stai accedendo al profilo di un'entità o stai cercando una panoramica in Detective, assicurati che URL sia nel formato giusto. Per i dettagli sulla formazione di un profiloURL, vedi Navigare verso un profilo di entità o Trovare una panoramica utilizzando. URL

Analisi dei gruppi di risultati

I gruppi di risultati di Amazon Detective ti consentono di esaminare più attività in relazione a un potenziale evento di sicurezza. Un gruppo di ricerca in Amazon Detective viene creato quando Detective rileva uno schema o una relazione tra più risultati che suggerisce che siano correlati allo stesso potenziale incidente di sicurezza. Questo raggruppamento aiuta a gestire e analizzare i risultati correlati in modo più efficiente.

È possibile analizzare la causa principale dei GuardDuty risultati di elevata gravità utilizzando i gruppi di ricerca. Se un autore della minaccia sta tentando di compromettere l' AWS ambiente, in genere esegue una sequenza di azioni che portano a molteplici risultati di sicurezza e a comportamenti insoliti. Queste operazioni sono spesso distribuite nel tempo e nelle entità. L'indagine isolata dei risultati relativi alla sicurezza può portare a un'interpretazione errata del loro significato e alla difficoltà di individuarne la causa principale. Amazon Detective risolve questo problema applicando una tecnica di analisi dei grafici che deduce le relazioni tra risultati ed entità e li raggruppa in un gruppo di risultati. Consigliamo di trattare i gruppi di risultati come punto di partenza per indagare sulle entità e sui risultati coinvolti.

Detective analizza i dati dei risultati e li raggruppa con altri risultati che potrebbero essere correlati in base alle risorse che condividono. Ad esempio, è molto probabile che i risultati relativi alle azioni intraprese dalle stesse sessioni di IAM ruolo o provenienti dallo stesso indirizzo IP facciano parte della stessa attività sottostante. È utile indagare sui risultati e sulle prove in gruppo, anche se le associazioni fatte da Detective non sono correlate.

I gruppi di ricerca vengono creati in base ai seguenti criteri.

- Prossimità temporale: i risultati che si verificano in un periodo di tempo ristretto vengono spesso raggruppati, poiché probabilmente sono correlati allo stesso incidente.
- Entità comuni: i risultati che coinvolgono le stesse entità, come indirizzi IP, utenti o risorse, vengono raggruppati. Questo aiuta a comprendere la portata dell'incidente in diverse parti dell'ambiente.
- Modelli e comportamenti — Il Detective analizza i modelli e i comportamenti contenuti nei risultati, come tipi simili di attacchi o attività sospette, per determinare le relazioni e raggrupparle di conseguenza.
- Tattiche, tecniche e procedure (TTPs): i risultati che hanno caratteristiche similiTTPs, come descritto in framework come MITRE ATT &CK, vengono raggruppati per evidenziare potenziali attacchi coordinati.

Questi criteri aiutano a semplificare il processo di indagine in modo da poterti concentrare su risultati correlati che probabilmente rappresentano lo stesso incidente di sicurezza.

Oltre ai risultati, ogni gruppo include le entità coinvolte nei risultati. Le entità possono includere risorse esterne, AWS ad esempio indirizzi IP o agenti utente.

> **Note**
>
> Dopo un GuardDuty risultato iniziale correlato a un altro risultato, il gruppo di ricerca con tutti i risultati correlati e tutte le entità coinvolte viene creato entro 48 ore.

Comprendere la pagina dei gruppi di risultati

La pagina dei gruppi di risultati elenca tutti i gruppi di risultati raccolti da Amazon Detective dal tuo grafico comportamentale. Prendi nota dei seguenti attributi dei gruppi di ricerca:

Gravità di un gruppo

A ciascun gruppo di risultati viene assegnata una gravità in base alla gravità dei risultati associati al AWS Security Finding Format (ASFF). ASFFi valori di gravità dei risultati sono Critico, Alto, Medio, Basso o Informativo, dal più elevato al meno grave. La gravità di un raggruppamento è uguale al risultato con gravità più elevata tra tutti i risultati del gruppo.

Ai gruppi costituiti da risultati con gravità Critica o Elevata che hanno un impatto su un gran numero di entità dovrebbe essere data priorità ai fini delle indagini, poiché è più probabile che rappresentino problemi di sicurezza ad alto impatto.

Titolo del gruppo

Nella colonna Titolo, ogni gruppo ha un ID univoco e un titolo non univoco. Questi si basano sul ASFF tipo di namespace del gruppo e sul numero di risultati all'interno di tale namespace nel cluster. Ad esempio, se un raggruppamento ha il titolo: Group with: TTP(2), Effect (1) e Unusual behavior (2), include cinque risultati totali costituiti da due risultati nello spazio dei nomi, un risultato nello spazio dei TTPnomi Effect e due risultati nello spazio dei nomi Unusual Behavior. Per un elenco completo dei namespace, consulta la tassonomia dei tipi per. ASFF

Tattiche in un gruppo

La colonna Tattiche di un gruppo indica in quale categoria di tattiche rientra l'attività. Le categorie di tattiche, tecniche e procedure nell'elenco seguente sono allineate alla matrice &CK. MITRE ATT

Puoi selezionare una tattica sulla catena per vedere una descrizione della tattica. Successivamente nella catena c'è un elenco delle tattiche rilevate all'interno del gruppo. Queste categorie e le attività che in genere rappresentano sono le seguenti:

- Accesso iniziale: un malintenzionato sta cercando di entrare nella rete di qualcun altro.
- Esecuzione: un malintenzionato sta cercando di entrare nella rete di qualcun altro.
- Persistenza: un malintenzionato sta cercando di mantenere il proprio punto d'appoggio.
- Aumento dei privilegi: un malintenzionato sta cercando di ottenere autorizzazioni di livello superiore.
- Evasione della difesa: un malintenzionato sta cercando di evitare di essere scoperto.
- Accesso alle credenziali: un malintenzionato sta cercando di rubare nomi di account e password.
- Rilevamento: un malintenzionato sta cercando di comprendere e conoscere un ambiente.

- Movimento laterale: un malintenzionato sta cercando di muoversi in un ambiente.
- Collezione: un malintenzionato sta cercando di raccogliere dati utili al suo obiettivo.
- Comando e controllo: un malintenzionato sta cercando di entrare nella rete di qualcun altro.
- Esfiltrazione: un malintenzionato sta cercando di rubare dati.
- Impatto: un malintenzionato sta cercando di manipolare, interrompere o distruggere i tuoi sistemi e i tuoi dati.
- Altro: indica un'attività derivante da un risultato che non è in linea con le tattiche elencate nella matrice.

Entità all'interno di un gruppo

La colonna Entità contiene dettagli sulle entità specifiche rilevate all'interno di questo raggruppamento. Seleziona questo valore per una suddivisione delle entità in base alle categorie Identità, Rete, Archiviazione ed Elaborazione. Esempi di entità in ogni categoria sono:

- Identità: IAM principi e Account AWS, ad esempio, utente e ruolo
- Rete: indirizzo IP o altre reti ed entità VPC
- Storage: bucket Amazon S3 o DDBs
- Calcola EC2 istanze Amazon o contenitori Kubernetes

Account all'interno di un gruppo

La colonna Account indica quali AWS account possiedono le entità coinvolte nei risultati del gruppo. Gli AWS account sono elencati per nome e AWS ID in modo da poter dare priorità alle indagini sulle attività che coinvolgono account critici.

Risultati all'interno di un gruppo

La colonna Risultati contiene un elenco delle entità all'interno di un gruppo per gravità. I risultati includono i risultati di Amazon, GuardDuty i risultati di Amazon Inspector, i risultati AWS sulla sicurezza e le prove di Detective. Puoi selezionare il grafico per visualizzare un conteggio esatto dei risultati in base alla gravità.

GuardDuty i risultati fanno parte del pacchetto principale di Detective e vengono inseriti di default. Tutti gli altri risultati AWS di sicurezza aggregati da Security Hub vengono inseriti come fonte di dati opzionale. Per maggiori dettagli, consulta Dati di origine utilizzati in un grafico di comportamento.

Risultati informativi nei gruppi di risultati

Amazon Detective identifica ulteriori informazioni relative a un gruppo di risultati sulla base dei dati del grafico di comportamento raccolti negli ultimi 45 giorni. Detective presenta queste informazioni come un risultato con gravità informativa. Le prove forniscono informazioni di supporto che evidenziano un'attività insolita o un comportamento sconosciuto potenzialmente sospetto se osservati all'interno di un gruppo di risultati. Ciò potrebbe includere geolocalizzazioni o API chiamate osservate di recente nell'ambito di un rilevamento. I risultati delle prove sono visualizzabili solo in Detective e non vengono inviati a AWS Security Hub.

Detective determina la posizione delle richieste utilizzando i database MaxMind GeoIP. MaxMind riporta un'accuratezza molto elevata dei propri dati a livello nazionale, sebbene la precisione vari in base a fattori quali il paese e il tipo di IP. Per ulteriori informazioni su MaxMind, consulta Geolocalizzazione MaxMind IP. Se ritieni che uno qualsiasi dei dati GeoIP sia errato, puoi inviare una richiesta di correzione a Maxmind all'indirizzo MaxMind Correct Geo Data. IP2

È possibile osservare le prove per diversi tipi principali (come IAM utente o IAM ruolo). Per alcuni tipi di prove, puoi osservare le prove per tutti gli account. Ciò significa che le prove influiscono sull'intero grafico di comportamento. Se si rileva un'evidenza probatoria per tutti gli account, si vedrà anche almeno un altro risultato probatorio informativo dello stesso tipo per un singolo IAM ruolo. Ad esempio, se visualizzi un risultato Nuova geolocalizzazione osservata per tutti gli account, ne vedrai un altra per Nuova geolocalizzazione osservata per un principale.

Tipi di prove nei gruppi di risultati

- Nuova geolocalizzazione osservata
- È stata osservata una nuova organizzazione del sistema autonomo (ASO)
- Nuovo agente utente osservato
- Nuova API chiamata emessa
- Nuova geolocalizzazione osservata per tutti gli account
- Nuovo IAM capitale osservato per tutti i conti

Profili dei gruppi di risultati

Quando si seleziona il titolo di un gruppo, si apre un profilo del gruppo di risultati con ulteriori dettagli su quel gruppo. Il pannello dei dettagli nella pagina del profilo dei gruppi di risultati supporta la visualizzazione di un massimo di 1.000 entità e risultati per i gruppi di risultati principali e secondari.

La pagina del profilo del gruppo mostra il periodo di validità impostato per il gruppo. Si tratta della data e dell'ora comprese tra il primo risultato o la prima prova inclusi nel gruppo al risultato o alla prova più recente aggiornata in un gruppo. Puoi anche vedere la gravità del gruppo di risultati, che è uguale alla categoria di gravità più alta tra i risultati del gruppo. Altri dettagli all'interno di questo pannello del profilo includono:

- La catena Tattiche coinvolte mostra quali tattiche sono attribuite ai risultati del gruppo. Le tattiche si basano sulla MITREATT&CK Matrix for Enterprise. Le tattiche sono mostrate come una catena di punti colorati che rappresenta la progressione tipica di un attacco dalle fasi iniziali a quelle più recenti. Ciò significa che i cerchi più a sinistra della catena rappresentano in genere attività meno gravi dove un malintenzionato sta tentando di ottenere o mantenere l'accesso al tuo ambiente. Al contrario, le attività rivolte a destra sono le più gravi e possono includere la manomissione o la distruzione dei dati.
- Le relazioni che questo gruppo intrattiene con altri gruppi. Occasionalmente, uno o più gruppi di risultati precedentemente non collegati potrebbero essere uniti in un nuovo gruppo sulla base di un collegamento appena scoperto, ad esempio un esito che coinvolge entità dei gruppi esistenti. In questo caso, Amazon Detective disattiva i gruppi principali e crea un gruppo secondario. Puoi ricondurre la discendenza di qualsiasi gruppo ai suoi gruppi principali. I gruppi possono avere le relazioni seguenti:
  - Gruppo di risultati secondario: un gruppo di risultati creato quando un risultato coinvolto in altri due gruppi di risultati è coinvolto in un nuovo risultato. I gruppi principali dei risultati sono elencati per ogni gruppo secondario.
  - Gruppo di risultati principale: un gruppo di risultati è principale quando da esso è stato creato un gruppo secondario. Se un gruppo di risultati è un gruppo principale, i relativi gruppi secondari vengono elencati insieme ad esso. Lo stato di un gruppo principale diventa Inattivo quando viene unito a un gruppo secondario Attivo.

Ci sono due schede informative che aprono i pannelli del profilo. Utilizzando le schede Entità coinvolte e Risultati coinvolti, è possibile visualizzare ulteriori dettagli sul gruppo.

Usa Esegui indagine per generare un report sulle indagini. Il rapporto generato descrive in dettaglio il comportamento anomalo che indica un compromesso.

Profilo all'interno dei gruppi

Entità coinvolte

Si concentra sulle entità del gruppo di risultati, compresi i risultati all'interno del gruppo a cui ciascuna entità è collegata. Vengono inoltre visualizzati i tag allegati a ciascuna entità in modo da poter identificare rapidamente le entità importanti in base ai tag. Seleziona un'entità per visualizzarne il profilo.

Risultati coinvolti

Contiene dettagli su ogni risultato, inclusa la gravità del risultato, ogni entità coinvolta e quando quel risultato è stato visto per la prima e l'ultima volta. Seleziona un tipo di risultato nell'elenco per aprire un pannello dei dettagli del risultato con informazioni aggiuntive su tale risultato. Come parte del pannello Risultati coinvolti, potresti visualizzare risultati informativi basati su prove di Detective dal tuo grafico di comportamento.

Visualizzazione dei gruppi di risultati

Amazon Detective offre una visualizzazione interattiva dei gruppi di risultati. Questa visualizzazione è progettata per aiutarti a esaminare i problemi in modo più rapido e approfondito con meno sforzo. Il pannello Visualizzazione del gruppo di risultati mostra i risultati e le entità coinvolte in un gruppo di risultati. È possibile utilizzare questa visualizzazione interattiva per analizzare, comprendere e valutare l'impatto del gruppo di risultati. Questo pannello consente di visualizzare le informazioni presentate nella tabella Entità coinvolte e Risultati coinvolti. Dalla presentazione visiva, è possibile selezionare i risultati o le entità per ulteriori analisi.

I gruppi di risultati di Detective con risultati aggregati sono un gruppo di risultati collegati allo stesso tipo di risorsa. Con i risultati aggregati, puoi valutare rapidamente la composizione di un gruppo di risultati e interpretare più rapidamente i problemi di sicurezza. Nel pannello dei dettagli dei gruppi di risultati, vengono combinati risultati simili ed è possibile espandere i risultati per visualizzare insieme risultati relativamente simili. Ad esempio, un nodo di evidenza, che presenta risultati informativi e risultati medi dello stesso tipo. Al momento, è possibile visualizzare il titolo, l'origine, il tipo e la gravità dei gruppi di risultati con risultati aggregati.

Da questo pannello interattivo puoi:

- Usa Esegui indagine per generare un report sulle indagini. Il report generato descrive in dettaglio il comportamento anomalo che indica una compromissione. Per maggiori dettagli, vedi Investigazioni Detective.
- Visualizzare maggiori dettagli sui gruppi di risultati con risultati aggregati per analizzare le prove, le entità e i risultati coinvolti.
- Visualizza le etichette delle entità e dei risultati per identificare le entità interessate con potenziali problemi di sicurezza. Puoi disattivare l'etichetta.
- Riorganizza le entità e i risultati per comprendere meglio la loro interconnessione. Isola le entità e i risultati da un gruppo spostando l'elemento selezionato nel gruppo di risultati.
- Seleziona le prove, le entità e i risultati per visualizzare maggiori dettagli su di essi. Per selezionare più elementi, scegli `command/control` e scegli gli elementi o trascinali e rilasciali usando il puntatore.
- Modifica il layout per adattare tutte le entità e i risultati alla finestra del gruppo di risultati. Visualizza quali tipi di entità sono prevalenti in un gruppo di risultati.

> **Note**
>
> Il pannello Visualizzazione del gruppo di risultati supporta la visualizzazione di gruppi di risultati con un massimo di 100 entità e risultati.

È possibile utilizzare il menu a discesa per visualizzare i risultati e le entità in un layout radiale, circolare, diretto dalla forza o a griglia. Il layout radiale offre una visualizzazione migliorata per una più facile interpretazione dei dati. Il layout a forza diretta posiziona le entità e i risultati in modo che i collegamenti abbiano una lunghezza costante tra gli elementi e che siano distribuiti in modo uniforme. Questo aiuta a ridurre le sovrapposizioni. Il layout selezionato definisce il posizionamento dei risultati nel pannello Visualizzazione.

Layout della sequenza temporale

Il layout della sequenza temporale offre un modo dinamico per visualizzare l'evoluzione dei gruppi di ricerca nel tempo. Questo ti consente di vedere la progressione degli eventi, aiutandoti a comprendere meglio la sequenza e la potenziale causalità degli incidenti di sicurezza utilizzando Detective.

Usa il cursore della timeline nella parte inferiore del pannello di visualizzazione per selezionare un momento specifico. La visualizzazione verrà aggiornata per mostrare lo stato del gruppo di ricerca in quel momento. Il pulsante play che ti consente di avanzare automaticamente nella timeline. Fai clic sul pulsante play per avviare l'animazione. La visualizzazione si aggiornerà in tempo reale, mostrando come cambia il gruppo di ricerca nel tempo. Usa il pulsante di pausa per interrompere l'animazione in qualsiasi momento.

Ora puoi filtrare i risultati in base al loro livello di gravità utilizzando il menu a discesa Filtro. Quando applichi un filtro, la visualizzazione si aggiornerà per mostrare solo i risultati che corrispondono al livello di gravità selezionato. Il filtro influisce solo sui risultati mostrati nella timeline, non nella visualizzazione completa di Finding Group. Ciò consente di concentrarsi rapidamente su problemi ad alta priorità o di esaminare tipi specifici di risultati.

Puoi utilizzare la funzionalità di filtro in combinazione con il layout della sequenza temporale per vedere come emergono ed evolvono nel tempo i risultati con diversi livelli di gravità.

Workflow investigativo migliorato

Con l'aggiunta del layout della sequenza temporale e delle funzionalità di filtro, ora puoi condurre indagini ancora più complete:

1. Inizia visualizzando l'intero gruppo di risultati utilizzando uno dei layout statici (Radial, Circle, Force-directed o Grid).
2. Usa le tempistiche per capire come si è sviluppata la situazione nel tempo.
3. Usa il pulsante play per avanzare automaticamente nella timeline, osservando i momenti o gli schemi chiave.
4. Fai una pausa nei punti significativi per approfondire.
5. Applica filtri per concentrarti sui risultati di livelli di gravità specifici.
6. Usa le scorciatoie da tastiera e gli strumenti di selezione per approfondire le entità e i risultati di interesse.

Questo flusso di lavoro migliorato consente un'indagine più dettagliata e approfondita di scenari di sicurezza complessi. È possibile condurre indagini di sicurezza più efficienti ed efficaci, con conseguente risoluzione degli incidenti più rapida e un miglioramento del livello di sicurezza generale.

Tasti di scelta rapida

Puoi utilizzare le seguenti scorciatoie da tastiera per interagire con il pannello di visualizzazione del gruppo di risultati:

- Clic: seleziona un singolo nodo, deseleziona tutti gli altri nodi, deseleziona tutti i nodi se si fa clic su uno spazio bianco.
- Ctrl + Click: seleziona un singolo nodo, non deseleziona gli altri nodi.
- Trascina: sposta la vista.
- Ctrl + Drag — Marquee seleziona, non deseleziona gli altri nodi.
- Shift + Drag — Marquee seleziona e deseleziona tutti gli altri nodi.
- Tasti freccia: modifica il focus tra i nodi.
- Ctrl + Space: seleziona o deseleziona il nodo attualmente focalizzato.
- Shift + Tasti freccia: modifica il focus tra i nodi e li seleziona.

La legenda dinamica cambia in base alle entità e ai risultati nel grafico corrente. Ti aiuta a identificare ciò che rappresenta ogni elemento visivo.

Riepilogo dei gruppi di risultati basato sull'IA generativa

Per impostazione predefinita, Amazon Detective fornisce automaticamente i riepiloghi di un singolo gruppo di risultati. I riepiloghi sono basati su modelli di intelligenza artificiale generativa (IA generativa) ospitati su Amazon Bedrock.

Con i gruppi di risultati, puoi esaminare più risultati di sicurezza, in quanto si riferiscono a un potenziale evento di sicurezza, e identificare i potenziali attori delle minacce. I riepiloghi dei gruppi di risultati si basano su queste funzionalità. I riepiloghi di gruppi di risultati utilizzano i dati per un gruppo di sicurezza, analizzano rapidamente le relazioni tra i risultati e le risorse interessate, quindi riassumono le potenziali minacce in linguaggio naturale. Puoi utilizzare questi riepiloghi per identificare le maggiori minacce alla sicurezza, migliorare l'efficienza delle indagini e abbreviare i tempi di risposta.

> **Note**
>
> I riepiloghi dei gruppi di sicurezza basati sull'IA generativa possono fornire, e non sempre, informazioni completamente accurate. Consulta la sezione [AWS Politica di intelligenza artificiale responsabile](#) per ulteriori informazioni.

Revisione del riepilogo del gruppo di risultati

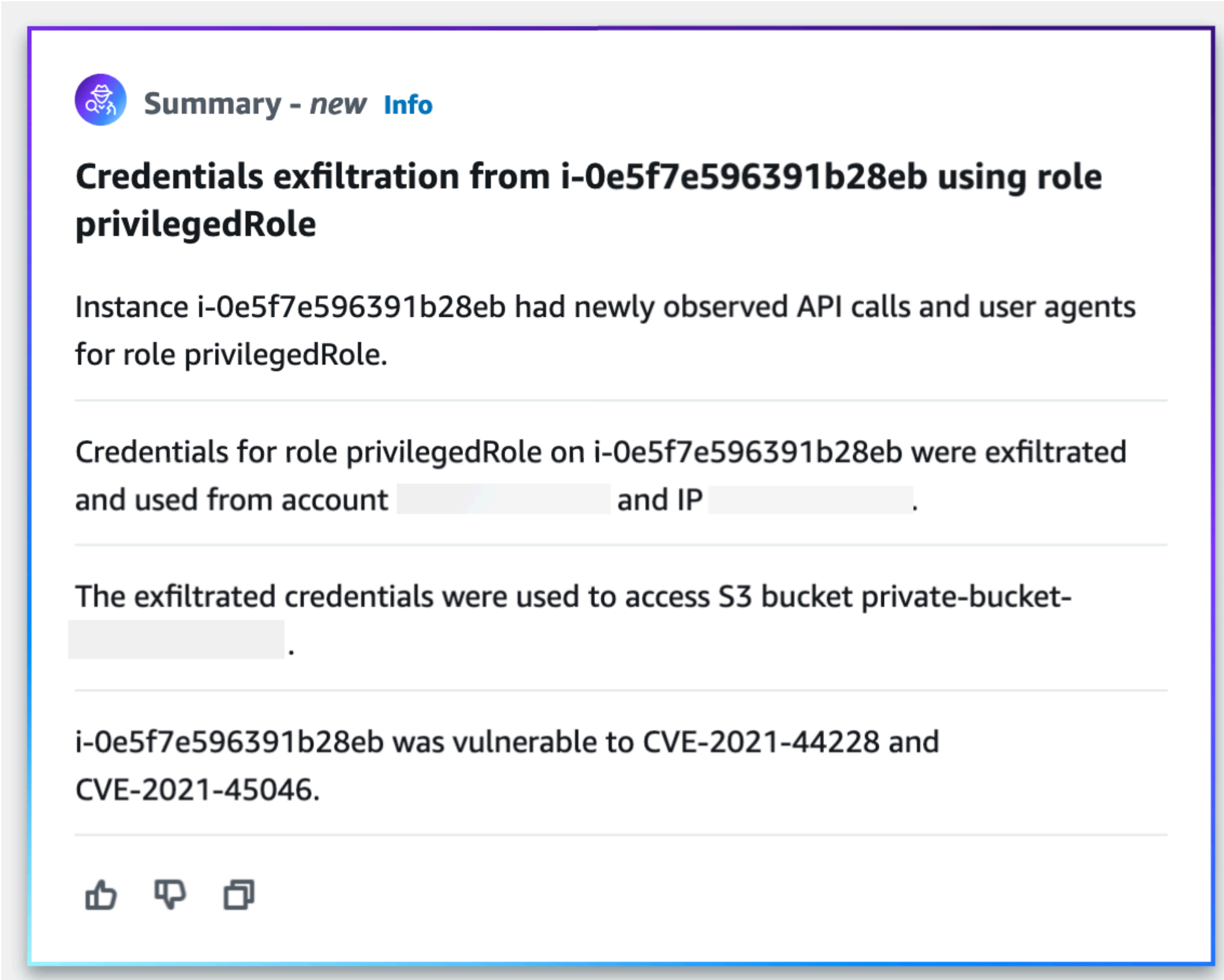
Il riepilogo del gruppo di risultati per un gruppo di risultati fornisce una spiegazione chiara e dettagliata di un evento di sicurezza. In linguaggio naturale, la spiegazione include un titolo succinto, un riepilogo delle risorse coinvolte e le informazioni dettagliate su tali risorse.

Rivedere un riepilogo del gruppo di risultati

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione scegli Gruppi di risultati.
3. Nella tabella Gruppi di risultati, scegli il gruppo di risultati di cui desideri visualizzare un riepilogo. Viene visualizzata una pagina dei dettagli.

Nella pagina dei dettagli, è possibile utilizzare il riquadro Riepilogo per esaminare un riepilogo descrittivo generato dei principali risultati del gruppo di risultati. È inoltre possibile esaminare un'analisi dei principali eventi di minaccia nel gruppo di risultati, che possono essere approfonditi ulteriormente. Per aggiungere il riepilogo generato alle tue note o a un sistema di creazione di ticket, scegli l'icona di copia nel riquadro. In questo modo, il riepilogo viene copiato negli appunti. Puoi anche condividere il tuo feedback sull'output di riepilogo del gruppo di risultati contenuto nel riepilogo, che può fornire un'esperienza migliore in futuro. Per condividere il tuo feedback, scegli l'icona con il pollice in su o il pollice in giù, a seconda della natura del feedback.

> **Note**
>
> Se fornisci un feedback sul riepilogo del gruppo di risultati, il tuo feedback non viene utilizzato per la messa a punto del modello. Li usiamo solo per garantire che le istruzioni in Detective siano realizzate in modo efficace.



Disabilitazione del riepilogo del gruppo di risultati

Per impostazione predefinita, il riepilogo dei gruppi di risultati è abilitato per i gruppi di risultati. Puoi disabilitare il riepilogo del gruppo di risultati in qualsiasi momento. Se li disabiliti, potrai abilitarli in un secondo momento.

Disabilitare il riepilogo del gruppo di risultati

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, scegli Preferences (Preferenze).
3. In Riepilogo del gruppo di risultati, scegli Modifica.
4. Disattiva Abilitato.

5. Seleziona Salva.

Abilitazione del riepilogo del gruppo di risultati

Se in precedenza hai disabilitato il riepilogo del gruppo di risultati, puoi abilitarlo nuovamente in qualsiasi momento.

Abilitare il riepilogo del gruppo di risultati

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, scegli Preferences (Preferenze).
3. In Riepilogo del gruppo di risultati, scegli Modifica.
4. Attiva Abilitato.
5. Seleziona Salva.

Regioni supportate

Il riepilogo del gruppo Finding è disponibile di seguito AWS Regioni.

- Stati Uniti orientali (Virginia settentrionale)
- US West (Oregon)
- Asia Pacifico (Tokyo)
- Europa (Francoforte)

Archiviazione di una ricerca su Amazon GuardDuty

Una volta completata l'indagine su un GuardDuty ritrovamento di Amazon, puoi archiviarlo su Amazon Detective. Questo ti evita la fatica di dover tornare GuardDuty per effettuare l'aggiornamento. L'archiviazione di un risultato indica che l'indagine è terminata.

Puoi archiviare un GuardDuty risultato dall'interno di Detective solo se sei anche l'account GuardDuty amministratore dell'account associato al risultato. Se non sei un account GuardDuty amministratore e tenti di archiviare un risultato, GuardDuty visualizza un errore.

Per archiviare un GuardDuty risultato

1. Accedi alla console AWS di gestione. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nella console Detective, nel pannello dei dettagli dei risultati, scegli Archivia ricerca.
3. Quando viene chiesto di confermare, seleziona Archivia.

Puoi visualizzare i GuardDuty risultati archiviati nella GuardDuty console. I risultati archiviati vengono archiviati GuardDuty per 90 giorni e possono essere visualizzati in qualsiasi momento durante tale periodo. È possibile visualizzare i risultati soppressi nella GuardDuty console selezionando Archived dalla tabella dei risultati oppure GuardDuty API utilizzando il criterio ListFindingsAPIcon un findingCriteria criterio di service.archived uguale a true. Per ulteriori informazioni, consulta Suppression Rules nella Amazon GuardDuty User Guide.

Analisi delle entità in Amazon Detective

Un'entità è un singolo oggetto estratto dai dati di origine. Gli esempi includono un indirizzo IP specifico, un'EC2istanza Amazon o un AWS account. Per un elenco dei tipi di evento, consulta the section called “Tipi di entità nella struttura dei dati del grafico di comportamento”.

Un profilo di entità di Amazon Detective è una singola pagina che fornisce informazioni dettagliate sull'entità e la sua attività. Puoi utilizzare un profilo di entità per ottenere dettagli di supporto per un'indagine su un risultato o come parte di una ricerca generale di attività sospette.

Indice

Utilizzo dei profili di entità

Un profilo di entità viene visualizzato quando si completa una delle seguenti operazioni:

- Dalla GuardDuty console Amazon, scegli l'opzione per indagare su un'entità correlata a un risultato selezionato.

  Per informazioni, consulta the section called “Passaggio da un'altra console”.
- Passa all'URL di Detective per il profilo dell'entità.

  Per informazioni, consulta the section called “Navigazione tramite un URL”.
- Usa la ricerca Detective nella console di Detective per cercare un'entità.
- Scegli un link al profilo dell'entità da un altro profilo di entità o da una panoramica dei risultati.

Periodo di validità per un profilo di entità

Quando si accede direttamente a un profilo di entità senza fornire il periodo di validità, questo periodo viene impostato sulle 24 ore precedenti.

Quando si passa a un profilo di entità da un altro profilo di entità, il periodo di validità selezionato correntemente rimane invariato.

Quando si passa a un profilo di entità da una panoramica di risultati, il periodo di validità viene impostato sulla finestra dell'ora del risultato.

Per informazioni sulla personalizzazione dell'intervallo temporale per limitare i dati visualizzati nei profili delle entità, consulta Gestione del periodo di validità.

Identificatore e tipo di entità

Nella parte superiore del profilo ci sono l'identificatore e il tipo di entità. A ogni tipo di entità è associata un'icona che fornisce un indicatore visivo del tipo di profilo.

Risultati coinvolti

Ogni profilo contiene un elenco di risultati in cui l'entità è stata coinvolta durante il periodo di validità.

Per cercare altre risorse coinvolte, è possibile visualizzare i dettagli di ogni risultato, modificare il periodo di validità in modo che rifletta la finestra dell'ora del risultato e passare alla panoramica dei risultati.

Per informazioni, consulta the section called “Visualizzazione dei risultati per un'entità”.

Gruppi di risultati che coinvolgono questa entità

Ogni profilo contiene un elenco di gruppi di risultati in cui è inclusa un'entità.

Un gruppo di risultati è composto da risultati, entità e prove che Detective raccoglie in un gruppo per fornire un contesto più approfondito sui possibili problemi di sicurezza.

Per ulteriori informazioni sui gruppi di risultati, consulta the section called “Ricerca di gruppi”.

Pannelli del profilo contenenti i dettagli dell'entità e i risultati delle analisi

Un profilo di entità contiene una serie di una o più schede. Ogni scheda contiene uno o più pannelli di profilo. Ogni pannello del profilo contiene testo e visualizzazioni generati dai dati del grafico di comportamento. I pannelli specifici di schede e profili sono personalizzati in base al tipo di entità.

Per la maggior parte delle entità, il pannello nella parte superiore della prima scheda fornisce informazioni di riepilogo di alto livello sull'entità.

Altri pannelli del profilo evidenziano diversi tipi di attività. Per un'entità coinvolta in un risultato, le informazioni contenute nei pannelli relativi al profilo dell'entità possono fornire ulteriori prove a sostegno del completamento di un'indagine. Ogni pannello del profilo fornisce l'accesso a linee guida su come utilizzare le informazioni. Per ulteriori informazioni, consulta the section called “Utilizzo della guida del pannello del profilo”.

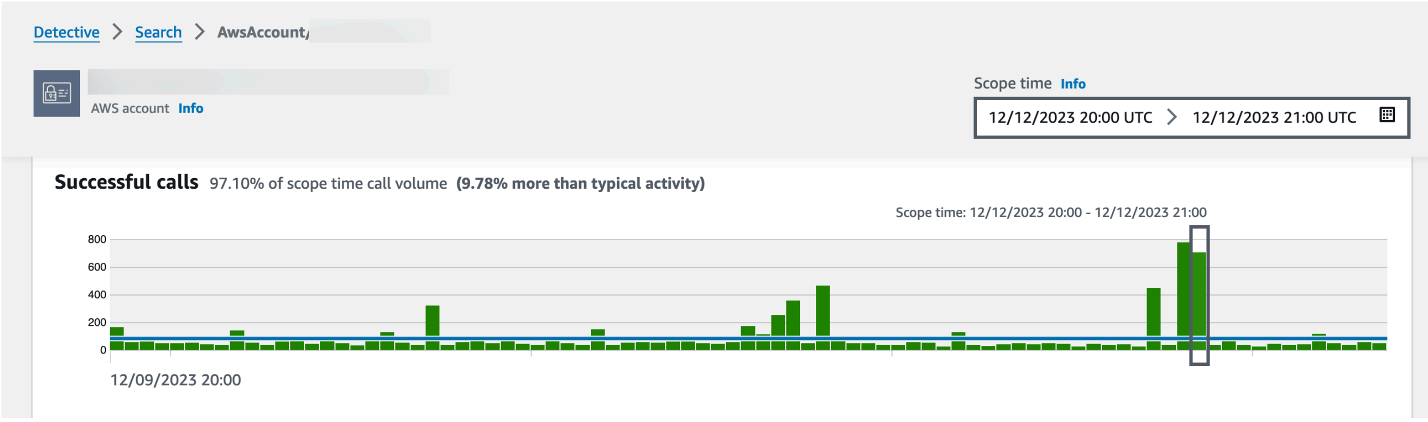
Per maggiori dettagli sui pannelli del profilo, sui tipi di dati che contengono e sulle opzioni disponibili per interagire con essi, consulta the section called “Pannelli di profilo”.

Navigazione in un profilo di entità

Un profilo di entità contiene una serie di una o più schede. Ogni scheda contiene uno o più pannelli di profilo. Ogni pannello del profilo contiene testo e visualizzazioni generati dai dati del grafico di comportamento.

Mentre scorri verso il basso una scheda del profilo, le seguenti informazioni rimangono visibili nella parte superiore del profilo:

- Tipo di entità
- Identificatore dell'entità
- Periodo di validità



Visualizzazione e interazione con i pannelli del profilo del Detective

Ogni profilo di entità sulla console di Amazon Detective è costituito da una serie di pannelli di profilo. Un pannello di profilo è una visualizzazione che fornisce dettagli generali o evidenzia attività specifiche associate a un'entità. I pannelli di profilo utilizzano diversi tipi di visualizzazioni per presentare diversi tipi di informazioni. Possono anche fornire collegamenti a dettagli aggiuntivi o ad altri profili.

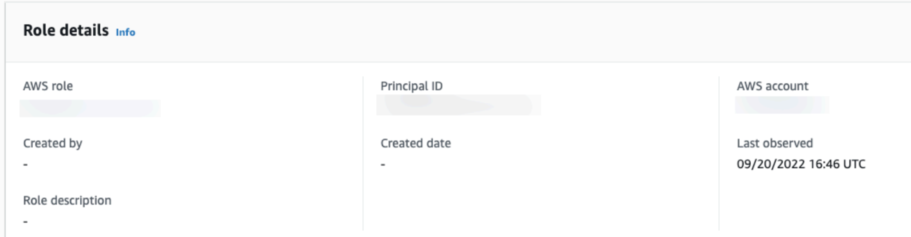
Ogni pannello di profilo ha lo scopo di aiutare gli analisti a trovare risposte a domande specifiche sulle entità e sulle attività ad esse associate. Le risposte a queste domande aiutano a concludere se l'attività rappresenti una minaccia reale.

I pannelli di profilo utilizzano diversi tipi di visualizzazioni per presentare diversi tipi di informazioni.

Tipi di informazioni su un pannello di profilo

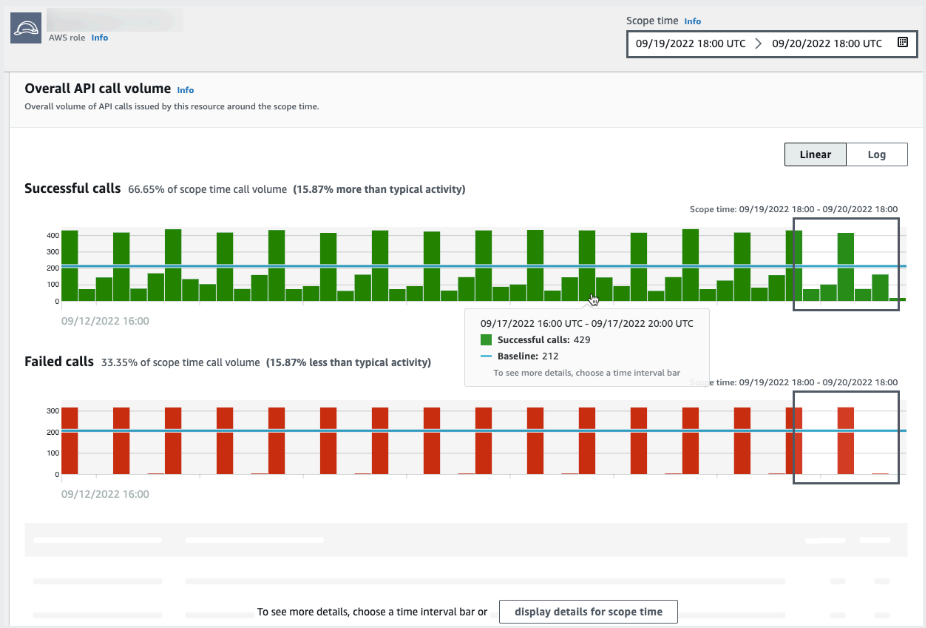
I pannelli di profilo in genere forniscono i seguenti tipi di dati.

Tipo di dati del pannello	Descrizione
Informazioni di alto livello su un risultato o un'entità	Il tipo di pannello più semplice fornisce alcune informazioni di base su un'entità. Esempi di informazioni incluse in un pannello includono l'identificatore, il nome, il tipo e la data di creazione.

<table>
<tr><th>Tipo di dati del pannello</th><th>Descrizione</th></tr>
<tr><td></td><td>


La maggior parte dei profili di entità contiene un pannello informativo per tale entità.
</td></tr>
<tr><td>Riepilogo generale dell'attività nel tempo</td><td>
Visualizza un riepilogo dell'attività di un'entità nel tempo.

Questo tipo di pannello offre una visione generale del comportamento di un'entità durante il periodo di validità.

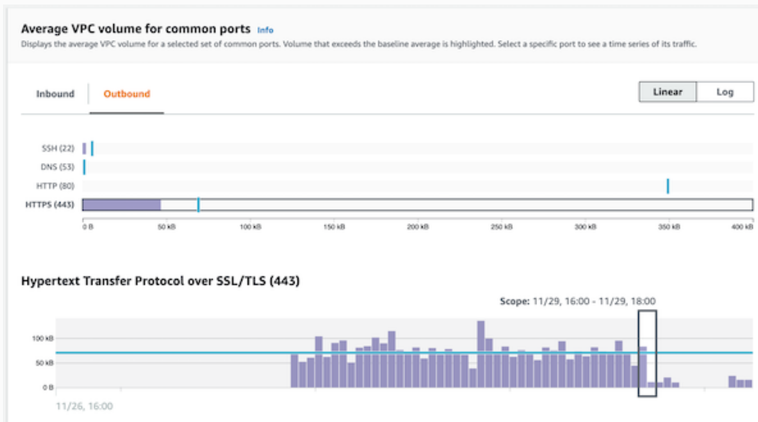


Di seguito sono elencati alcuni esempi di dati di riepilogo forniti nei pannelli di profilo di Detective:

- APIChiamate fallite e riuscite
- Volume in entrata e in uscita VPC
</td></tr>
</table>

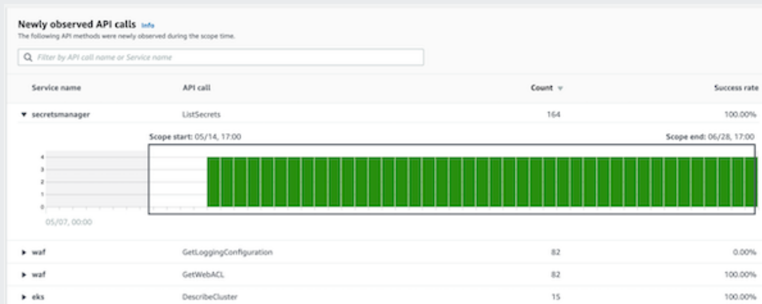
<table>
<tr><th>Tipo di dati del pannello</th><th>Descrizione</th></tr>
<tr><td>Riepilogo delle attività raggruppate per valori</td><td>Visualizza un riepilogo delle attività di un'entità, raggruppate in base a valori specifici.

Ad esempio, puoi vedere questo tipo di pannello del profilo sul profilo. EC2 Il pannello del profilo mostra il volume medio di dati del registro di VPC flusso da e verso un'EC2istanza per le porte comuni associate a tipi specifici di servizi.


</td></tr>
</table>

<table>
<tr><th>Tipo di dati del pannello</th><th>Descrizione</th></tr>
<tr><td>Attività iniziata solo durante il periodo di validità</td><td>
Durante un'indagine, è utile vedere quali attività hanno iniziato a verificarsi solo in un determinato periodo di tempo.

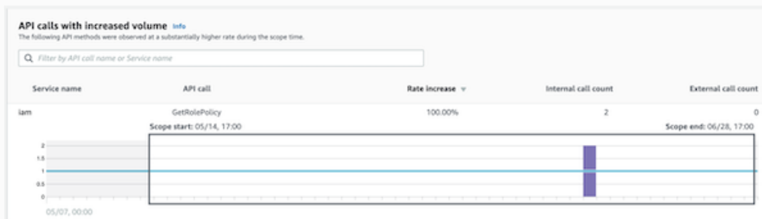
Ad esempio, ci sono API chiamate, località geografiche o user agent mai visti prima?



Se il grafico di comportamento è ancora in modalità di addestramento, il pannello del profilo visualizza un messaggio di notifica. Il messaggio viene rimosso quando il grafico di comportamento ha accumulato almeno due settimane di dati. Per ulteriori informazioni sulla modalità di addestramento, consulta the section called “Periodo di addestramento per nuovi grafici di comportamento”.
</td></tr>
</table>

<table>
<tr><th>Tipo di dati del pannello</th><th>Descrizione</th></tr>
<tr><td>Attività che è cambiata in modo significativo durante il periodo di validità</td><td>Analogamente ai nuovi pannelli di attività, i pannelli di profilo possono anche visualizzare le attività che sono cambiate in modo significativo durante il periodo di validità.

Ad esempio, un utente potrebbe effettuare regolarmente una determinata API chiamata alcune volte alla settimana. Se lo stesso utente invia improvvisamente la stessa chiamata più volte in un solo giorno, ciò potrebbe essere una prova di attività dannosa.



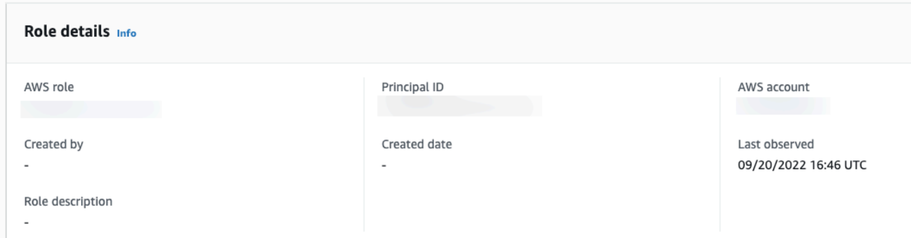
Se il grafico di comportamento è ancora in modalità di addestramento, il pannello del profilo visualizza un messaggio di notifica. Il messaggio viene rimosso quando il grafico di comportamento ha accumulato almeno due settimane di dati. Per ulteriori informazioni sulla modalità di addestramento, consulta the section called “Periodo di addestramento per nuovi grafici di comportamento”.</td></tr>
</table>

Tipi di visualizzazioni del pannello di profilo

Il contenuto del pannello di profilo può assumere una delle seguenti forme.

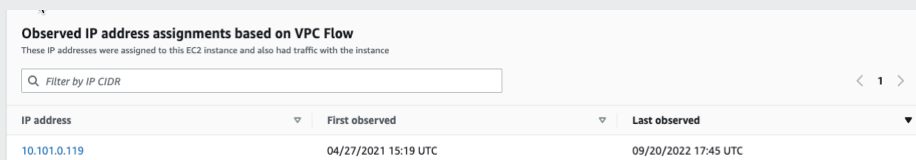
<table>
<tr><th>Tipo di visualizzazione</th><th>Descrizione</th></tr>
<tr><td>Coppie chiave/valore</td><td>Il tipo di visualizzazione più semplice è un set di coppie chiave-valore.

Un pannello di informazioni su risultati o entità è l'esempio più comune di pannello di coppie chiave-valore.</td></tr>
</table>

<table>
<tr><th>Tipo di visualizzazione</th><th>Descrizione</th></tr>
<tr><td></td><td>


Le coppie chiave-valore possono essere utilizzate anche per aggiungere altre informazioni ad altri tipi di pannelli.

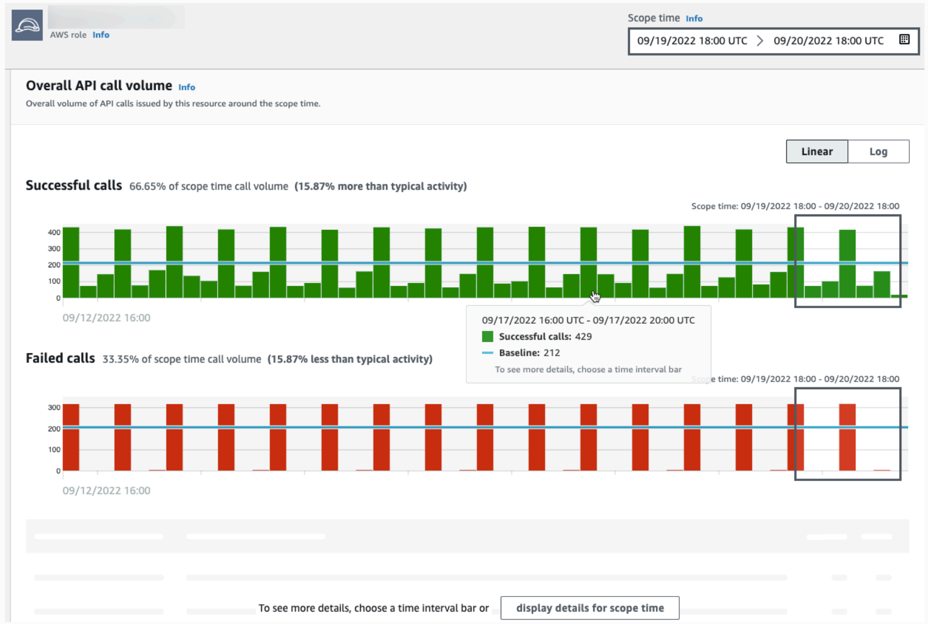
Da un pannello di coppie chiave-valore, se un valore è un identificatore di un'entità, è possibile passare al suo profilo.
</td></tr>
<tr><td>Tabella</td><td>
Una tabella è un semplice elenco di elementi composto da più colonne.



È possibile ordinare, filtrare e sfogliare la tabella.

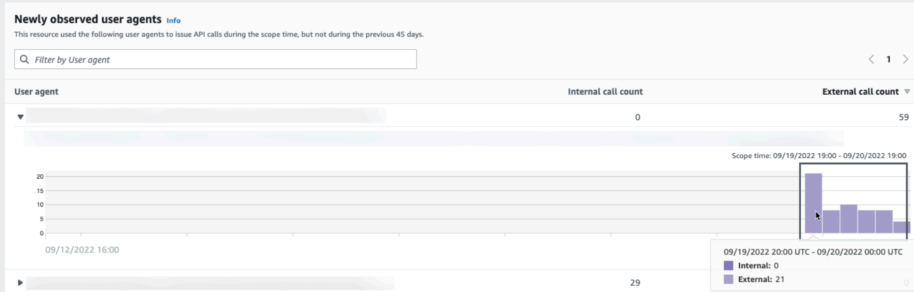
È possibile modificare il numero di voci da visualizzare su ogni pagina. Per informazioni, consulta the section called “Preferenze per i pannelli di profilo”.

Se un valore nella tabella è un identificatore di un'entità, è possibile passare al suo profilo.
</td></tr>
</table>

Tipo di visualizzazione	Descrizione
Sequenza temporale	Una visualizzazione della sequenza temporale mostra un valore aggregato per intervalli definiti nel tempo.  La sequenza temporale evidenzia il periodo di validità corrente e include il tempo periferico aggiuntivo prima e dopo il periodo di validità. L'ora periferica fornisce il contesto per l'attività nel periodo di validità. Passa il mouse su un intervallo di tempo per visualizzare un riepilogo dei dati relativi a quell'intervallo di tempo.

<table>
<tr><th>Tipo di visualizzazione</th><th>Descrizione</th></tr>
<tr><td>Tabella espandibile</td><td>

Una tabella espandibile combina tabelle e sequenze temporali.



La visualizzazione inizia come una tabella.

È possibile ordinare, filtrare e sfogliare la tabella.

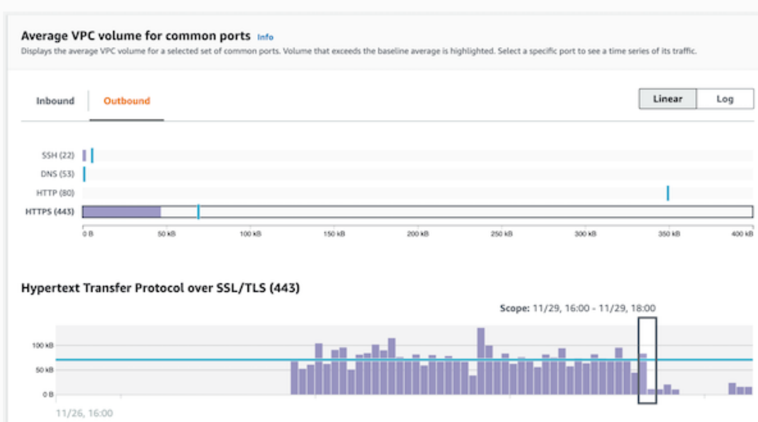
È possibile modificare il numero di voci da visualizzare su ogni pagina. Per informazioni, consulta the section called “Preferenze per i pannelli di profilo”.

È quindi possibile espandere ogni riga per mostrare una visualizzazione della sequenza temporale specifica per quella riga.

</td></tr>
<tr><td>Grafico a barre</td><td>

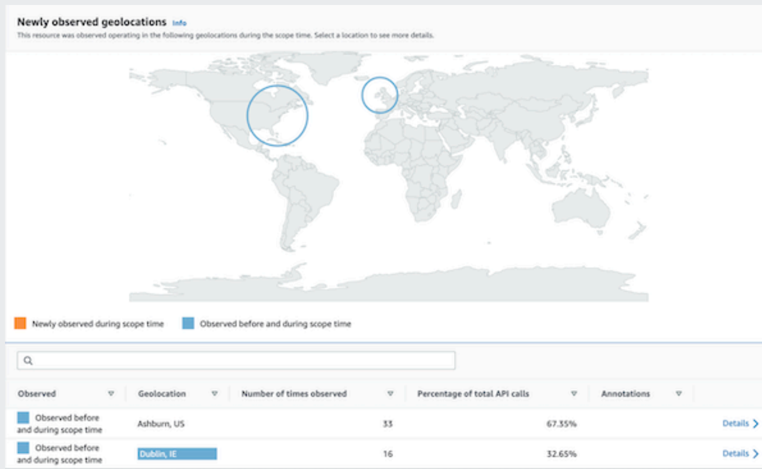
Un grafico a barre mostra i valori in base ai raggruppamenti.

A seconda del grafico, potresti essere in grado di scegliere una barra per visualizzare una sequenza temporale dell'attività correlata.



</td></tr>
</table>

<table>
<tr><th>Tipo di visualizzazione</th><th>Descrizione</th></tr>
<tr><td>Grafico di geolocalizzazione</td><td>Un grafico di geolocalizzazione mostra una mappa contrassegnata per evidenziare i dati in base alla posizione geografica. Può essere seguito da una tabella contenente dettagli sulle singole geolocalizzazioni.



Tieni presente che durante l'elaborazione dei dati geografici in entrata, Detective arrotonda i valori di latitudine e longitudine a un singolo punto decimale.</td></tr>
</table>

Note sul contenuto del pannello del profilo

Quando si visualizza il contenuto di un pannello di profilo, considera i seguenti elementi:

Avviso sui dati di conteggio approssimativo

Questo avviso indica che gli elementi con conteggi estremamente bassi non vengono visualizzati a causa del volume di dati applicabili.

Per garantire un conteggio completamente accurato, riduci la quantità di dati. Il modo più semplice per farlo è ridurre la durata del periodo di validità. Per informazioni, consulta the section called “Gestione del periodo di validità”.

Arrotondamento per località geografiche

Detective arrotonda tutti i valori di latitudine e longitudine a un solo punto decimale.

Modifiche al modo in cui Detective rappresenta API le chiamate

A partire dal 14 luglio 2021, Detective tiene traccia del servizio che ha effettuato ogni API chiamata. Ogni volta che Detective mostra un API metodo, mostra anche il servizio associato. Nei pannelli dei profili che visualizzano informazioni sulle API chiamate, le chiamate vengono sempre raggruppate in base al servizio. Per i dati che Detective ha importato prima di tale data, il nome del servizio è indicato come Servizio sconosciuto.

Inoltre, a partire dal 14 luglio 2021, per gli account e i ruoli, i dettagli dell'attività nel pannello del profilo del volume complessivo AKID delle API chiamate non mostrano più la risorsa che ha emesso la chiamata. Per gli account, Detective visualizza l'identificatore del principale (utente o ruolo) che ha emesso la chiamata. Per i ruoli, Detective visualizza l'identificatore della sessione dei ruoli. Per i dati che Detective ha importato prima del 14 luglio 2021, l'identificatore è elencato come Risorsa sconosciuta.

Per i pannelli di profilo che visualizzano un elenco di API chiamate, la timeline associata evidenzia il periodo di tempo durante il quale si è verificata questa transizione. L'evento clou inizia il 14 luglio 2021 e termina quando l'aggiornamento si è completamente propagato in Detective.

Impostazione delle preferenze per un pannello di profilo

Per i pannelli di profilo, puoi personalizzare il numero di righe che appaiono su ogni pagina nei pannelli di profilo e configurare la preferenza del formato del timestamp.

Impostazione della lunghezza della tabella

Per i pannelli di profilo che contengono tabelle o tabelle espandibili, è possibile configurare il numero di righe da visualizzare su ogni pagina.

Imposta la tua preferenza per il numero di voci su ogni pagina.

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Preferenze.
3. Nella pagina Preferenze, in Lunghezza tabella, fai clic su Modifica.
4. Scegli il numero di righe della tabella che desideri visualizzare su ogni pagina.
5. Seleziona Salva.

Impostazione del formato del timestamp

Per i pannelli del profilo, puoi configurare la preferenza del formato timestamp che verrà applicata a tutti i timestamp per ogni IAM utente o ruolo IAM in Detective.

> **Note**
>
> La preferenza per il formato del timestamp non viene applicata all'intero account. AWS

Imposta la preferenza per il timestamp.

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Preferenze.
3. Nella pagina Preferenze, in Preferenze timestamp, visualizza e modifica la visualizzazione preferita per tutti i timestamp.
4. Per impostazione predefinita, il formato del timestamp è impostato su. UTC Fai clic su Modifica per scegliere il fuso orario locale.

   Esempio:

   Example

   UTC- 20/09/22 16:39 UTC

   Locale - 20/09/2022 09:39 (- 07:00) UTC
5. Seleziona Salva.

Navigazione diretta a un profilo di entità o alla panoramica di risultati

Per passare direttamente al profilo di un'entità o a una panoramica dei risultati in Amazon Detective, puoi utilizzare una delle opzioni riportate di seguito.

- Da Amazon GuardDuty or AWS Security Hub, puoi passare da una GuardDuty scoperta al corrispondente profilo di ricerca del Detective.

- È possibile creare un URL di Detective che identifichi un risultato o un'entità e stabilisca il periodo di validità da utilizzare.

Passare a un profilo di entità o cercare una panoramica su Amazon oppure GuardDuty AWS Security Hub

Dalla GuardDuty console Amazon, puoi accedere al profilo di entità di un'entità correlata a un risultato.

Dalle AWS Security Hub console GuardDuty e, puoi anche accedere a una panoramica dei risultati. Ciò fornisce anche collegamenti ai profili di entità per le entità coinvolte.

Questi collegamenti possono contribuire a semplificare il processo di indagine. Puoi usare rapidamente Detective per vedere l'attività dell'entità associata e determinare i passaggi successivi. Puoi quindi archiviare un risultato se si tratta di un falso positivo o approfondire per determinare la portata del problema.

Come passare alla console Amazon Detective

I link alle indagini sono disponibili per tutti i GuardDuty risultati. GuardDuty consente inoltre di scegliere se accedere al profilo di un'entità o alla panoramica dei risultati.

Passare a Detective dalla console GuardDuty

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Se necessario, scegli Risultati nel riquadro di navigazione a sinistra.
3. Nella pagina GuardDuty Risultati, scegli il risultato.

   Il riquadro dei dettagli del risultato viene visualizzato sulla destra dell'elenco dei risultati.
4. Nel riquadro dei dettagli dei risultati, scegli Analisi in Detective.

   GuardDuty mostra un elenco di oggetti disponibili su cui indagare in Detective.

   L'elenco contiene sia le entità correlate, come gli indirizzi IP o le istanze EC2, sia i risultati.
5. Scegli un'entità o il risultato.

   La console di Detective si apre in una nuova scheda. La console si apre sul profilo dell'entità o del risultato.

Se non hai abilitato Detective, la console si apre su una pagina di destinazione che fornisce una panoramica di Detective. Da lì, puoi scegliere di abilitare Detective.

Passare a Detective dalla console Centrale di sicurezza

1. Apri la AWS Security Hub console all'indirizzo https://console.aws.amazon.com/securityhub/.
2. Se necessario, scegli Risultati nel riquadro di navigazione a sinistra.
3. Nella pagina Security Hub Findings, scegli un GuardDuty risultato.
4. Nel riquadro dei dettagli, scegli Indaga in Detective, quindi scegli Analizza il risultato.

   Quando scegli Analizza il risultato, la console Detective si apre in una nuova scheda. La console si apre con la panoramica dei risultati.

   La console di Detective mostra sempre la Regione da cui proviene il risultato, anche se si passa dalla Regione di aggregazione. Per ulteriori informazioni sull'aggregazione dei risultati, consulta Aggregazione dei risultati tra le Regioni nella Guida per l'utente di AWS Security Hub .

   Se non hai abilitato Detective, la console si apre sulla pagina iniziale di Detective. Da lì, puoi abilitare Detective.

Risoluzione dei problemi relativi al pivot

Per usare il pivot, deve essere vera una delle seguenti condizioni:

- Il tuo account deve essere un account amministratore sia per Detective che per il servizio da cui stai provenendo.
- Hai assunto un ruolo tra account che consente all'account amministratore di accedere al grafico di comportamento.

Per ulteriori informazioni sulla raccomandazione di allineare gli account degli amministratori, consulta Allineamento consigliato con Amazon e. GuardDuty AWS Security Hub

Se il passaggio non funziona, controlla quanto segue.

- Il risultato appartiene a un account membro abilitato nel tuo grafico di comportamento? Se l'account associato non è stato invitato al grafico di comportamento come account membro, il grafico non conterrà dati relativi a quell'account.

Se un account membro invitato non ha accettato l'invito, il grafico di comportamento non conterrà dati relativi a quell'account.

- Il risultato è archiviato? Il Detective non riceve i risultati archiviati da GuardDuty.
- Il risultato si è verificato prima che Detective iniziasse a importare dati nel tuo grafico di comportamento? Se il risultato non è presente nei dati importati da Detective, il grafico di comportamento non conterrà dati relativi.
- Il risultato proviene dalla Regione corretta? Ogni grafico di comportamento è specifico per una Regione. Un grafico di comportamento non contiene dati provenienti da altre Regioni.

Navigazione a un profilo di entità o alla panoramica di risultati tramite un URL

Per passare al profilo di un'entità o a una panoramica dei risultati in Amazon Detective, puoi utilizzare un URL che fornisce un collegamento diretto. L'URL identifica il risultato o l'entità. Può anche specificare il periodo di validità da utilizzare sul profilo. Detective conserva fino a un anno di dati storici sugli eventi.

Formato dell'URL di un profilo

> **Note**
>
> Se utilizzi il vecchio formato URL, Detective ti reindirizzerà automaticamente al nuovo URL. Il vecchio formato dell'URL era: https://console.aws.amazon.com/detective/home?region=*Region*#*type*/*namespace*/*instanceID*?*parameters*

Il nuovo formato dell'URL del profilo è il seguente:

- Per le entità: https://console.aws.amazon.com/detective/home?region=*Region*#*entities*/*namespace*/*instanceID*?*parameters*
- Per i risultati: https://console.aws.amazon.com/detective/home?region=*Region*#*findings*/*instanceID*?*parameters*

L'URL richiede i seguenti valori.

Region

La Regione che desideri utilizzare.

tipo

Il tipo di elemento per il profilo verso cui stai navigando.

- `entities`: indica che stai navigando verso un profilo di entità
- `findings`: indica che stai navigando verso una panoramica dei risultati

spazio dei nomi

Per le entità, lo spazio dei nomi è il nome del tipo di entità.

- `AwsAccount`
- `AwsRole`
- `AwsRoleSession`
- `AwsUser`
- `Ec2Instance`
- `FederatedUser`
- `IpAddress`
- `S3Bucket`
- `UserAgent`
- `FindingGroup`
- `KubernetesSubject`
- `ContainerPod`
- `ContainerCluster`
- `ContainerImage`

instanceID

L'identificatore di istanza del risultato o dell'entità.

- Per un GuardDuty risultato, l'identificatore del GuardDuty ritrovamento.
- Per un AWS account, l'ID dell'account.
- Per AWS ruoli e utenti, l'ID principale del ruolo o dell'utente.
- Per gli utenti federati, l'ID principale dell'utente federato. L'ID principale è *<identityProvider>*:*<username>* o *<identityProvider>*:*<audience>*:*<username>*.

- Per gli indirizzi IP, l'indirizzo IP.
- Per gli agenti utente, il nome dell'agente utente.
- Per istanze EC2, l'ID dell'istanza.
- Per le sessioni di ruolo, l'identificatore di sessione. L'identificatore della sessione utilizza il formato `<rolePrincipalID>:<sessionName>`.
- Per i bucket S3, il nome del bucket.
- Per un UUID FindingGroups, ad esempio `ca6104bc-a315-4b15-bf88-1c1e60998f83`
- Per le risorse EKS, utilizza i seguenti formati:
  - Cluster EKS: `<clusterName>~<accountId>~EKS`
  - `Pod Kubernetes: ~ ~EKS` <podUid><clusterName><accountId>
  - Soggetto Kubernetes: `<subjectName>~<clusterName>~<accountId>`
  - Immagine di container: `<registry>/<repository>:<tag>@<digest>`

Il risultato o l'entità devono essere associati a un account abilitato nel grafico di comportamento.

L'URL può includere anche i seguenti parametri opzionali, che vengono utilizzati per impostare il periodo di validità. Per ulteriori informazioni sul periodo di validità e su come viene utilizzato con i profili, consulta the section called “Gestione del periodo di validità”.

`scopeStart`

L'ora di inizio del periodo di validità da utilizzare sul profilo. L'ora di inizio deve essere compresa negli ultimi 365 giorni.

Il valore è il timestamp epoch.

Se si fornisce un'ora di inizio ma non un'ora di fine, il periodo di validità termina all'ora corrente.

`scopeEnd`

L'ora di fine del periodo di validità da utilizzare sul profilo.

Il valore è il timestamp epoch.

Se si fornisce un'ora di fine, ma non un'ora di inizio, il periodo di validità include tutto il periodo di tempo prima dell'ora di fine.

Se non si specifica il periodo di validità, viene utilizzato il periodo di validità predefinito.

- Per i risultati, il periodo di validità predefinito utilizza la prima e l'ultima volta in cui l'attività del risultato è stata osservata.
- Per le entità, il periodo di validità predefinito è pari alle 24 ore precedenti.

Di seguito puoi trovare un esempio di URL di Detective:

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

Questo URL di esempio fornisce le istruzioni riportate di seguito.

- Visualizza il profilo dell'entità per l'indirizzo IP 192.168.1.
- Utilizza un periodo di validità che inizia lunedì 18 marzo 2019 12:00:00 GMT e termina lunedì 18 marzo 2019 12:00:00 GMT.

Risoluzione dei problemi relativi a un URL

Se l'URL non mostra il profilo previsto, verifica innanzitutto che l'URL utilizzi il formato corretto e di aver fornito i valori corretti.

- Hai iniziato con l'URL corretto (`findings` o `entities`)?
- Hai specificato lo spazio dei nomi corretto?
- Hai fornito l'identificatore corretto?

Se i valori sono corretti, puoi anche controllare quanto segue.

- Il risultato o l'entità appartengono a un account membro abilitato nel tuo grafico di comportamento? Se l'account associato non è stato invitato al grafico di comportamento come account membro, il grafico non conterrà dati relativi a quell'account.

  Se un account membro invitato non ha accettato l'invito, il grafico di comportamento non conterrà dati relativi a quell'account.
- Un risultato viene archiviato? Detective non riceve i risultati archiviati da Amazon GuardDuty.
- Il risultato o l'entità si sono verificati prima che Detective iniziasse a importare dati nel tuo grafico di comportamento? Se il reperto o l'entità non è presente nei dati che il Detective inserisce, il grafico di comportamento non contiene i relativi dati.

- Il risultato o l'entità provengono dalla Regione corretta? Ogni grafico di comportamento è specifico per una Regione. Un grafico di comportamento non contiene dati provenienti da altre Regioni.

Aggiunta di URL di Detective per i risultati a Splunk

Il progetto Splunk Trumpet consente di inviare dati dai servizi a Splunk. AWS

Puoi configurare il progetto Trumpet per generare URL Detective per i risultati di Amazon. GuardDuty Puoi quindi utilizzare questi URL per passare direttamente da Splunk ai corrispondenti profili di risultati di Detective.

Il progetto Trumpet è disponibile all'indirizzo https://github.com/splunk/. GitHub splunk-aws-project-trumpet

Nella pagina di configurazione del progetto Trumpet, da AWS CloudWatch Eventi, scegli Detective GuardDuty URLs.

Passaggio da un pannello di profilo a un'altra console

Per EC2 istanze, IAM utenti e IAM ruoli, puoi passare direttamente dal pannello del profilo dei dettagli alla console corrispondente. Le informazioni disponibili dalla console possono fornire un input aggiuntivo per le indagini di sicurezza.

Nel pannello del EC2 profilo dei dettagli dell'EC2istanza, l'identificatore dell'istanza è collegato alla EC2 console Amazon.

Nel pannello del profilo dei dettagli utente, il nome utente è collegato alla IAM console.

Nel pannello del profilo con i dettagli del ruolo, il nome del ruolo è collegato alla IAM console.

Passaggio da un pannello di profilo a un altro profilo di entità

Quando un pannello di profilo contiene un identificatore di un'entità diversa, in genere si tratta di un collegamento a quel profilo di entità. Le eccezioni sono i collegamenti ad Amazon EC2 e alle IAM console nei profili di EC2 istanza, IAM utenti e IAM ruoli. Per informazioni, consulta the section called “Passaggio a un'altra console”.

Ad esempio, da un elenco di indirizzi IP, potresti essere in grado di visualizzare il profilo per un indirizzo IP specifico. In questo modo puoi vedere se sono disponibili altre informazioni che possono aiutarti a completare l'indagine.

Esplorazione dei dettagli dell'attività su un pannello del profilo

Durante un'indagine, potresti voler approfondire il modello di attività di un'entità.

Nei seguenti pannelli del profilo, puoi visualizzare un riepilogo dei dettagli dell'attività:

- Volume complessivo delle API chiamate, ad eccezione del pannello del profilo utente-agente
- Geolocalizzazioni appena osservate
- Volume VPC di flusso complessivo
- VPCvolume di flusso da e verso l'indirizzo IP di ricerca, per i risultati associati a un singolo indirizzo IP
- Dettagli container
- VPCvolume di flusso per i cluster
- Attività complessiva di Kubernetes API

I dettagli dell'attività possono rispondere a questi tipi di domande:

- Quali indirizzi IP sono stati utilizzati?
- Dove si trovavano quegli indirizzi IP?
- Quali API chiamate ha effettuato ciascun indirizzo IP e da quali servizi le ha effettuate?
- Quali principali o identificatori delle chiavi di accesso (AKIDs) sono stati utilizzati per effettuare le chiamate?
- Quali risorse sono state utilizzate per effettuare quelle chiamate?
- Quante chiamate sono state effettuate? Quante hanno avuto successo e quante hanno fallito?
- Quale volume di dati del registro di VPC flusso è stato inviato da o verso ciascun indirizzo IP?
- Quali contenitori erano attivi per un determinato cluster, immagine o pod?

Argomenti

- Dettagli sull'attività per il volume complessivo delle API chiamate
- Dettagli dell'attività per una geolocalizzazione
- Dettagli dell'attività per il volume complessivo del VPC flusso
- Attività complessiva di Kubernetes API che coinvolge il cluster EKS

Dettagli sull'attività per il volume complessivo delle API chiamate

I dettagli dell'attività per Volume complessivo delle API chiamate mostrano le API chiamate emesse in un intervallo di tempo selezionato.

Per visualizzare i dettagli dell'attività per un singolo intervallo di tempo, scegli l'intervallo di tempo sul grafico.

Per visualizzare i dettagli dell'attività per il periodo di validità corrente, scegli Visualizza dettagli per il periodo di validità.

Tieni presente che Detective ha iniziato a memorizzare e visualizzare il nome del servizio per API le chiamate a partire dal 14 luglio 2021. Tale data è evidenziata nella sequenza temporale del pannello del profilo. Per le attività che si verificano prima di tale data, il nome del servizio è Servizio sconosciuto.

Contenuto dei dettagli dell'attività (utenti, ruoli, account, sessioni di ruolo, EC2 istanze, bucket S3)

Per IAM utenti, IAM ruoli, account, sessioni di ruolo, EC2 istanze e bucket S3, i dettagli dell'attività contengono le seguenti informazioni:

- Ogni scheda fornisce informazioni sul set di API chiamate emesse durante l'intervallo di tempo selezionato.

  Per i bucket S3, le informazioni riflettono API le chiamate effettuate al bucket S3.

  Le API chiamate sono raggruppate in base ai servizi che le hanno chiamate. Per i bucket S3, il servizio è sempre Amazon S3. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.
- Per ogni immissione, i dettagli dell'attività mostrano il numero di chiamate riuscite e non riuscite. La scheda Indirizzi IP osservati mostra anche la posizione di ogni indirizzo IP.
- Ogni voce mostra informazioni su chi ha effettuato le chiamate. Per gli account, i dettagli dell'attività identificano gli utenti o i ruoli. Per i ruoli, i dettagli dell'attività identificano le sessioni di ruolo. Per gli utenti e le sessioni di ruolo, i dettagli dell'attività identificano gli identificatori delle chiavi di accesso ()AKIDs.

  Tieni presente che a partire dal 14 luglio 2021, per i profili degli account, i dettagli dell'attività mostrano gli utenti o i ruoli anzichéAKIDs. Per i profili di ruolo, i dettagli dell'attività mostrano le sessioni di ruolo anzichéAKIDs. Per le attività che si sono svolte prima del 14 luglio 2021, il chiamante viene elencato come Risorsa sconosciuta.

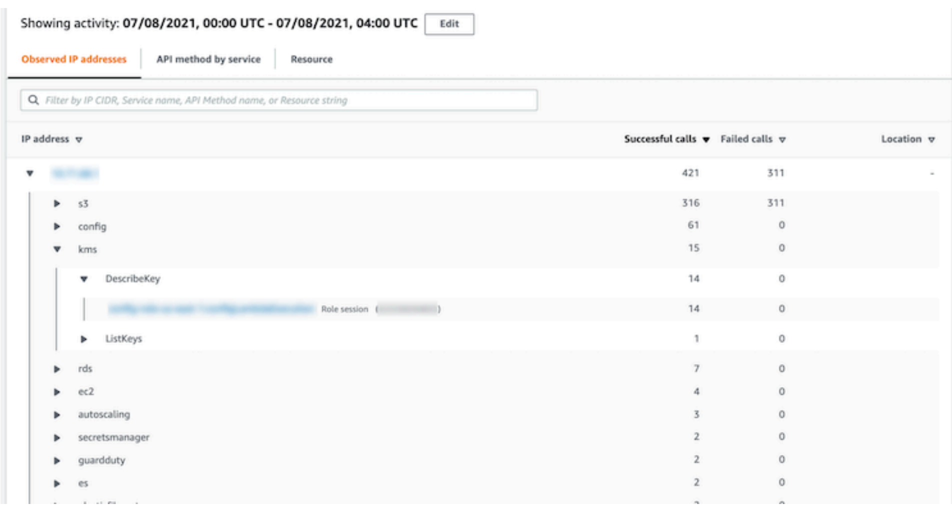
I dettagli dell'attività contengono le seguenti schede:

Indirizzi IP osservati

Visualizza inizialmente l'elenco degli indirizzi IP utilizzati per effettuare API chiamate.

È possibile espandere ogni indirizzo IP per visualizzare l'elenco delle API chiamate emesse da tale indirizzo IP. Le API chiamate sono raggruppate in base ai servizi che le hanno chiamate. Per i bucket S3, il servizio è sempre Amazon S3. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.

È quindi possibile espandere ogni API chiamata per visualizzare l'elenco dei chiamanti provenienti da quell'indirizzo IP. A seconda del profilo, il chiamante potrebbe essere un utente, un ruolo, una sessione di ruolo o. AKID

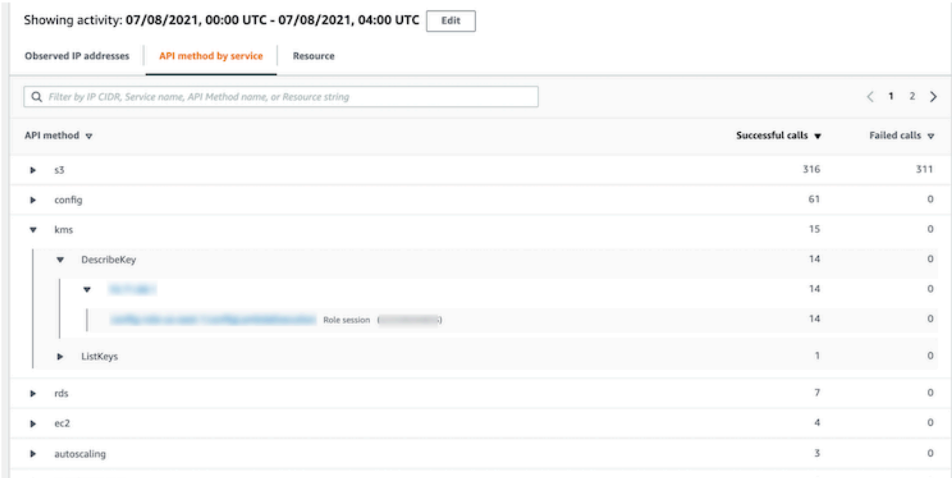


APImetodo per servizio

Visualizza inizialmente l'elenco delle API chiamate emesse. Le API chiamate sono raggruppate in base ai servizi che le hanno emesse. Per i bucket S3, il servizio è sempre Amazon S3. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.

È possibile espandere ciascun API metodo per visualizzare l'elenco degli indirizzi IP da cui sono state emesse le chiamate.

È quindi possibile espandere ogni indirizzo IP per visualizzare l'elenco delle AKIDs API chiamate emesse da quell'indirizzo IP.

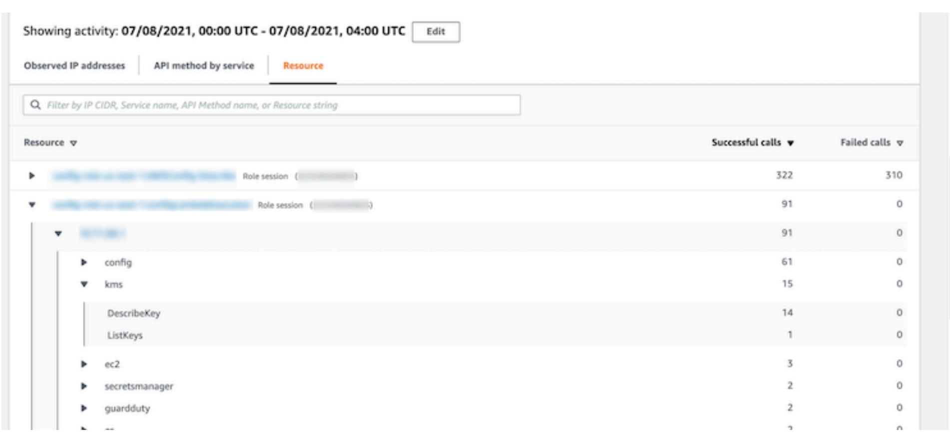


ID della risorsa o della chiave di accesso

Visualizza inizialmente l'elenco di utenti, ruoli, sessioni di ruolo o AKIDs che sono stati utilizzati per effettuare API chiamate.

È possibile espandere ogni chiamante per visualizzare l'elenco degli indirizzi IP da cui ha API emesso le chiamate.

È quindi possibile espandere ogni indirizzo IP per visualizzare l'elenco delle API chiamate emesse da quell'indirizzo IP da quel chiamante. Le API chiamate vengono raggruppate in base ai servizi che le hanno emesse. Per i bucket S3, il servizio è sempre Amazon S3. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.



Contenuto dei dettagli dell'attività (indirizzi IP)

Per gli indirizzi IP, i dettagli dell'attività contengono le seguenti informazioni:

- Ogni scheda fornisce informazioni sull'insieme di API chiamate emesse nell'intervallo di tempo selezionato. Le API chiamate sono raggruppate in base ai servizi che le hanno emesse. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.
- Per ogni immissione, i dettagli dell'attività mostrano il numero di chiamate riuscite e non riuscite.

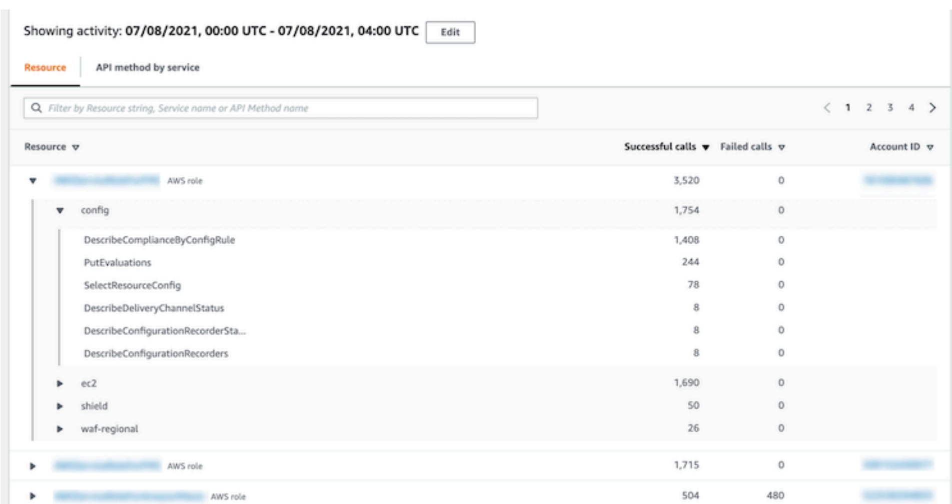
I dettagli dell'attività contengono le seguenti schede:

Risorsa

Visualizza inizialmente l'elenco delle risorse che hanno emesso API chiamate dall'indirizzo IP.

Per ogni risorsa, l'elenco include il nome della risorsa, il tipo e l'account AWS .

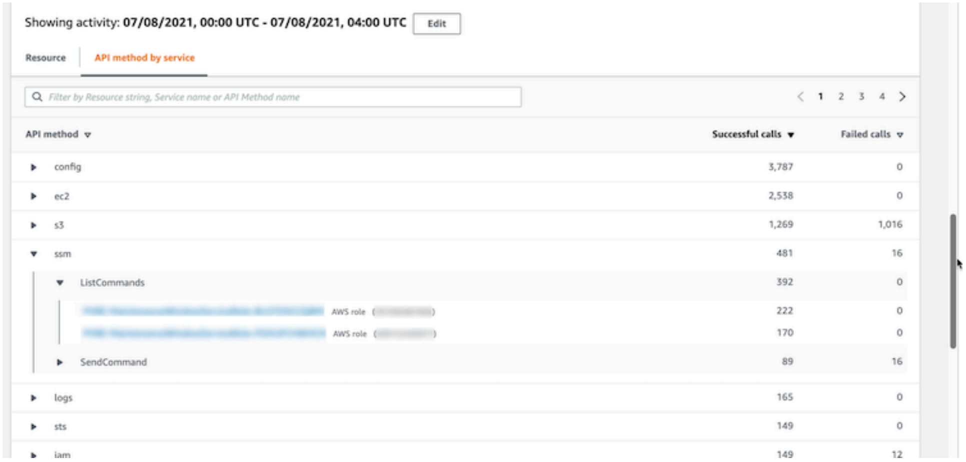
È possibile espandere ogni risorsa per visualizzare l'elenco delle API chiamate emesse dalla risorsa dall'indirizzo IP. Le API chiamate sono raggruppate in base ai servizi che le hanno emesse. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.



APImetodo per servizio

Visualizza inizialmente l'elenco delle API chiamate emesse. Le API chiamate sono raggruppate in base ai servizi che le hanno emesse. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.

È possibile espandere ogni API chiamata per visualizzare l'elenco delle risorse che hanno emesso la API chiamata dall'indirizzo IP durante il periodo di tempo selezionato.



Ordinamento dei dettagli dell'attività

Puoi ordinare i dettagli dell'attività in base a una qualsiasi delle colonne dell'elenco.

Quando si ordina utilizzando la prima colonna, viene ordinato solo l'elenco di primo livello. Gli elenchi di livello inferiore sono sempre ordinati in base al numero di chiamate riuscite. API

Filtro dei dettagli dell'attività

È possibile utilizzare le opzioni di filtro per concentrarsi su sottoinsiemi o aspetti specifici dell'attività rappresentata nei dettagli dell'attività.

In tutte le schede, puoi filtrare l'elenco in base a uno qualsiasi dei valori nella prima colonna.

Aggiungere un filtro

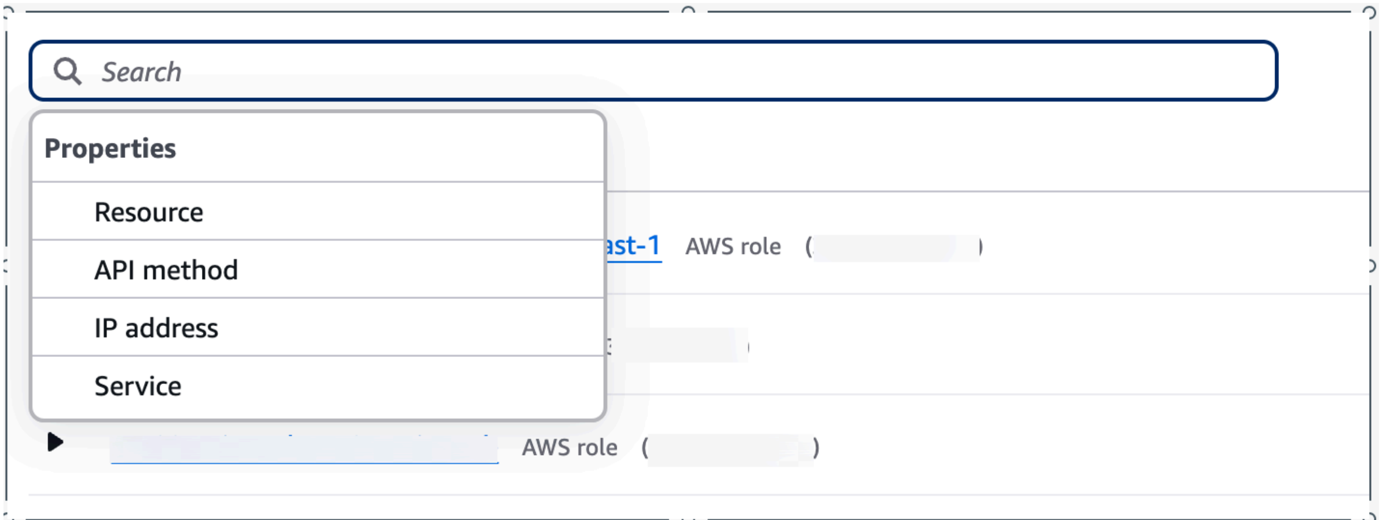
1. Scegli la casella di filtro.
2. In Proprietà, scegli la proprietà da utilizzare per il filtraggio.
3. Fornisci il valore da utilizzare per il filtraggio. Il filtro supporta valori parziali. Ad esempio, quando si filtra per API metodo, se si filtra per**`Instance`**, i risultati includono qualsiasi API operazione contenuta `Instance` nel nome. Quindi sia `ListInstanceAssociations` che `UpdateInstanceInformation` corrisponderebbero.

   Per i nomi di servizio, API i metodi e gli indirizzi IP, è possibile specificare un valore o scegliere un filtro integrato.

Per APISottostringhe comuni, scegliete la sottostringa che rappresenta il tipo di operazione, ad esempio`List`, `Create` o. `Delete` Ogni nome API di metodo inizia con il tipo di operazione.

Per CIDRquanto riguarda i modelli, è possibile scegliere di includere solo indirizzi IP pubblici, indirizzi IP privati o indirizzi IP che corrispondono a uno CIDR schema specifico.

4. Scegliete un'opzione booleana ***`Resource`*** oppure ***`Service`***: Contiene o! : Non contiene; o o ***`IP address`*** = Uguale a ***`API method`*** o! : non equivale a impostare filtri.



Per rimuovere un filtro, scegli l'icona x nell'angolo in alto a destra.

Per cancellare tutti i filtri, scegli Cancella filtro.

Selezione dell'intervallo di tempo per i dettagli dell'attività

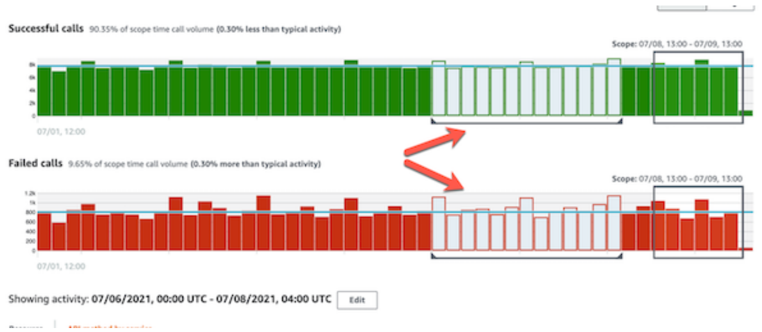
Quando si visualizzano per la prima volta i dettagli dell'attività, l'intervallo di tempo corrisponde al periodo di validità o a un intervallo di tempo selezionato. È possibile modificare l'intervallo di tempo per i dettagli dell'attività.

Modificare l'intervallo di tempo per i dettagli dell'attività

1. Scegli Modifica.
2. In Modifica finestra temporale, scegli l'ora di inizio e di fine da utilizzare.

   Per impostare la finestra temporale sul periodo di validità predefinito per il profilo, scegli Imposta il periodo di validità predefinito.
3. Scegli la Finestra temporale di aggiornamento.

L'intervallo di tempo per i dettagli dell'attività è evidenziato nei grafici del pannello del profilo.



Esecuzione di query sui log non elaborati

Amazon Detective è ora integrato con Security Lake, il che significa che puoi interrogare e recuperare i dati dei log non elaborati archiviati da Security Lake. Per ulteriori dettagli su questa integrazione, consulta Integrazione tra Detective e Security Lake.

Grazie a questa integrazione, puoi raccogliere ed eseguire query su log ed eventi dalle seguenti origini supportate in modo nativo da Security Lake.

- AWS CloudTrail gestione degli eventi versione 1.0 e successive
- Amazon Virtual Private Cloud (AmazonVPC) Flow Logs versione 1.0 e successive
- Log di controllo di Amazon Elastic Kubernetes Service (EKSAmazon) versione 2.0

> **Note**
>
> Non sono previsti costi supplementari per l'interrogazione dei log di dati non elaborati in Detective. I costi di utilizzo per altri AWS Servizi, incluso Amazon Athena, si applicano ancora alle tariffe pubblicate.

Interrogare i log non elaborati

1. Scegli i dettagli di visualizzazione per il periodo di validità.
2. Da qui, puoi iniziare a interrogare i log non elaborati.
3. Nella tabella di anteprima dei log non elaborati, è possibile visualizzare i log e gli eventi recuperati interrogando i dati da Security Lake. Per maggiori dettagli sui log degli eventi non elaborati, puoi visualizzare i dati visualizzati in Amazon Athena.

Dalla tabella Interroga log non elaborati, puoi annullare la richiesta di query, visualizzare i risultati in Amazon Athena e scaricare i risultati come file con valori separati da virgole (.csv).

Se vedi i log in Detective ma la query non ha prodotto risultati, ciò potrebbe accadere per i seguenti motivi.

- I log non elaborati possono diventare disponibili in Detective prima di essere visualizzati nelle tabelle di log di Security Lake. Riprova più tardi.
- È possibile che in Security Lake manchino dei log . Se hai atteso per un periodo di tempo prolungato, significa che i log non sono presenti in Security Lake. Contatta l'amministratore di Security Lake per risolvere il problema.

Dettagli dell'attività per una geolocalizzazione

I dettagli dell'attività relativi alle geolocalizzazioni osservate di recente mostrano le API chiamate emesse da una geolocalizzazione durante il periodo di riferimento. Le API chiamate includono tutte le chiamate emesse dalla geolocalizzazione. Non si limitano alle chiamate che hanno utilizzato il risultato o l'entità del profilo. Per i bucket S3, le chiamate di attività sono API chiamate effettuate al bucket S3.

Detective determina la posizione delle richieste utilizzando i database MaxMind GeoIP. MaxMind riporta un'accuratezza molto elevata dei propri dati a livello nazionale, sebbene la precisione vari in base a fattori quali il paese e il tipo di IP. Per ulteriori informazioni su MaxMind, consulta Geolocalizzazione MaxMind IP. Se ritieni che uno qualsiasi dei dati GeoIP sia errato, puoi inviare una richiesta di correzione a Maxmind all'indirizzo MaxMind Correct Geo Data. IP2

Le API chiamate sono raggruppate in base ai servizi che le hanno emesse. Per i bucket S3, il servizio è sempre Amazon S3. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.

Per visualizzare i dettagli dell'attività, completa una delle seguenti operazioni:

- Sulla mappa, scegli una geolocalizzazione.
- Nell'elenco, scegli Dettagli per una geolocalizzazione.

I dettagli dell'attività sostituiscono l'elenco di geolocalizzazione. Per tornare all'elenco di geolocalizzazione, scegli Torna a tutti i risultati.

Tieni presente che Detective ha iniziato a memorizzare e visualizzare il nome del servizio per API le chiamate a partire dal 14 luglio 2021. Per le attività che si verificano prima di tale data, il nome del servizio è Servizio sconosciuto.

Contenuto dei dettagli dell'attività

Ogni scheda fornisce informazioni su tutte le API chiamate emesse dalla geolocalizzazione durante il periodo di riferimento.

Per ogni indirizzo IP, risorsa e API metodo, l'elenco mostra il numero di chiamate riuscite e non riusciteAPI.

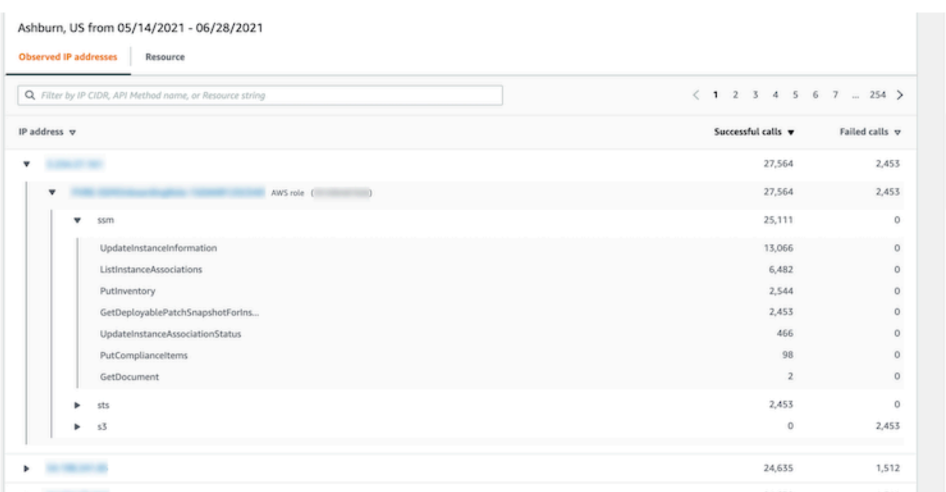
I dettagli dell'attività contengono le seguenti schede:

Indirizzi IP osservati

Visualizza inizialmente l'elenco degli indirizzi IP utilizzati per effettuare API chiamate dalla geolocalizzazione selezionata.

È possibile espandere ogni indirizzo IP per visualizzare le risorse che hanno emesso API chiamate da quell'indirizzo IP. L'elenco mostra il nome della risorsa. Per visualizzare l'ID principale, passa il mouse sul nome.

È quindi possibile espandere ogni risorsa per visualizzare le API chiamate specifiche emesse da quell'indirizzo IP da quella risorsa. Le API chiamate sono raggruppate in base ai servizi che le hanno emesse. Per i bucket S3, il servizio è sempre Amazon S3. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.

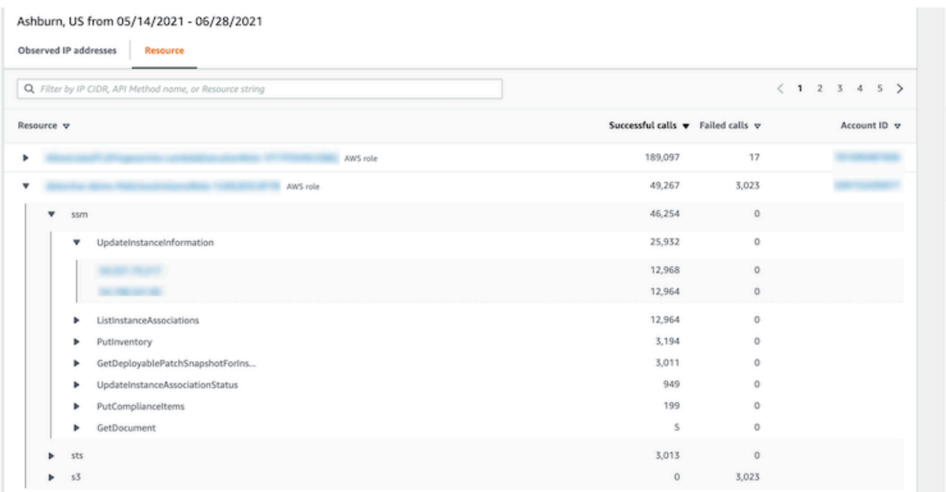


Risorsa

Visualizza inizialmente l'elenco delle risorse che hanno emesso API chiamate dalla geolocalizzazione selezionata. L'elenco mostra il nome della risorsa. Per visualizzare l'ID principale, passa il mouse sul nome. Per ogni risorsa, la scheda Risorsa mostra anche l' Account AWS associato.

È possibile espandere ogni utente o ruolo per visualizzare l'elenco delle API chiamate emesse da quella risorsa. Le API chiamate sono raggruppate in base ai servizi che le hanno emesse. Per i bucket S3, il servizio è sempre Amazon S3. Se Detective non è in grado di determinare il servizio che ha emesso una chiamata, la chiamata viene elencata in Servizio sconosciuto.

È quindi possibile espandere ogni API chiamata per visualizzare l'elenco di indirizzi IP da cui la risorsa ha emesso la API chiamata.



Ordinamento dei dettagli dell'attività

Puoi ordinare i dettagli dell'attività in base a una qualsiasi delle colonne dell'elenco.

Quando si ordina utilizzando la prima colonna, viene ordinato solo l'elenco di primo livello. Gli elenchi di livello inferiore sono sempre ordinati in base al numero di chiamate riuscite. API

Filtro dei dettagli dell'attività

È possibile utilizzare le opzioni di filtro per concentrarsi su sottoinsiemi o aspetti specifici dell'attività rappresentata nei dettagli dell'attività.

In tutte le schede, puoi filtrare l'elenco in base a uno qualsiasi dei valori nella prima colonna.

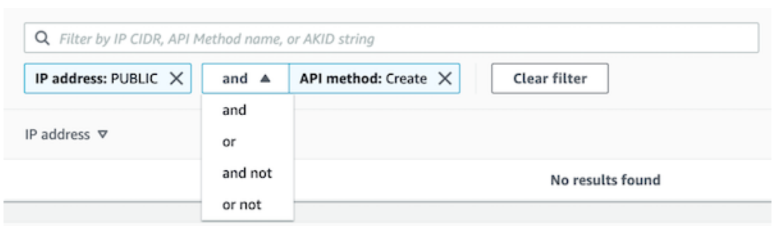
Aggiungere un filtro

1. Scegli la casella di filtro.
2. In Proprietà, scegli la proprietà da utilizzare per il filtraggio.
3. Fornisci il valore da utilizzare per il filtraggio. Il filtro supporta valori parziali. Ad esempio, quando si filtra per API metodo, se si filtra per**`Instance`**, i risultati includono qualsiasi API operazione contenuta `Instance` nel nome. Quindi sia `ListInstanceAssociations` che `UpdateInstanceInformation` corrisponderebbero.

   Per i nomi di servizio, API i metodi e gli indirizzi IP, è possibile specificare un valore o scegliere un filtro integrato.

   Per APISottostringhe comuni, scegliete la sottostringa che rappresenta il tipo di operazione, ad esempio`List`, `Create` o. `Delete` Ogni nome API di metodo inizia con il tipo di operazione.

   Per CIDRquanto riguarda i modelli, è possibile scegliere di includere solo indirizzi IP pubblici, indirizzi IP privati o indirizzi IP che corrispondono a uno CIDR schema specifico.
4. Se disponi di più filtri, scegli un'opzione booleana per impostare il modo in cui tali filtri sono collegati.

5. Per rimuovere un filtro, scegli l'icona x nell'angolo in alto a destra.
6. Per cancellare tutti i filtri, scegli Cancella filtro.

Dettagli dell'attività per il volume complessivo del VPC flusso

EC2Ad esempio, i dettagli dell'attività per Volume di VPC flusso complessivo mostrano le interazioni tra l'EC2istanza e gli indirizzi IP durante un intervallo di tempo selezionato.

Per un pod Kubernetes, Overall VPC flow volume mostra il volume complessivo di byte in entrata e in uscita dall'indirizzo IP assegnato al pod Kubernetes per tutti gli indirizzi IP di destinazione. L'indirizzo IP del pod Kubernetes non è univoco quando `hostNetwork:true`. In questo caso, il pannello mostra il traffico verso altri pod con la stessa configurazione e il nodo che li ospita.

Per un indirizzo IP, i dettagli dell'attività per Overall VPC flow Volume mostrano le interazioni tra l'indirizzo IP e EC2 le istanze durante un intervallo di tempo selezionato.

Per visualizzare i dettagli dell'attività per un singolo intervallo di tempo, scegli l'intervallo di tempo sul grafico.

Per visualizzare i dettagli dell'attività per il periodo di validità corrente, scegli Visualizza dettagli per il periodo di validità.

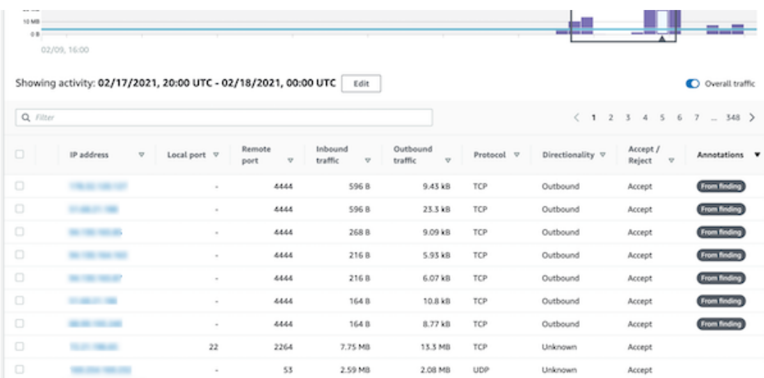
Contenuto dei dettagli dell'attività

Il contenuto riflette l'attività nell'intervallo di tempo selezionato.

EC2Ad esempio, i dettagli dell'attività contengono una voce per ogni combinazione univoca di indirizzo IP, porta locale, porta remota, protocollo e direzione.

Per un indirizzo IP, i dettagli dell'attività contengono una voce per ogni combinazione univoca di EC2 istanza, porta locale, porta remota, protocollo e direzione.

Ogni voce mostra il volume del traffico in entrata, il volume del traffico in uscita e se la richiesta di accesso è stata accettata o rifiutata. Nella profili dei risultati, la colonna Annotazioni indica quando un indirizzo IP è correlato al risultato corrente.



Ordinamento dei dettagli dell'attività

Puoi ordinare i dettagli dell'attività in base a una qualsiasi delle colonne nella tabella.

Per impostazione predefinita, i dettagli dell'attività vengono ordinati prima in base alle annotazioni, quindi in base al traffico in entrata.

Filtro dei dettagli dell'attività

Per concentrarti su un'attività specifica, puoi filtrare i dettagli dell'attività in base ai seguenti valori:

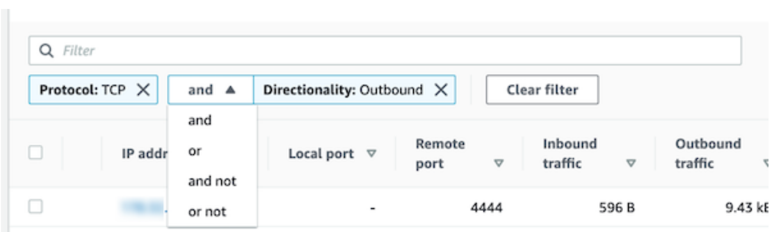
- Indirizzo IP o EC2 istanza
- Porta locale o remota
- Direzione
- Protocollo
- Se la richiesta è stata accettata o rifiutata

Aggiungere e rimuovere filtri

1. Scegli la casella di filtro.
2. In Proprietà, scegli la proprietà da utilizzare per il filtraggio.
3. Fornisci il valore da utilizzare per il filtraggio. Il filtro supporta valori parziali.

   Per filtrare in base all'indirizzo IP, puoi specificare un valore o scegliere un filtro integrato.

   Per CIDRquanto riguarda i modelli, puoi scegliere di includere solo indirizzi IP pubblici, indirizzi IP privati o indirizzi IP che corrispondono a CIDR uno schema specifico.
4. Se disponi di più filtri, scegli un'opzione booleana per impostare il modo in cui tali filtri sono collegati.



5. Per rimuovere un filtro, scegli l'icona x nell'angolo in alto a destra.
6. Per cancellare tutti i filtri, scegli Cancella filtro.

Selezione dell'intervallo di tempo per i dettagli dell'attività

Quando si visualizzano per la prima volta i dettagli dell'attività, l'intervallo di tempo corrisponde al periodo di validità o a un intervallo di tempo selezionato. È possibile modificare l'intervallo di tempo per i dettagli dell'attività.

Modificare l'intervallo di tempo per i dettagli dell'attività

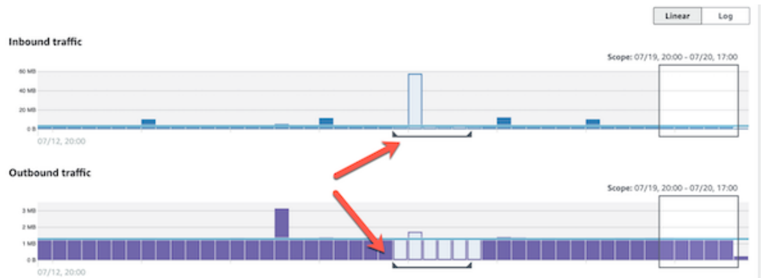
1. Scegli Modifica.

2. In Modifica finestra temporale, scegli l'ora di inizio e di fine da utilizzare.

   Per impostare la finestra temporale sul periodo di validità predefinito per il profilo, scegli Imposta il periodo di validità predefinito.

3. Scegli la Finestra temporale di aggiornamento.

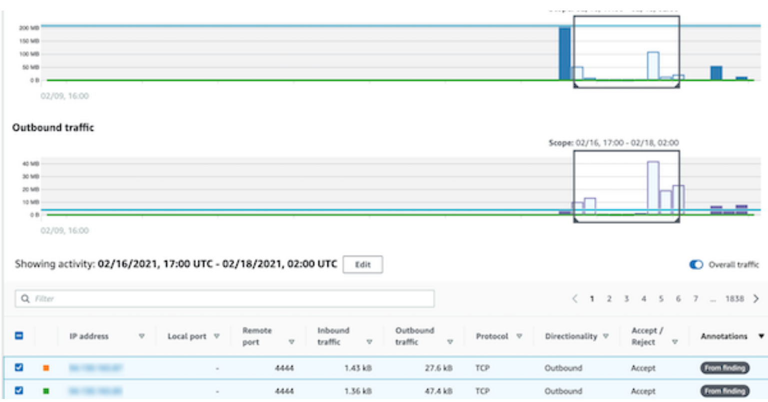
L'intervallo di tempo per i dettagli dell'attività è evidenziato nei grafici del pannello del profilo.



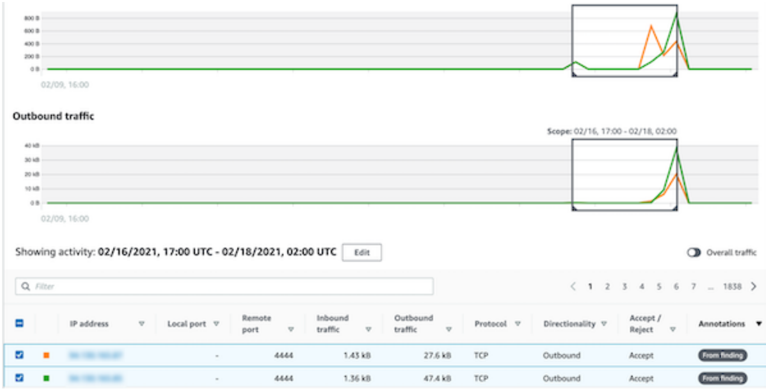
Visualizzazione del volume di traffico per le righe selezionate

Quando identifichi le righe che ti interessano, sui grafici principali puoi visualizzare il volume di traffico nel tempo relativo a tali righe.

Per ogni riga da aggiungere ai grafici, seleziona la casella di controllo. Per ogni riga selezionata, il volume viene visualizzato come una linea sui grafici in entrata o in uscita.



Per concentrarti sul volume di traffico per le voci selezionate, puoi nascondere il volume complessivo. Per mostrare o nascondere il volume di traffico complessivo, attiva Traffico complessivo.



Visualizzazione del VPC flusso di traffico per i EKS cluster

Detective ha visibilità sui log di flusso di Amazon Virtual Private Cloud (AmazonVPC), che rappresentano il traffico che attraversa i cluster Amazon Elastic Kubernetes Service (Amazon). EKS Per le risorse Kubernetes, il contenuto dei log di VPC flusso dipende dalla Container Network Interface () distribuita nel cluster. CNI EKS

Un EKS cluster con una configurazione predefinita utilizza il VPC CNI plug-in Amazon. Per maggiori dettagli, consulta [Managing VPC CNI](#) in the Amazon EKS User Guide. Il VPC CNI plug-in Amazon invia il traffico interno con l'indirizzo IP del pod e traduce l'indirizzo IP di origine nell'indirizzo IP del nodo per la comunicazione esterna. Detective può acquisire e correlare il traffico interno al pod corretto, ma non può fare lo stesso per il traffico esterno.

Se vuoi che Detective abbia visibilità sul traffico esterno dei tuoi pod, abilita External Source Network Address Translation (SNAT). L'abilitazione SNAT presenta limitazioni e svantaggi. Per maggiori dettagli, consulta [SNATla sezione relativa ai pod](#) nella Amazon EKS User Guide.

Se utilizzi un CNI plugin diverso, Detective ha una visibilità limitata ai pod con`hostNetwork:true`. Per questi pod, il pannello VPCFlow mostra tutto il traffico diretto all'indirizzo IP del pod. Ciò include il traffico verso il nodo host e qualsiasi pod sul nodo con la configurazione `hostNetwork:true`.

Detective visualizza il traffico nel pannello di VPCflusso di un EKS pod per le seguenti configurazioni del EKS cluster:

- In un cluster con il VPC CNI plug-in Amazon, qualsiasi pod con la configurazione che `hostNetwork:false` invia traffico all'interno VPC del cluster.
- In un cluster con il VPC CNI plug-in Amazon e la configurazione`AWS_VPC_K8S_CNI_EXTERNALSNAT=`**`true`**, qualsiasi pod con traffico di `hostNetwork:false` invio all'esterno VPC del cluster.

- Qualsiasi pod con la configurazione `hostNetwork:true`. Il traffico proveniente dal nodo viene mescolato al traffico proveniente da altri pod con la configurazione `hostNetwork:true`.

Detective non visualizza il traffico nel pannello di VPCflusso per:

- In un cluster con il VPC CNI plug-in Amazon e la configurazione`AWS_VPC_K8S_CNI_EXTERNALSNAT=false`, qualsiasi pod con la configurazione che `hostNetwork:false` invia traffico all'esterno VPC del cluster.
- In un cluster senza il VPC CNI plug-in Amazon per Kubernetes, qualsiasi pod con la configurazione. `hostNetwork:false`
- Qualsiasi pod che invia traffico a un altro pod ospitato nello stesso nodo.

Visualizzazione del VPC flusso di traffico per Amazon condiviso VPCs

Detective ha visibilità sui log di flusso di Amazon Virtual Private Cloud (AmazonVPC) per la condivisione VPCs di:

- Se un account membro di Detective ha un account Amazon condiviso VPC e ci sono altri account non Detective che lo utilizzanoVPC, Detective monitora tutto il traffico proveniente da tale VPC account e fornisce la visualizzazione di tutto il flusso di traffico all'interno del. VPC
- Se hai un'EC2istanza Amazon all'interno di un Amazon condiviso VPC e il VPC proprietario condiviso non è un membro di Detective, Detective non monitorerà alcun traffico proveniente daVPC. Se desideri visualizzare il flusso di traffico all'interno diVPC, devi aggiungere il VPC proprietario di Amazon come membro del tuo Detective graph.

Attività complessiva di Kubernetes API che coinvolge il cluster EKS

I dettagli dell'attività per l'APIattività complessiva di Kubernetes che coinvolge il EKS cluster mostrano il numero di API chiamate Kubernetes riuscite e non riuscite emesse durante un intervallo di tempo selezionato.

Per visualizzare i dettagli dell'attività per un singolo intervallo di tempo, scegli l'intervallo di tempo sul grafico.

Per visualizzare i dettagli dell'attività per il periodo di validità corrente, scegli Visualizza dettagli per il periodo di validità.

Contenuto dei dettagli dell'attività (cluster, pod, utente, ruolo, sessione di ruolo)

Per un cluster, un pod, un utente, un ruolo o una sessione di ruolo, i dettagli dell'attività contengono le seguenti informazioni:

- Ogni scheda fornisce informazioni sul set di API chiamate emesse durante l'intervallo di tempo selezionato.

  Per i cluster, le API chiamate sono avvenute all'interno del cluster.

  Per i pod, le API chiamate erano indirizzate al pod.

  Per gli utenti, i ruoli e le sessioni di ruolo, le API chiamate venivano emesse da utenti di Kubernetes che si erano autenticati come utente, ruolo o sessione di ruolo.
- Per ogni immissione, i dettagli dell'attività mostrano il numero di chiamate riuscite, non riuscite, non autorizzate e proibite.
- Le informazioni includono l'indirizzo IP, il tipo di chiamata Kubernetes, l'entità interessata dalla chiamata e il soggetto (account o utente del servizio) che ha effettuato la chiamata. Dai dettagli dell'attività, puoi passare ai profili relativi all'indirizzo IP, al soggetto e all'entità interessata.

I dettagli dell'attività contengono le seguenti schede:

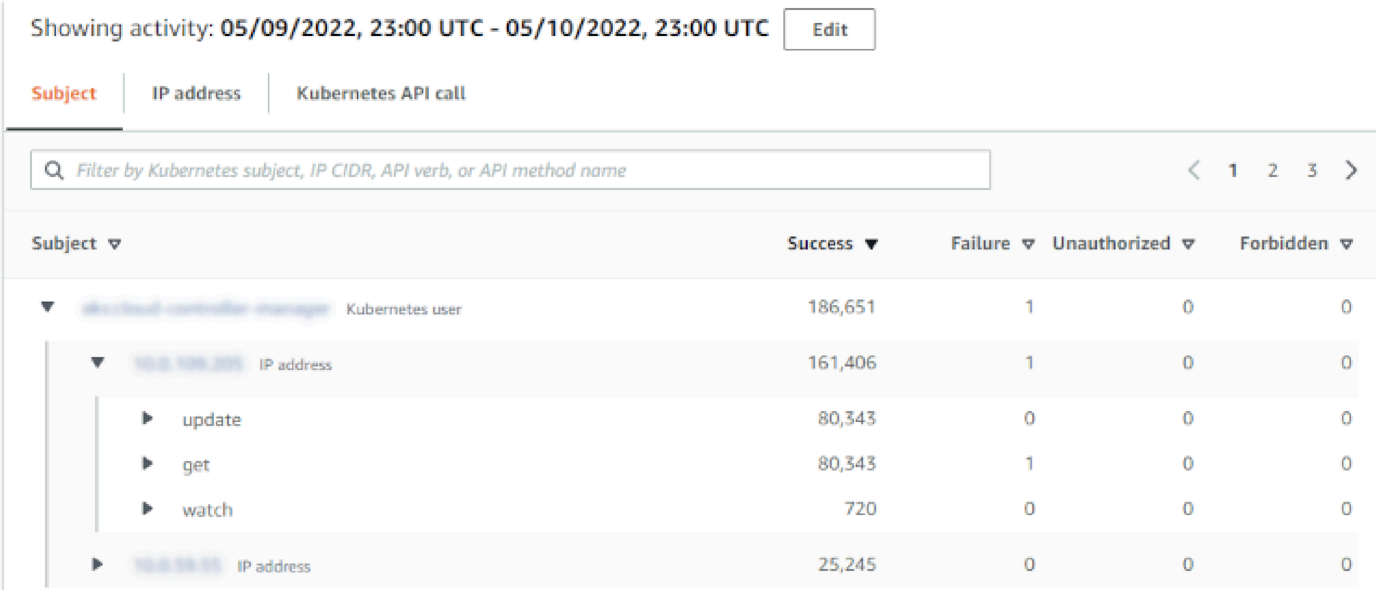
Oggetto

Visualizza inizialmente l'elenco degli account di servizio e degli utenti utilizzati per effettuare chiamate. API

È possibile espandere ogni account di servizio e utente per visualizzare l'elenco degli indirizzi IP da cui l'account o l'utente ha effettuato API le chiamate.

Puoi quindi espandere ogni indirizzo IP per mostrare le API chiamate Kubernetes effettuate da quell'account o utente a partire da quell'indirizzo IP.

Espandi la API chiamata Kubernetes per visualizzare l'identificazione dell'azione `requestURI` eseguita.



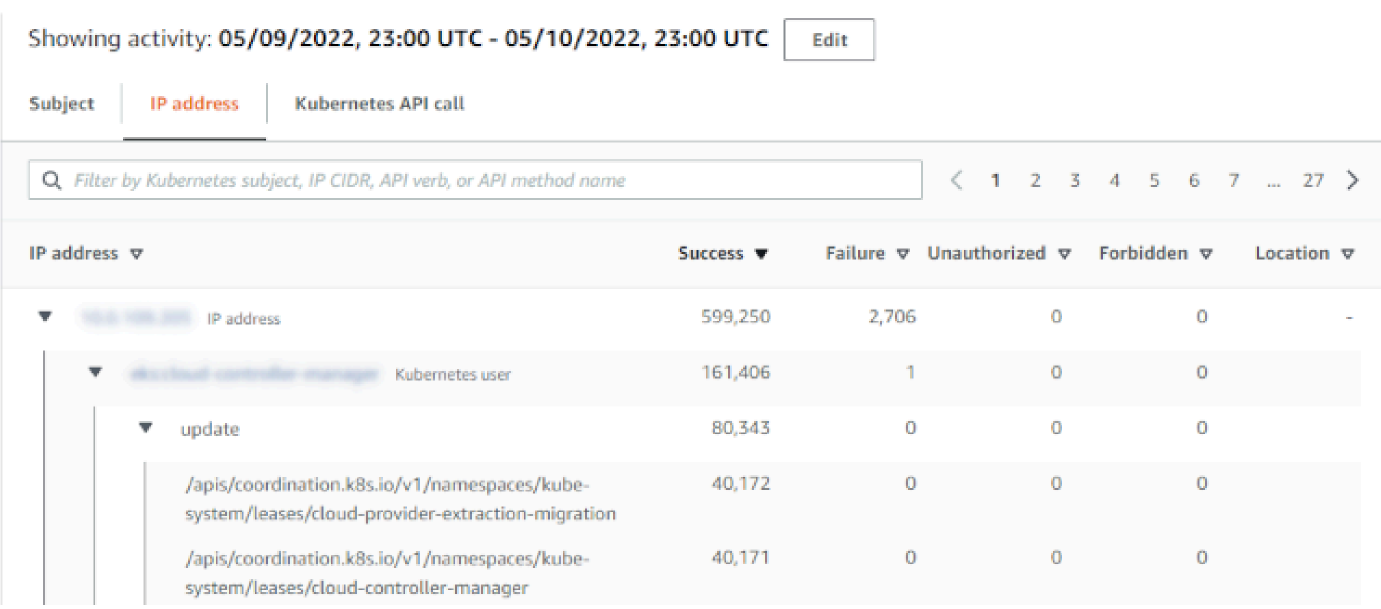
Indirizzo IP

Visualizza inizialmente l'elenco degli indirizzi IP da cui sono state effettuate le API chiamate.

Puoi espandere ogni chiamata per visualizzare l'elenco dei soggetti Kubernetes (account di servizio e utenti) che hanno effettuato la chiamata.

È quindi possibile espandere ciascun oggetto fino a un elenco di tipi di API chiamate effettuate dall'oggetto durante il periodo di riferimento.

Espandi il tipo di API chiamata per visualizzare la richiesta e URI identificare l'azione che è stata eseguita.



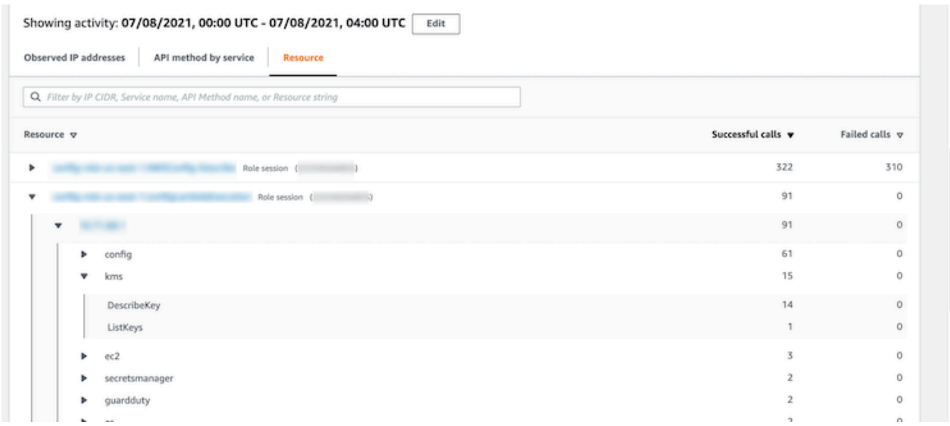
Chiamata Kubernetes API

Visualizza inizialmente l'elenco dei verbi di chiamata KubernetesAPI.

Puoi espandere ogni API verbo per visualizzare quello associato a quell'azione requestURIs .

Puoi quindi espandere ogni richiesta URI per visualizzare l'oggetto di Kubernetes (account e utenti del servizio) che ha effettuato la chiamata. API

Espandi l'oggetto per vedere quale soggetto IPs è stato utilizzato per effettuare la chiamata. API



Ordinamento dei dettagli dell'attività

Puoi ordinare i dettagli dell'attività in base a una qualsiasi delle colonne dell'elenco.

Quando si ordina utilizzando la prima colonna, viene ordinato solo l'elenco di primo livello. Gli elenchi di livello inferiore sono sempre ordinati in base al numero di chiamate riuscite. API

Filtro dei dettagli dell'attività

È possibile utilizzare le opzioni di filtro per concentrarsi su sottoinsiemi o aspetti specifici dell'attività rappresentata nei dettagli dell'attività.

In tutte le schede, puoi filtrare l'elenco in base a uno qualsiasi dei valori nella prima colonna.

Selezione dell'intervallo di tempo per i dettagli dell'attività

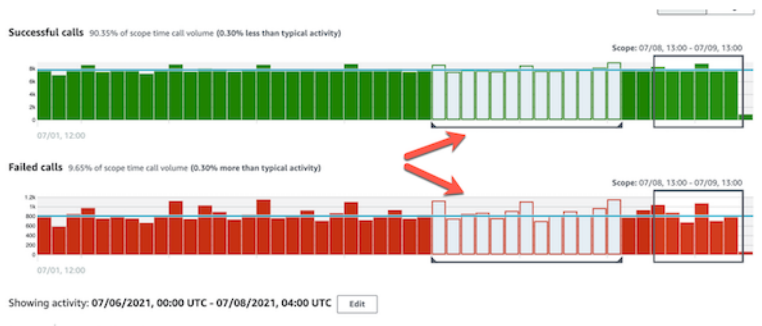
Quando si visualizzano per la prima volta i dettagli dell'attività, l'intervallo di tempo corrisponde al periodo di validità o a un intervallo di tempo selezionato. È possibile modificare l'intervallo di tempo per i dettagli dell'attività.

Modificare l'intervallo di tempo per i dettagli dell'attività

1. Scegli Modifica.
2. In Modifica finestra temporale, scegli l'ora di inizio e di fine da utilizzare.

   Per impostare la finestra temporale sul periodo di validità predefinito per il profilo, scegli Imposta il periodo di validità predefinito.
3. Scegli la Finestra temporale di aggiornamento.

L'intervallo di tempo per i dettagli dell'attività è evidenziato nei grafici del pannello del profilo.



Utilizzo della guida del pannello del profilo durante un'indagine

Ogni pannello del profilo è progettato per fornire risposte a domande specifiche che sorgono quando si conduce un'indagine e si analizza l'attività delle entità correlate.

La guida fornita per ogni pannello del profilo ti aiuta a trovare queste risposte.

Le linee guida del pannello del profilo iniziano con una singola frase sul pannello stesso. Questa guida fornisce una breve spiegazione dei dati presentati nel pannello.

Per visualizzare una guida più dettagliata per un pannello, scegli Altre informazioni dall'intestazione del pannello. Questa guida estesa viene visualizzata nel riquadro di aiuto.

La guida può fornire questi tipi di informazioni:

- Una panoramica del contenuto del pannello
- Come usare il pannello per rispondere alle domande pertinenti
- Passaggi successivi suggeriti in base alle risposte

Gestione del periodo di validità

Personalizza il periodo di validità utilizzato per limitare i dati visualizzati nei profili di entità.

I grafici, le sequenze temporali e gli altri dati visualizzati nei profili di entità si basano tutti sul periodo di validità corrente. Il periodo di validità è il riepilogo dell'attività di un'entità nel tempo. Viene visualizzato nella parte in alto a destra di ogni profilo nella console Amazon Detective. I dati visualizzati su tali grafici, sequenze temporali e altre visualizzazioni si basano sul periodo di validità. Per alcuni pannelli di profilo, viene aggiunto del tempo prima e dopo il periodo di validità per fornire un contesto. In Detective, tutti i timestamp sono visualizzati in UTC per impostazione predefinita. È possibile selezionare il fuso orario locale modificando le preferenze del timestamp. Per aggiornare la preferenza Timestamp, consulta the section called “Impostazione del formato del timestamp”.

L'analisi dei dati di Detective utilizza il periodo di validità per verificare la presenza di attività insolite. Il processo di analisi rileva l'attività durante il periodo di validità, quindi la confronta con l'attività dei 45 giorni precedenti il periodo di validità. Inoltre, utilizza tale intervallo di tempo di 45 giorni per generare linee di base di attività.

In una panoramica dei risultati, il periodo di validità riflette la prima e l'ultima volta che il risultato è stato osservato. Per ulteriori informazioni sulla panoramica dei risultati, consulta the section called “Panoramica degli esiti”.

Man mano che si conduce un'indagine, è possibile modificare il periodo di validità. Ad esempio, se l'analisi originale si basava sull'attività di un solo giorno, è possibile estendere il periodo a una settimana o un mese. Il periodo prolungato può aiutare a capire meglio se l'attività rientra in uno schema normale o inusuale.

È inoltre possibile impostare il periodo di validità in modo che corrisponda a un risultato associato per l'entità corrente.

Quando si modifica il periodo di validità, Detective ripete l'analisi e aggiorna i dati visualizzati in base al nuovo periodo di validità.

Il periodo di validità non può essere inferiore a un'ora e non può essere superiore a un anno. Le ore di inizio e fine devono essere un'ora.

Impostazione di date e ore di inizio e fine specifiche

Puoi impostare le date di inizio e fine del periodo di validità dalla console Detective.

Impostare orari di inizio e fine specifici per il nuovo periodo di validità

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. In un profilo di entità, scegli il periodo di validità.
3. Nel pannello Modifica periodo di validità, in Inizio, scegli la nuova data e ora di inizio per il periodo. Per la nuova ora di inizio, scegli solo l'ora.
4. In Fine, scegli la nuova data e ora di fine per il periodo di validità. Per la nuova ora di fine, scegli solo l'ora. L'ora di fine deve essere almeno un'ora dopo l'ora di inizio.
5. Al termine della modifica, per salvare le modifiche e aggiornare i dati visualizzati, scegli Aggiorna periodo di validità.

Modifica della durata del periodo di validità

Quando imposti la durata del periodo di validità, Detective imposta l'intervallo di tempo su quel periodo di tempo dall'ora corrente.

Modificare la durata del periodo di validità

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. In un profilo di entità, scegli il periodo di validità.
3. Nel pannello Modifica periodo di validità, accanto a Cronologico, scegli la durata del periodo di validità.

   La specifica di un intervallo di tempo aggiorna le impostazioni di inizio e fine.
4. Al termine della modifica, per salvare le modifiche e aggiornare i dati visualizzati, scegli Aggiorna periodo di validità.

Configurazione del periodo di validità su una finestra dell'ora del risultato

A ogni risultato è associata una finestra temporale che riflette la prima e l'ultima volta in cui il risultato è stato osservato. Quando si visualizza una panoramica dei risultati, il periodo di validità passa alla finestra dell'ora dei risultati.

Da un profilo di entità, è possibile allineare il periodo di validità alla finestra temporale relativa a un risultato associato. Ciò consente di esaminare l'attività che si è svolta in quel periodo.

Per allineare il periodo di validità a una finestra dell'ora del risultato, nel pannello Risultati associati, scegli il risultato che desideri utilizzare.

Detective inserisce i dettagli del risultato e imposta il periodo di validità sulla finestra dell'ora del risultato.

Impostazione del periodo di validità nella pagina di riepilogo

Mentre esamini la pagina Riepilogo, puoi modificare il periodo di validità in modo da visualizzare l'attività per qualsiasi periodo di 24 ore nei 365 giorni precedenti.

Impostare il periodo di validità nella pagina Riepilogo

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Riepilogo.
3. Nel pannello Periodo di validità, accanto a Riepilogo, puoi modificare la data e l'ora di inizio. L'ora di inizio deve essere compresa negli ultimi 365 giorni.

   Quando modifichi la data e l'ora di inizio, la data e l'ora di fine vengono aggiornate automaticamente a 24 ore dall'ora di inizio scelta.

   > **Note**
   >
   > Con Detective puoi accedere fino a un anno di dati storici degli eventi. Per ulteriori informazioni sui dati di origine in Detective, consulta Dati di origine utilizzati in un grafico comportamentale.

4. Al termine della modifica, per salvare le modifiche e aggiornare i dati visualizzati, scegli Aggiorna periodo di validità.

Visualizzazione dei dettagli dei risultati associati in Detective

Ogni profilo di entità contiene un pannello dei risultati associato che elenca i risultati che hanno interessato l'entità nel periodo di validità corrente. Un'indicazione che un'entità è stata compromessa è la sua presenza in molteplici risultati. I tipi di risultati possono anche fornire informazioni sul tipo di attività di cui preoccuparsi.

Il pannello dei risultati associato viene visualizzato immediatamente sotto il pannello del profilo dei dettagli dell'entità.

Per ciascun risultato, sono incluse le informazioni seguenti:

- Il titolo del risultato, che è anche un collegamento alla panoramica dei risultati.
- L' AWS account associato al risultato, che è anche un collegamento al profilo dell'account
- Il tipo di risultato
- Il primo orario in cui è stato osservato il risultato
- L'orario più recente in cui è stato osservato il risultato
- La gravità del risultato

Per visualizzare i dettagli di un risultato, scegli il pulsante radio corrispondente al risultato. Detective compila il pannello dei dettagli dei risultati nella parte destra della pagina. Detective modifica anche il periodo di validità in modo che diventi la finestra temporale del risultato. In questo modo, potrai concentrarti sulle attività che si sono svolte in quel periodo.

Se si è passati al profilo dell'entità da una panoramica dei risultati, tale risultato viene selezionato automaticamente e vengono visualizzati i dettagli del risultato.

Dai dettagli del risultato, per tornare alla panoramica dei risultati, scegli Visualizza tutte le entità correlate.

Puoi anche archiviare il risultato. Per maggiori dettagli, consulta Archiviazione di un GuardDuty risultato Amazon.

Visualizzazione dei dettagli per entità ad alto volume in Detective

Nel grafico di comportamento, Amazon Detective tiene traccia delle relazioni tra le entità. Ad esempio, ogni grafico comportamentale registra quando un AWS utente crea un AWS ruolo e quando un'EC2istanza si connette a un indirizzo IP.

Quando un'entità ha troppe relazioni durante un periodo di tempo, Detective non riesce a memorizzare tutte le relazioni. Quando ciò si verifica durante il periodo di validità corrente, Detective ti avvisa. Detective fornisce anche un elenco delle occorrenze di entità ad alto volume.

Cos'è un'entità ad alto volume?

Durante un determinato intervallo di tempo, un'entità potrebbe essere l'origine o la destinazione di un numero estremamente elevato di connessioni. Ad esempio, un'EC2istanza può avere connessioni da milioni di indirizzi IP.

Detective mantiene un limite al numero di connessioni che può gestire durante ogni intervallo di tempo. Se un'entità supera tale limite, Detective scarta le connessioni per quell'intervallo di tempo.

Ad esempio, supponiamo che il limite sia di 100.000.000 di connessioni per intervallo di tempo. Se un'EC2istanza è connessa da più di 100.000.000 di indirizzi IP durante un intervallo di tempo, Detective elimina le connessioni da quell'intervallo di tempo.

Tuttavia, potresti essere in grado di analizzare tale attività in base all'entità all'altra estremità della relazione. Per continuare con l'esempio, mentre un'EC2istanza può essere connessa da milioni di indirizzi IP, un singolo indirizzo IP si connette a molte meno istanze. EC2 Ogni profilo di indirizzo IP fornisce dettagli sulle EC2 istanze a cui l'indirizzo IP si è connesso.

Visualizzazione della notifica di entità ad alto volume su un profilo

Detective visualizza un avviso nella parte superiore del profilo del risultato o dell'entità se il periodo di validità include un intervallo di tempo in cui l'entità ha un volume elevato. Per quanto riguarda i profili dei risultati, l'avviso è per l'entità coinvolta.

L'avviso include l'elenco delle relazioni che hanno intervalli di tempo ad alto volume. Ogni voce dell'elenco contiene una descrizione della relazione e l'inizio dell'intervallo di tempo ad alto volume.

Un intervallo di tempo ad alto volume potrebbe essere un indicatore di attività sospette. Per capire quali altre attività si sono verificate nello stesso momento, puoi concentrare la tua indagine su un intervallo di tempo ad alto volume. L'avviso relativo alle entità a volumi elevati include un'opzione per impostare il periodo di validità in base a tale intervallo di tempo.

Impostare il periodo di validità su un intervallo di tempo ad alto volume

1. Nell'avviso relativo all'entità ad alto volume, scegli l'intervallo di tempo.
2. Nel menu a comparsa, scegli Applica periodo di validità.

Visualizzazione dell'elenco delle entità ad alto volume per il periodo di validità corrente

La pagina Entità ad alto volume contiene un elenco di intervalli di tempo ed entità ad alto volume durante il periodo di validità corrente.

Visualizzare la pagina Entità ad alto volume

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.

2. Nel pannello di navigazione di Detective, scegli Entità ad alto volume.

Ogni voce dell'elenco contiene le seguenti informazioni:

- L'inizio dell'intervallo di tempo ad alto volume
- L'identificatore e il tipo di entità.
- La descrizione della relazione, ad esempio "EC2istanza connessa dall'indirizzo IP»

È possibile filtrare e ordinare l'elenco in base a qualsiasi colonna. Puoi anche accedere al profilo di entità per un'entità coinvolta.

Passare al profilo di un'entità

1. Nell'elenco Entità ad alto volume, scegli la riga da cui navigare.
2. Scegli Visualizza il profilo con il periodo di validità ad alto volume.

Quando utilizzi questa opzione per accedere a un profilo di entità, il periodo di validità viene impostato come segue:

- Il periodo di validità inizia 30 giorni prima dell'intervallo di tempo ad alto volume.
- Il periodo di validità termina alla fine dell'intervallo di tempo ad alto volume.

Alla ricerca di un reperto o di un'entità in Detective

Con la funzione di ricerca di Amazon Detective, puoi cercare un risultato o un'entità. Dai risultati della ricerca, puoi passare al profilo di un'entità o a una panoramica dei risultati. Se la ricerca restituisce più di 10.000 risultati, vengono esportati solo i primi 10.000. La modifica dei criteri di ordinamento modifica i risultati restituiti.

Puoi esportare i risultati della ricerca in un file di valori separati da virgola (CSV). Questo file contiene i dati restituiti nella pagina di ricerca. I dati vengono esportati in formato valori separati da virgole (). CSV Il nome del file dei dati esportati segue il formato pattern -mm-dd.csv. detective-page-panel-yyyy È possibile arricchire le indagini di sicurezza manipolando i dati utilizzando altri AWS servizi, applicazioni di terze parti o programmi per fogli di calcolo che supportano l'importazione. CSV

> **Note**
>
> Se è in corso un'esportazione, attendi il completamento dell'operazione prima di provare a esportare altri dati.

Completamento della ricerca

Per completare la ricerca, scegli il tipo di entità da cercare. Quindi immetti l'identificatore esatto o un identificatore con caratteri jolly `*` o `?`. Per cercare una serie di indirizzi IP, puoi anche utilizzare le notazioni a punti. CIDR Consulta le seguenti stringhe di ricerca di esempio.

Per gli indirizzi IP:

- `1.0.*.*`
- `1.0.133.*`
- `1.0.0.0/16`
- `0.239.48.198/31`

Per tutti gli altri tipi di entità:

- `Admin`
- `ad*`

- `ad*n`
- `ad*n*`
- `adm?n`
- `a?m*`
- `*min`

Per ogni tipo di entità, sono supportati i seguenti identificatori:

- Per Findings, l'identificatore del risultato o la ricerca Amazon Resource Name (ARN).
- Per AWS gli account, l'ID dell'account.
- Per AWS i ruoli e AWS gli utenti, l'ID principale, il nome o ilARN.
- Per i cluster Container, il nome del cluster oARN.
- Per le immagini di container, il repository o il riepilogo completo dell'immagine di container.
- Per i contenitori Pods o Tasks, il nome del contenitore o il nome UID del contenitore.
- Ad EC2 esempio, l'identificatore dell'istanza o il. ARN
- Per il gruppo di risultati, l'identificatore del gruppo di risultati.
- Per gli indirizzi IP, l'indirizzo in notazione a punti CIDR o in notazione a punti.
- Per i soggetti Kubernetes (account di servizio o utenti), il nome.
- Per una sessione di ruolo, puoi utilizzare uno dei seguenti valori per la ricerca:
  - L'identificatore di sessione del ruolo.

    L'identificatore della sessione del ruolo utilizza il formato `<rolePrincipalID>:<sessionName>`.

    Ecco un esempio: `AROA12345678910111213:MySession`.
  - Sessione di ruolo ARN
  - Nome della sessione
  - ID principale del ruolo assunto
  - Nome del ruolo assunto
- Per i bucket S3, il nome o il bucket. ARN
- Per gli utenti federati, l'ID principale o il nome utente. L'ID principale è `<identityProvider>:<username>` o `<identityProvider>:<audience>:<username>`.

- Per gli agenti utente, il nome dell'agente utente.

Ricercare un risultato o un'entità

1. Accedi alla AWS Management Console. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione selezionare Search (Cerca).
3. Dal menu Scegli il tipo, scegli il tipo di elemento che stai cercando.

   Tieni presente che quando scegli Utente, puoi cercare un utente AWS o un utente federato.

   La sezione Esempi dai dati contiene un set di identificatori del tipo selezionato presenti nei dati del grafico di comportamento. Per visualizzare il profilo di uno degli esempi, scegli il relativo identificatore.
4. Immetti l'identificatore esatto o un identificatore con caratteri jolly da cercare.

   La ricerca non fa distinzione tra maiuscole e minuscole.
5. Scegli Cerca o premi Invio.

Utilizzo dei risultati della ricerca

Una volta completata la ricerca, Detective visualizza un elenco di un massimo di 10.000 risultati corrispondenti. Per le ricerche che utilizzano un identificatore univoco, esiste un solo risultato corrispondente.

Dai risultati, per accedere al profilo dell'entità o alla panoramica dei risultati, scegli l'identificatore.

Per i risultati, i ruoli, gli utenti e EC2 le istanze, i risultati della ricerca includono l'account associato. Per passare al profilo dell'account, scegli l'identificatore dell'account.

Risoluzione dei problemi di ricerca

Se Detective non trova il risultato o l'entità, verifica innanzitutto di aver inserito l'identificatore corretto. Se l'identificatore è corretto, puoi anche controllare quanto segue.

- Il risultato o l'entità appartengono a un account membro abilitato nel tuo grafico di comportamento? Se l'account associato non è stato invitato al grafico di comportamento come account membro, il grafico non conterrà dati relativi a quell'account.

Se un account membro invitato non ha accettato l'invito, il grafico di comportamento non conterrà dati relativi a quell'account.

- Un risultato viene archiviato? Detective non riceve i risultati archiviati da Amazon GuardDuty.
- Il risultato o l'entità si sono verificati prima che Detective iniziasse a importare dati nel tuo grafico di comportamento? Se il reperto o l'entità non è presente nei dati che il Detective inserisce, il grafico di comportamento non contiene i relativi dati.
- Il risultato o l'entità provengono dalla Regione corretta? Ogni grafico di comportamento è specifico per un Regione AWS. Un grafico di comportamento non contiene dati provenienti da altre Regioni.

Gestione degli account in Detective

Quando un account abilita Detective, diventa l'account amministratore per il grafico di comportamento e sceglie gli account membri per il grafico. Un account amministratore può invitare gli account a partecipare a un grafico comportamentale. Quando l'account accetta l'invito, Detective abilita l'account come account membro. Gli account membri aggiunti su invito possono rimuovere se stessi dal grafico di comportamento.

Quando un account viene abilitato come account membro, Detective inizia a importare ed estrarre i dati dell'account membro in quel grafico di comportamento.

Ogni grafico di comportamento contiene i dati di uno o più account. Un grafico di comportamento può contenere fino a 1.200 account membri.

Se sei integrato con AWS Organizations, l'account di gestione dell'organizzazione designa l'account amministratore Detective per l'organizzazione. Quell'account amministratore di Detective diventa quindi l'account amministratore per il grafico di comportamento dell'organizzazione. L'account amministratore di Detective abilita qualsiasi account dell'organizzazione come account membro nel grafico di comportamento dell'organizzazione. Gli account dell'organizzazione non possono rimuoversi dal grafico di comportamento dell'organizzazione.

Amazon Detective addebita a ciascun account i dati con cui contribuisce per ogni grafico di comportamento. Per informazioni sul monitoraggio del volume di dati per ogni account in un grafico comportamentale, consulta Previsione e monitoraggio dei costi di Amazon Detective.

Indice

Restrizioni e raccomandazioni sugli account in Detective

Quando gestisci gli account di Amazon Detective, considera le seguenti restrizioni e raccomandazioni.

Numero massimo di account membri

Detective consente fino a 1.200 account membri in ogni grafico di comportamento.

Se lo utilizzi AWS Organizations per gestire gli account, per impostazione predefinita Detective mostra fino a 5000 account membri nella pagina Gestione account. Se desideri visualizzare tutti gli account, seleziona Carica tutti gli account. Potrebbero essere necessari alcuni minuti per restituire tutti i risultati.

Account e Regioni

Se si utilizza AWS Organizations per gestire gli account, l'account di gestione dell'organizzazione designa un account amministratore Detective per l'organizzazione. L'account amministratore di Detective diventa l'account amministratore per il grafico di comportamento dell'organizzazione.

L'account amministratore di Detective deve essere lo stesso in tutte le Regioni. L'account di gestione dell'organizzazione designa l'account amministratore di Detective separatamente in ciascuna Regione. L'account amministratore di Detective gestisce anche i grafici del comportamento dell'organizzazione e gli account membri separatamente in ciascuna Regione.

Per gli account membro creati per invito, l'associazione amministratore-membro viene creata solo nella Regione da cui viene inviato l'invito. L'account amministratore deve abilitare Detective in ogni Regione e dispone di un grafico del comportamento separato in ogni Regione. L'account amministratore invita quindi ogni account ad associarsi come account membro in quella Regione.

Un account può essere un account membro di più grafici del comportamento nella stessa Regione. Un account può essere solo l'account amministratore di un grafico del comportamento per Regione. Un account può essere un account amministratore in diverse Regioni.

Allineamento degli account degli amministratori con Security Hub e GuardDuty

Per garantire il corretto GuardDuty funzionamento delle integrazioni con AWS Security Hub e Amazon, consigliamo di utilizzare lo stesso account come account amministratore in tutti questi servizi.

Per informazioni, consulta the section called "Allineamento consigliato con e GuardDuty AWS Security Hub".

Concessione delle autorizzazioni necessarie per gli account amministratore

Per garantire che un account amministratore disponga delle autorizzazioni necessarie per gestire il relativo grafico comportamentale, allega la policy `AmazonDetectiveFullAccess` gestita al principale. IAM

Riflesso degli aggiornamenti dell'organizzazione in Detective

Le modifiche a un'organizzazione non si riflettono immediatamente in Detective.

Per la maggior parte delle modifiche, ad esempio account dell'organizzazione nuovi e rimossi, perché Detective riceva una notifica potrebbe essere necessaria fino a un'ora.

La propagazione di una modifica all'account amministratore Detective designato in Organizations richiede meno tempo.

Utilizzo di Organizations per gestire gli account basati su grafici comportamentali

Potresti avere già un grafico di comportamento con gli account membri che hanno accettato un invito manuale. Se sei registrato AWS Organizations, segui la procedura seguente per utilizzare Organizations per abilitare e gestire gli account dei membri invece di utilizzare la procedura di invito manuale:

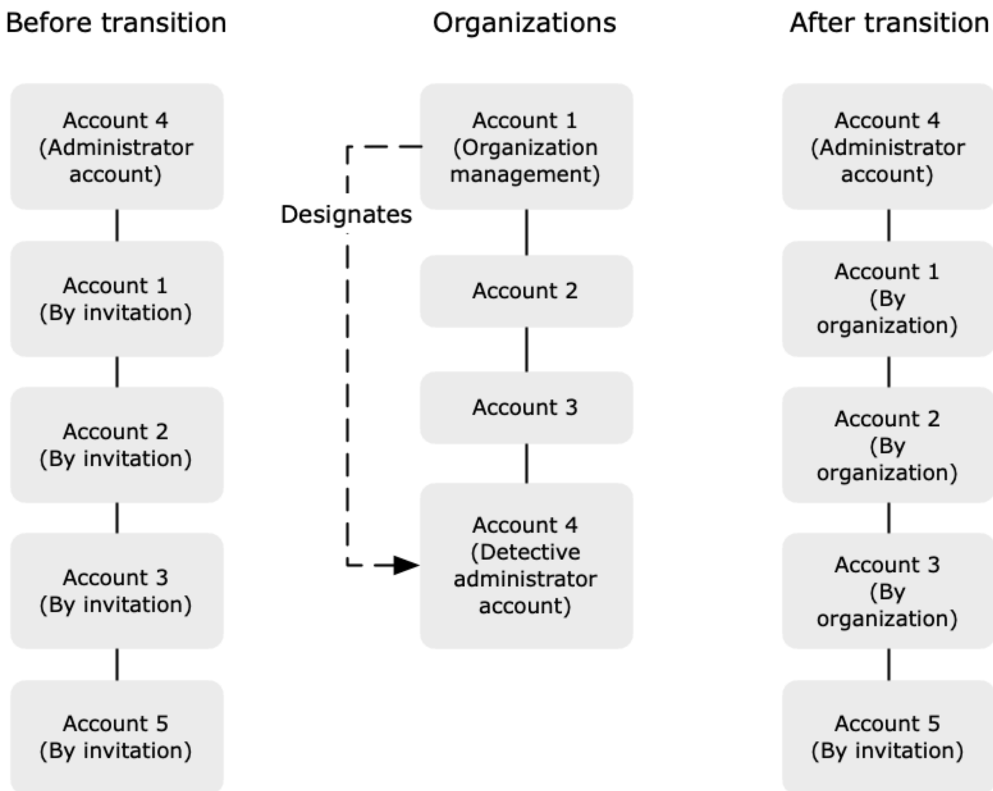
1. Designa l'account amministratore di Detective per l'organizzazione. Questo crea il grafico di comportamento dell'organizzazione.

   Se l'account amministratore di Detective ha già un grafico di comportamento, quel grafico diventa il grafico di comportamento dell'organizzazione.

2. Abilita gli account dell'organizzazione come account membri nel grafico di comportamento dell'organizzazione.

   Se il grafico di comportamento dell'organizzazione dispone di account membri esistenti che sono account dell'organizzazione, tali account vengono abilitati automaticamente.

Il diagramma seguente mostra una panoramica della struttura del grafico di comportamento prima della transizione, la configurazione in Organizations e la struttura degli account del grafico di comportamento dopo la transizione.



Designa un account amministratore di Detective per l'organizzazione.

L'account di gestione dell'organizzazione designa un account amministratore di Detective dalla tua organizzazione. Per informazioni, consulta the section called "Designazione dell'account amministratore di Detective".

Per semplificare la transizione, Detective consiglia di scegliere un account amministratore corrente come account amministratore di Detective per l'organizzazione.

Se esiste un account amministratore delegato per Detective in Organizations, è necessario utilizzare tale account o l'account di gestione dell'organizzazione come account amministratore di Detective.

Altrimenti, la prima volta che si designa un account amministratore di Detective diverso dall'account di gestione dell'organizzazione, Detective chiama Organizations per rendere quell'account l'account amministratore delegato di Detective.

Abilitare gli account dell'organizzazione come account membri

L'account amministratore di Detective è l'account amministratore per il grafico di comportamento dell'organizzazione. L'account amministratore di Detective sceglie gli account dell'organizzazione da abilitare come account membri nel grafico di comportamento dell'organizzazione. Per informazioni, consulta the section called “Gestione degli account membri dell'organizzazione”.

Nella pagina Account, l'account amministratore di Detective visualizza tutti gli account dell'organizzazione.

Se l'account amministratore di Detective era già l'account amministratore per un grafico di comportamento, quel grafico diventa il grafico di comportamento dell'organizzazione. Gli account dell'organizzazione che erano già account membri nel grafico di comportamento vengono abilitati automaticamente come account membro. Lo stato degli altri account dell'organizzazione è Non membro.

Gli account dell'organizzazione hanno il tipo Per organizzazione, anche se in precedenza erano account membri per invito.

Gli account membri che non appartengono all'organizzazione hanno il tipo Per invito.

La pagina Gestione dell'account fornisce anche un'opzione, Abilita automaticamente i nuovi account dell'organizzazione, per abilitare automaticamente i nuovi account man mano che vengono aggiunti a un'organizzazione. Per informazioni, consulta the section called “Abilitazione di nuovi account aziendali”. L'opzione è inizialmente disattivata.

Quando l'account amministratore di Detective visualizza per la prima volta la pagina Gestione dell'account, viene visualizzato un messaggio che contiene il pulsante Abilita tutti gli account dell'organizzazione. Quando scegli Abilita tutti gli account dell'organizzazione, Detective completa le seguenti operazioni:

- Abilita tutti gli account dell'organizzazione correnti come account membri.
- Attiva l'opzione per abilitare automaticamente nuovi account dell'organizzazione.

Nell'elenco degli account membri è disponibile anche l'opzione Abilita tutti gli account dell'organizzazione.

Designazione dell'amministratore Detective di un'organizzazione

Nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective gestisce l'appartenenza al grafico di comportamento per tutti gli account dell'organizzazione.

Come viene gestito l'account dell'amministratore del Detective: l'account di gestione dell'organizzazione designa l'account amministratore Detective per l'organizzazione di ogni Regione AWS.

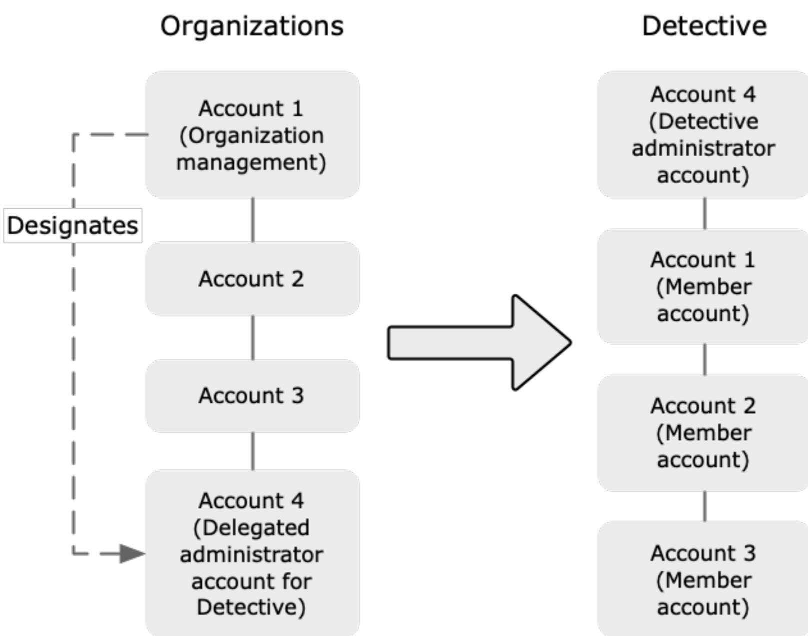
Impostazione dell'account amministratore di Detective come account amministratore delegato: l'account amministratore di Detective diventa anche l'account amministratore delegato per Detective in AWS Organizations. L'eccezione è se l'account di gestione dell'organizzazione si designa come account amministratore del Detective. L'account di gestione dell'organizzazione non può essere un amministratore delegato in Organizations.

Dopo aver impostato l'account amministratore delegato in Organizations, l'account di gestione dell'organizzazione può scegliere solo l'account amministratore delegato o il proprio account come account amministratore di Detective. Ti consigliamo di scegliere l'account amministratore delegato in tutte le Regioni.

Creazione e gestione del grafico del comportamento dell'organizzazione: quando l'account di gestione dell'organizzazione sceglie un account amministratore Detective, Detective crea un nuovo grafico comportamentale per quell'account. Questo grafico di comportamento è il grafico di comportamento dell'organizzazione.

Se l'account amministratore di Detective è un account amministratore per un grafico di comportamento esistente, quel grafico di comportamento diventa il grafico di comportamento dell'organizzazione.

L'account amministratore di Detective sceglie gli account dell'organizzazione da abilitare come account membri nel grafico di comportamento dell'organizzazione.



L'account amministratore di Detective può anche inviare inviti agli account che non appartengono all'organizzazione. Per ulteriori informazioni, consulta the section called “Gestione degli account membri dell'organizzazione” e the section called “Gestione degli account membri invitati”.

Autorizzazioni richieste per configurare l'account amministratore di Detective: per garantire che l'account di gestione dell'organizzazione sia in grado di configurare l'account amministratore di Detective, puoi allegare la politica `AmazonDetectiveOrganizationsAccess` gestita al tuo AWS Identity and Access Management (IAM) entità.

Designazione di un amministratore Detective

L'account di gestione dell'organizzazione può utilizzare la console Detective per designare l'account amministratore di Detective.

Non è necessario abilitare Detective per gestire l'account amministratore di Detective. Puoi gestire l'account amministratore di Detective dalla pagina Abilita Detective.

Enable Detective page (Console)

Per designare un amministratore del Detective dalla pagina Abilita Detective, segui questi passaggi.

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Scegli Avvia.

3. Nel pannello Autorizzazioni richieste per gli account amministratore, concedi le autorizzazioni necessarie all'account che scegli in modo che possa funzionare come amministratore di Detective con accesso completo a tutte le operazioni in Detective. Per operare come amministratore, consigliamo di allegare la policy `AmazonDetectiveFullAccess` al principale.
4. Scegli Allega politica da IAM per visualizzare la politica consigliata direttamente nella IAM console.
5. A seconda che tu disponga o meno delle autorizzazioni nella IAM console, procedi come segue:
   - Se disponi delle autorizzazioni per operare nella IAM console, allega la policy consigliata al principale che usi per Detective.
   - Se non disponi delle autorizzazioni per operare nella IAM console, copia l'Amazon Resource Name (ARN) della policy e forniscilo al tuo IAM amministratore. Possono quindi allegare la policy per tuo conto.
6. In Amministratore delegato, scegli l'account amministratore di Detective.

   Le opzioni disponibili dipendono dal fatto se si dispone di un account amministratore delegato per Detective in Organizations.

   - Se non disponi di un account amministratore delegato per Detective in Organizations, inserisci l'identificatore dell'account per designarlo come account amministratore di Detective.

     Potresti avere già un account amministratore e un grafico di comportamento ottenuti dalla procedura di invito manuale. In tal caso, consigliamo di designare quell'account come account amministratore di Detective.

     Se disponi di un account amministratore delegato in Organizations for Amazon GuardDuty, AWS Security Hub, o Amazon Macie, quindi Detective ti chiederà di selezionare uno di questi account. Puoi anche inserire un account diverso.
   - Se disponi di un account amministratore delegato per Detective in Organizations, ti verrà richiesto di scegliere quell'account o il tuo account. Ti consigliamo di scegliere l'account amministratore delegato in tutte le Regioni.
7. Scegli Delega.

Se hai abilitato Detective o sei un account membro in un grafico di comportamento esistente, allora puoi designare l'account amministratore di Detective dalla pagina Generale.

General page (Console)

Per designare un amministratore Detective dalla pagina Generale, segui questi passaggi.

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Generale.
3. Nel pannello Policy gestite, puoi saperne di più su tutte le policy gestite supportate da Detective. Puoi concedere le autorizzazioni necessarie a un account a seconda delle operazioni che desideri che gli utenti eseguano in Detective. Per operare come amministratore, consigliamo di allegare la policy `AmazonDetectiveFullAccess` al principale.
4. A seconda che disponi o meno delle autorizzazioni nella IAM console, procedi come segue:
   - Se disponi delle autorizzazioni per operare nella IAM console, allega la policy consigliata al principale che usi per Detective.
   - Se non disponi delle autorizzazioni per operare nella IAM console, copia l'Amazon Resource Name (ARN) della policy e forniscilo al tuo IAM amministratore. Possono quindi allegare la policy per tuo conto.

   Le opzioni disponibili dipendono dal fatto se si dispone di un account amministratore delegato per Detective in Organizations.

   - Se non disponi di un account amministratore delegato per Detective in Organizations, inserisci l'identificatore dell'account per designarlo come account amministratore di Detective.

     Potresti avere già un account amministratore e un grafico di comportamento ottenuti dalla procedura di invito manuale. In tal caso, ti consigliamo di designare quell'account come account amministratore di Detective.

     Se disponi di un account amministratore delegato in Organizations for Amazon GuardDuty, AWS Security Hub, o Amazon Macie, quindi Detective ti chiederà di selezionare uno di questi account. Puoi anche inserire un account diverso.

- Se disponi di un account amministratore delegato per Detective in Organizations, ti verrà richiesto di scegliere quell'account o il tuo account. Ti consigliamo di scegliere l'account amministratore delegato in tutte le Regioni.

5. Scegli Delega.

Detective API, AWS CLI

Per designare l'account amministratore del Detective, puoi utilizzare una API chiamata o il AWS Command Line Interface. È necessario utilizzare le credenziali dell'account di gestione dell'organizzazione.

Se disponi già di un account amministratore delegato per Detective nelle organizzazioni, devi scegliere quell'account o il tuo account; ti consigliamo di scegliere l'account amministratore delegato.

Per designare l'account amministratore del Detective (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`EnableOrganizationAdminAccount`operazione. È necessario fornire il AWS identificatore dell'account amministratore di Detective. Per ottenere l'identificatore dell'account, utilizza l'operazione `ListOrganizationAdminAccounts`.
- AWS CLI: Nella riga di comando, esegui il `enable-organization-admin-account`comando.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

Esempio

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Rimozione dell'account amministratore di Detective

L'account di gestione dell'organizzazione può rimuovere l'account amministratore di Detective corrente in una Regione. Quando rimuovi l'account amministratore di Detective, Detective lo rimuove solo dalla Regione corrente. Non modifica l'account amministratore delegato in Organizations.

Quando l'account di gestione dell'organizzazione rimuove l'account amministratore di Detective in una Regione, Detective elimina il grafico di comportamento dell'organizzazione. Detective è disabilitato per l'account amministratore di Detective rimosso.

Per rimuovere l'attuale account amministratore delegato per Detective, si utilizza OrganizationsAPI. Quando si rimuove l'account amministratore delegato per Detective in Organizations, Detective elimina tutti i grafici di comportamento dell'organizzazione in cui l'account amministratore delegato è l'account amministratore di Detective. I grafici di comportamento dell'organizzazione che hanno l'account di gestione dell'organizzazione come account amministratore di Detective non sono interessati.

Console

Dalla console Detective, è possibile rimuovere l'account amministratore di Detective.

Quando rimuovi l'account amministratore di Detective, Detective viene disabilitato per l'account e il grafico di comportamento dell'organizzazione viene eliminato. L'account amministratore di Detective viene rimosso solo nella regione corrente.

> **Important**
> La rimozione di un account amministratore di Detective non influisce sull'account amministratore delegato in Organizations.

Rimuovere l'account amministratore di Detective (pagina Abilita Detective)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Scegli Avvia.
3. In Amministratore delegato, scegli Disabilita Amazon Detective.
4. Nella finestra di dialogo di conferma, inserisci **`disable`** e quindi seleziona Disabilita Amazon Detective.

Rimuovere un account amministratore di Detective (pagina Generale)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Generale.

3. In Amministratore delegato, scegli Disabilita Amazon Detective.
4. Nella finestra di dialogo di conferma, inserisci **`disable`** e quindi seleziona Disabilita Amazon Detective.

Detective API, AWS CLI

Per rimuovere l'account amministratore di Detective, puoi utilizzare una API chiamata o il AWS CLI. È necessario utilizzare le credenziali dell'account di gestione dell'organizzazione.

Quando rimuovi l'account amministratore di Detective, Detective viene disabilitato per l'account e il grafico di comportamento dell'organizzazione viene eliminato.

> **Important**
>
> La rimozione di un account amministratore di Detective non influisce sull'account amministratore delegato in Organizations.

Per rimuovere l'account amministratore di Detective (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`DisableOrganizationAdminAccount`operazione.

  Quando si utilizza il Detective API per rimuovere l'account amministratore del Detective, questo viene rimosso solo nella regione in cui è stata emessa la API chiamata o il comando.
- AWS CLI: Nella riga di comando, esegui il `disable-organization-admin-account`comando.

```
aws detective disable-organization-admin-account
```

Rimozione dell'account amministratore delegato

La rimozione dell'account amministratore di Detective non rimuove automaticamente l'account amministratore delegato in Organizations. Per rimuovere l'account amministratore delegato per Detective, puoi utilizzare OrganizationsAPI.

Quando si rimuove l'account amministratore delegato, vengono eliminati tutti i grafici di comportamento dell'organizzazione in cui l'account amministratore delegato è l'account amministratore di Detective. Disabilita inoltre Detective per l'account in quelle Regioni.

Per rimuovere l'account amministratore delegato (OrganizationsAPI, AWS CLI)

- OrganizzazioniAPI: usa l'`DeregisterDelegatedAdministrator`operazione. È necessario fornire l'identificatore dell'account amministratore di Detective e il principale di servizio per Detective, ovvero `detective.amazonaws.com`.
- AWS CLI: Nella riga di comando, esegui il `deregister-delegated-administrator`comando.

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

Esempio

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --
service-principal detective.amazonaws.com
```

Operazioni disponibili per gli account

Gli account amministratore e gli account membri hanno accesso alle seguenti operazioni di Detective. Nella tabella, i valori hanno i seguenti significati:

- Qualsiasi: l'account può eseguire l'operazione per tutti gli account dello stesso account amministratore di Detective.
- Personale: l'account può eseguire l'operazione solo sul proprio account.
- Trattino (–): l'account non può eseguire l'operazione.

Nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective determina quali account dell'organizzazione abilitare come account membri. Può configurare Detective per abilitare automaticamente nuovi account dell'organizzazione come account membri oppure può abilitare manualmente gli account dell'organizzazione.

Un account amministratore può invitare gli account a diventare account membri in un grafico di comportamento Quando un account membro accetta l'invito ed è abilitato, Amazon Detective inizia a importare ed estrarre i dati dell'account membro in quel grafico di comportamento.

Per i grafici di comportamento diversi dal grafico di comportamento dell'organizzazione, tutti gli account membri sono account invitati.

La tabella seguente riporta le autorizzazioni predefinite per gli account amministratore e membro. Puoi utilizzare IAM politiche personalizzate per limitare ulteriormente l'accesso alle caratteristiche e alle funzioni del Detective.

Azione	Account amministratore (organizzazione)	Account amministratore (invito)	Membro (organizzazione)	Membro (invito)
Visualizzazione degli account	Qualsiasi	Qualsiasi	Personale (visualizza gli account amministratori)	Personale (visualizza gli account amministratori)
Rimozione di un account membro	Qualsiasi Gli account invitati vengono rimossi Gli account dell'orga nizzazione sono dissociati	Qualsiasi	–	Personale
Aggiunta o rimozione dei pacchetti di origini dati facoltative	Qualsiasi (l'impostazione si applica a tutti gli account membri)	Qualsiasi (l'impostazione si applica a tutti gli account membri)	–	–
Disabilitazione di Detective	Personale	Personale	–	–
Visualizz azione dei dati del grafico di comportamento	Qualsiasi	Qualsiasi	–	–

Azione	Account amministratore (organizzazione)	Account amministratore (invito)	Membro (organizzazione)	Membro (invito)
Abilitazione o disabilitazione dei pacchetti di origini dati facoltative	Tutti	Tutti	–	–

Visualizzazione dell'elenco di account

L'account amministratore può utilizzare la console Detective o API visualizzare un elenco di account. L'elenco può includere:

- Account che l'account amministratore ha invitato a partecipare al grafico del comportamento. Questi account hanno un tipo Su invito.
- Per il grafico di comportamento dell'organizzazione, tutti gli account dell'organizzazione. Questi account hanno un tipo Per organizzazione.

I risultati non includono gli account membri invitati che hanno rifiutato un invito o che l'account amministratore ha rimosso dal grafico del comportamento. Include solo gli account con i seguenti stati.

Verifica in corso

Per gli account invitati, Detective sta verificando l'indirizzo e-mail dell'account prima di inviare l'invito.

Per gli account dell'organizzazione, il Detective sta verificando che l'account appartenga all'organizzazione. Detective verifica inoltre che sia stato l'account amministratore di Detective ad abilitare l'account.

Verifica non riuscita

La verifica non è riuscita. L'invito non è stato inviato o l'account dell'organizzazione non è stato abilitato come membro.

Invited (Invitato)

Per gli account invitati. L'invito è stato inviato, ma l'account membro non ha ancora risposto.

Non membro

Per gli account dell'organizzazione nel grafico del comportamento dell'organizzazione. L'account dell'organizzazione non è attualmente un account membro. Non contribuisce con i dati al grafico del comportamento dell'organizzazione.

Abilitato

Per gli account invitati, l'account membro ha accettato l'invito e contribuisce i dati al grafico del comportamento.

Per gli account dell'organizzazione nel grafico del comportamento dell'organizzazione, l'account amministratore di Detective ha abilitato l'account come account membro. L'account contribuisce con i dati al grafico del comportamento dell'organizzazione.

Non abilitato

Per gli account invitati, l'account membro ha accettato l'invito, ma non può essere abilitato.

Per gli account dell'organizzazione nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective ha provato ad abilitare l'account, ma non è stato possibile.

Per gli account invitati, il Detective controlla il numero di account dei membri. Il numero massimo di account membri per un grafico di comportamento è 1.200. Se il grafico del comportamento contiene già 1.200 account membri, non è possibile abilitare nuovi account.

Detective verifica se il volume di dati rientra nella quota di Detective. Il volume di dati che fluiscono in un grafico di comportamento deve essere inferiore al massimo consentito da Detective. Se l'attuale volume importato supera il limite di 10 TB al giorno per il volume di dati del grafico del comportamento, Detective non ti consentirà di aggiungere altri account membro.

Elenco degli account (console)

Puoi usare il AWS Management Console per visualizzare e filtrare il tuo elenco di account.

Visualizzare l'elenco degli account (console)

1. Accedi alla AWS Management Console. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.

2. Nel riquadro di navigazione di Detective, scegli Gestione account.

   L'elenco degli account membri contiene i seguenti account:

   - Il tuo account
   - Account che hai invitato a contribuire con i dati al grafico del comportamento
   - Nel grafico del comportamento dell'organizzazione, tutti gli account dell'organizzazione

   Per ogni account, l'elenco riporta le seguenti informazioni.

   - L'identificatore AWS dell'account.
   - Per gli account dell'organizzazione, il nome dell'account.
   - Il tipo di account (Per invito o Per organizzazione).
   - Per gli account invitati, l'indirizzo e-mail dell'utente root dell'account.
   - Lo stato dell'account.
   - Il volume di dati giornaliero dell'account. Detective non può recuperare il volume di dati per gli account che non sono abilitati come account membri.
   - La data dell'ultimo aggiornamento dello stato dell'account.

Puoi utilizzare le schede nella parte superiore della tabella per filtrare l'elenco in base allo stato dell'account membro. Ogni scheda mostra il numero di account membri corrispondenti.

- Scegli Tutti per visualizzare tutti gli account membri.
- Scegli Abilitato per visualizzare gli account con lo stato Abilitato.
- Scegli Non abilitato per visualizzare gli account con uno stato diverso da Abilitato.

Puoi anche aggiungere altri filtri all'elenco degli account membri.

Aggiungere un filtro all'elenco degli account nel grafico del comportamento (console)

1. Scegli la casella di filtro.
2. Scegli la colonna da utilizzare per filtrare l'elenco:
3. Per la colonna specificata, scegli il valore da utilizzare per il filtro.
4. Per rimuovere un filtro, scegli l'icona x in alto a destra.

5. Per aggiornare l'elenco con le informazioni di stato più recenti, scegli l'icona di aggiornamento in alto a destra.

Elencare gli account dei membri (DetectiveAPI, AWS CLI)

Puoi utilizzare una API chiamata o il AWS Command Line Interface per visualizzare un elenco di account membri nel tuo grafico comportamentale.

Per ottenere il grafico ARN del comportamento da utilizzare nella richiesta, usa l'`ListGraphs`operazione.

Per recuperare un elenco degli account dei membri (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`ListMembers`operazione. Per identificare il grafico del comportamento desiderato, specificate il grafico del comportamentoARN.

  Tieni presente che per il grafico del comportamento dell'organizzazione, `ListMembers` non restituisce gli account dell'organizzazione che non hai abilitato come account membri o che hai dissociato dal grafico del comportamento.
- AWS CLI: alla riga di comando, esegui il comando `list-members`.

  ```
  aws detective list-members --graph-arn <behavior graph ARN>
  ```

  Esempio:

  ```
  aws detective list-members --graph-arn arn:aws:detective:us-
  east-1:111122223333:graph:123412341234
  ```

Per recuperare dettagli su account membri specifici nel tuo grafico comportamentale (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`GetMembers`operazione. Specificate il grafico del comportamento ARN e l'elenco degli identificatori degli account per gli account dei membri.
- AWS CLI: alla riga di comando, esegui il comando `get-members`.

  ```
  aws detective get-members --account-ids <member account IDs> --graph-arn <behavior
   graph ARN>
  ```

Esempio:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Gestione degli account aziendali come account dei membri del Detective

Nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective determina quali account dell'organizzazione abilitare come account membri. Per impostazione predefinita, i nuovi account dell'organizzazione non sono abilitati come account membri. Il loro stato è Non membro. L'account amministratore di Detective può configurare Detective per abilitare automaticamente nuovi account dell'organizzazione come account membri nel grafico di comportamento dell'organizzazione.

L'amministratore del Detective può configurare Detective per abilitare automaticamente i nuovi account dell'organizzazione come account membro. Quando scegli di abilitare automaticamente gli account dell'organizzazione, Detective inizia ad abilitare nuovi account come account membri quando vengono aggiunti all'organizzazione. Detective non abilita gli account dell'organizzazione esistenti che non sono ancora abilitati.

Il Detective può abilitare manualmente gli account dell'organizzazione come account membro, se non si desidera abilitare automaticamente i nuovi account dell'organizzazione. Possono anche abilitare manualmente gli account dell'organizzazione dissociati. L'amministratore di Detective non può abilitare un account dell'organizzazione come account membro se il grafico del comportamento dell'organizzazione ha già un massimo di 1.200 account abilitati. In questo caso, lo stato dell'account dell'organizzazione rimane Non membro.

L'amministratore del Detective può anche dissociare gli account dell'organizzazione dal grafico del comportamento dell'organizzazione. Per interrompere l'importazione di dati da un account dell'organizzazione nel grafico di comportamento dell'organizzazione, puoi dissociare l'account. I dati esistenti per quell'account rimangono nel grafico di comportamento.

Indice

- Dissociazione degli account dell'organizzazione dagli account dei membri del Detective

Attivazione di nuovi account aziendali come account per membri del Detective

L'account amministratore di Detective può configurare Detective per abilitare automaticamente nuovi account dell'organizzazione come account membri nel grafico di comportamento dell'organizzazione.

Quando vengono aggiunti nuovi account all'organizzazione, questi vengono aggiunti all'elenco nella pagina Gestione degli account. Per gli account dell'organizzazione, Tipo è Per organizzazione.

Per impostazione predefinita, i nuovi account dell'organizzazione non sono abilitati come account membri. Il loro stato è Non membro.

Quando scegli di abilitare automaticamente gli account dell'organizzazione, Detective inizia ad abilitare nuovi account come account membri quando vengono aggiunti all'organizzazione. Detective non abilita gli account dell'organizzazione esistenti che non sono ancora abilitati.

Detective può abilitare gli account dell'organizzazione come account membro solo se il numero massimo di account membri per un grafico comportamentale è 1.200. Se il grafico di comportamento contiene già 1.200 account membri, non è possibile abilitare nuovi account.

Console

Sulla pagina Gestione dell'account, l'impostazione Abilita automaticamente i nuovi account dell'organizzazione determina se abilitare automaticamente i nuovi account man mano che vengono aggiunti a un'organizzazione.

Abilitare automaticamente nuovi account dell'organizzazione come account membri

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Attiva l'opzione Abilitare automaticamente i nuovi account dell'organizzazione.

DetectiveAPI/AWS CLI

Per determinare se abilitare automaticamente i nuovi account dell'organizzazione come account membri di Detective, l'account amministratore può utilizzare il Detective API o il AWS Command Line Interface.

Per visualizzare e gestire la configurazione, è necessario fornire il grafico del comportamentoARN. Per ottenere ilARN, utilizzare l'`ListGraphs`operazione.

Visualizzare la configurazione corrente per l'abilitazione automatica degli account dell'organizzazione

- DetectiveAPI: Usa l'`DescribeOrganizationConfiguration`operazione.

  Nella risposta, se i nuovi account dell'organizzazione vengono abilitati automaticamente, `AutoEnable` è `true`.
- AWS CLI: alla riga di comando, esegui il comando `describe-organization-configuration`.

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

  Esempio

```
aws detective describe-organization-configuration --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Abilitare automaticamente nuovi account dell'organizzazione

- DetectiveAPI: Usa l'`UpdateOrganizationConfiguration`operazione. Per abilitare automaticamente nuovi account dell'organizzazione, imposta `AutoEnable` su `true`.
- AWS CLI: alla riga di comando, esegui il comando `update-organization-configuration`.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN>
 --auto-enable | --no-auto-enable
```

  Esempio

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --auto-enable
```

Attivazione degli account dell'organizzazione come account per membri del Detective

Se non abiliti automaticamente i nuovi account dell'organizzazione, puoi abilitarli manualmente. È inoltre necessario abilitare manualmente gli account che sono stati dissociati.

Determinazione se un account può essere abilitato

Non è possibile abilitare un account dell'organizzazione come account membro se il grafico di comportamento dell'organizzazione ha già un massimo di 1.200 account abilitati. In questo caso, lo stato dell'account dell'organizzazione rimane Non membro. L'account non fornisce dati al grafico di comportamento.

Non appena l'account membro può essere abilitato, Detective modifica automaticamente lo stato dell'account membro in Abilitato. Ad esempio, lo stato dell'account membro cambia in Abilitato se l'account amministratore rimuove gli account di altri membri per liberare spazio per un account.

Console

Dalla pagina Gestione degli account, è possibile abilitare gli account dell'organizzazione come account membri.

Abilitare gli account dell'organizzazione come account membri

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Per visualizzare l'elenco degli account che non sono attualmente abilitati, scegli Non abilitato.
4. Puoi selezionare account aziendali specifici o abilitare tutti gli account dell'organizzazione.

   Per abilitare gli account dell'organizzazione selezionati:

   a. Seleziona ogni account dell'organizzazione che desideri abilitare.
   b. Scegli Abilita account.

   Per abilitare tutti gli account dell'organizzazione, scegli Abilita tutti gli account dell'organizzazione.

Detective API/AWS CLI

È possibile utilizzare il Detective API o il AWS Command Line Interface per abilitare gli account dell'organizzazione come account membro nel grafico del comportamento dell'organizzazione. Per ottenere il grafico ARN del comportamento da utilizzare nella richiesta, utilizzate l'`ListGraphs`operazione.

Abilitare gli account dell'organizzazione come account membri

- DetectiveAPI: Usa l'`CreateMembers`operazione. È necessario fornire il graficoARN.

  Per ogni account, specifica l'identificatore dell'account. Gli account dell'organizzazione nel grafico di comportamento dell'organizzazione non ricevono un invito. Non è necessario specificare un indirizzo e-mail o altre informazioni sull'invito.
- AWS CLI: alla riga di comando, esegui il comando `create-members`.

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-
arn <behavior graph ARN>
```

  Esempio

```
aws detective create-members --accounts AccountId=444455556666
 AccountId=123456789012 --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Dissociazione degli account dell'organizzazione dagli account dei membri del Detective

Per interrompere l'importazione di dati da un account dell'organizzazione nel grafico di comportamento dell'organizzazione, puoi dissociare l'account. I dati esistenti per quell'account rimangono nel grafico di comportamento.

Quando si dissocia un account dell'organizzazione, lo stato cambia in Non membro. Detective interrompe l'importazione di dati da quell'account, ma l'account rimane nell'elenco.

Console

Dalla pagina Gestione degli account, è possibile dissociare gli account dell'organizzazione come account membri.

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Per visualizzare l'elenco degli account abilitati, scegli Abilitato.
4. Seleziona la casella di controllo per ogni account da dissociare.
5. Scegli Azioni. Quindi scegli Disabilita account.

   Lo stato dell'account per gli account dissociati cambia in Non membro.

Detective API/AWS CLI

Per ottenere il grafico ARN del comportamento da utilizzare nella richiesta, utilizzate l'`ListGraphs`operazione.

Per dissociare gli account dell'organizzazione dal grafico del comportamento dell'organizzazione

- DetectiveAPI: Usa l'`DeleteMembers`operazione. Specificate il grafico ARN e l'elenco degli identificatori degli account per i quali gli account membri devono dissociarsi.
- AWS CLI: alla riga di comando, esegui il comando `delete-members`.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

  Esempio

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Gestione degli account dei membri invitati in Detective

Un account amministratore di Detective può invitare gli account a diventare account membri nel relativo grafico comportamentale. Un grafico di comportamento può contenere fino a 1.200 account membri. Quando un account membro accetta l'invito ed è abilitato, Amazon Detective inizia a importare ed estrarre i dati dell'account membro in quel grafico di comportamento.

Per invitare singoli account, puoi specificare manualmente gli account dei membri da invitare a contribuire con i loro dati a un grafico comportamentale. Se desideri aggiungere un elenco di account membri, puoi scegliere di fornire un file.csv contenente un elenco di account membri da invitare al tuo grafico comportamentale.

Per i grafici comportamentali diversi dal grafico del comportamento dell'organizzazione, tutti gli account dei membri sono account invitati. L'account amministratore Detective può anche invitare account che non sono account dell'organizzazione al grafico del comportamento dell'organizzazione.

A un livello superiore, la procedura per invitare gli account a contribuire a un grafico di comportamento è la seguente.

1. Per ogni account membro da aggiungere, l'account amministratore fornisce l'identificatore dell' AWS account e l'indirizzo e-mail dell'utente root.
2. Detective verifica che l'indirizzo e-mail sia l'indirizzo e-mail dell'utente root per l'account. Se le informazioni sull'account sono valide, Detective invia l'invito all'account membro.

   Detective non esegue questa convalida né invia inviti via e-mail agli account dei membri nelle seguenti aree geografiche:

   - AWS GovCloud Regione (Stati Uniti orientali)
   - AWS GovCloud Regione (Stati Uniti occidentali)

   Per le altre regioni, puoi `DisableEmailNotification` usare l'CreateMembersoperazione del DetectiveAPI. Se `DisableEmailNotification` è impostato su true, Detective non invierà inviti agli account dei membri. Si tratta di un'impostazione utile per gli account gestiti centralmente.
3. L'account membro accetta o rifiuta l'invito.

   Anche se l'account amministratore non invia e-mail di invito, l'account membro deve comunque rispondere all'invito.
4. Dopo che l'account membro ha accettato l'invito, Detective inizia a inserire i dati dell'account del membro nel grafico del comportamento.
5. Non appena l'account membro può essere abilitato, Detective ne modifica automaticamente lo stato in Abilitato.

   Ad esempio, lo stato dell'account membro cambia in Abilitato se l'account amministratore rimuove gli account di altri membri per liberare spazio per un account.

   Se più di un account non è abilitato, Detective abilita gli account nell'ordine in cui sono stati invitati. Il processo per verificare se abilitare gli account non abilitati viene eseguito ogni ora.

L'account amministratore può anche abilitare gli account manualmente anziché attendere il processo automatico. Ad esempio, l'account amministratore potrebbe voler selezionare gli account da abilitare. Per informazioni su come abilitare un account membro, consultathe section called “Abilitazione di un account membro che non è abilitato”.

Tieni presente che Detective ha iniziato ad abilitare automaticamente gli account che non sono abilitati il 12 maggio 2021. Gli account che non erano abilitati prima di allora non vengono abilitati automaticamente. L'account amministratore li deve abilitare manualmente.

L'account amministratore può rimuovere gli account membri invitati dal grafico di comportamento. Detective non rimuove alcun dato esistente dal grafico di comportamento, che aggrega i dati tra gli account membri.

Indice

Invitare singoli account a visualizzare un grafico comportamentale

Puoi specificare manualmente gli account membri da invitare per contribuire con i loro dati a un grafico di comportamento.

Console

Per selezionare manualmente gli account dei membri da invitare utilizzando la console Detective.

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Scegli Azioni. Quindi scegli Invita account.
4. In Aggiungi account, scegli Aggiungi singoli account.
5. Per aggiungere un account membro all'elenco degli inviti, procedi nel seguente modo.

   a. Scegli Aggiungi account.

   b. Per ID AWS account, inserisci l'ID AWS dell'account.
   c. Per Indirizzo e-mail, immetti l'indirizzo e-mail dell'utente root per l'account.

6. Per rimuovere un account dall'elenco, scegli Rimuovi per quell'account.
7. In Personalizza e-mail di invito, aggiungi contenuti personalizzati da includere nell'e-mail di invito.

   Ad esempio, puoi utilizzare quest'area per fornire le informazioni di contatto. Oppure usalo per ricordare all'account membro che deve allegare la IAM politica richiesta al suo utente o ruolo prima di poter accettare l'invito.
8. La IAMpolitica relativa agli account dei membri contiene il testo della IAM politica richiesta per gli account dei membri. L'e-mail di invito include questo testo della policy. Per copiare il testo della policy, scegli Copia.
9. Seleziona Invite (Invita).

Detective API/AWS CLI

Puoi usare il Detective API o il AWS Command Line Interface per invitare gli account dei membri a contribuire con i loro dati a un grafico del comportamento. Per ottenere il grafico ARN del tuo comportamento da utilizzare nella richiesta, usa l'`ListGraphs`operazione.

Per invitare gli account dei membri a un grafico comportamentale (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`CreateMembers`operazione. È necessario fornire il graficoARN. Per ogni account, specifica l'identificatore dell'account e l'indirizzo e-mail dell'utente root.

  Per non inviare le e-mail di invito agli account membri, imposta `DisableEmailNotification` su true. Per impostazione predefinita, `DisableEmailNotification` è false.

  Se invii le e-mail di invito, puoi facoltativamente fornire un testo personalizzato da aggiungere all'e-mail di invito.
- AWS CLI: alla riga di comando, esegui il comando `create-members`.

  ```
  aws detective create-members --accounts AccountId=<AWS account
   ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --
  message "<Custom message text>"
  ```

  Esempio

```
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."
```

Per indicare di non inviare le e-mail di invito agli account membri, includi `--disable-email-notification`.

```
aws detective create-members --accounts AccountId=<AWS account
 ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --
disable-email-notification
```

Esempio

```
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
```

Invitare un elenco di account membri a un grafico comportamentale

Dalla console Detective, puoi fornire un file `.csv` contenente un elenco di account membri da invitare al tuo grafico di comportamento.

La prima riga nel file è la riga di intestazione. Ogni account viene quindi riportato su una riga separata. Ogni voce dell'account membro contiene l'ID AWS dell'account e l'indirizzo e-mail dell'utente root dell'account.

Esempio:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Quando Detective elabora il file, ignora gli account già invitati, a meno che lo stato dell'account non sia Verifica non riuscita. Questo stato indica che l'indirizzo e-mail fornito per l'account non corrispondeva all'indirizzo e-mail dell'utente root dell'account. In tal caso, Detective elimina l'invito originale e riprova per verificare l'indirizzo e-mail e inviare l'invito.

Questa opzione fornisce anche un modello da utilizzare per creare l'elenco di account.

Invitare gli account membri da un elenco .csv (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Scegli Azioni. Quindi scegli Invita account.
4. In Aggiungi account, scegli Aggiungi da .csv.
5. Per scaricare un file modello da cui lavorare, scegli Scarica modello in formato .csv.
6. Per selezionare il file contenente l'elenco degli account, scegli Scegli il file .csv.
7. In Rivedi gli account membri, verifica l'elenco degli account membri che Detective ha trovato nel file.
8. In Personalizza e-mail di invito, aggiungi contenuti personalizzati da includere nell'e-mail di invito.

   Ad esempio, puoi fornire informazioni di contatto o ricordare all'account membro la IAM politica richiesta.
9. La IAMpolitica relativa agli account dei membri contiene il testo della IAM politica richiesta per gli account dei membri. L'e-mail di invito include questo testo della policy. Per copiare il testo della policy, scegli Copia.
10. Seleziona Invite (Invita).

Aggiungere un elenco di account membri in tutte le regioni

Detective fornisce uno script GitHub Python open source che consente di eseguire le seguenti operazioni:

- Aggiungi un elenco specifico di account membri ai grafici di comportamento di un account amministratore in un elenco specifico di Regioni.
- Se l'account amministratore non dispone di un grafico di comportamento in una Regione, lo script abilita anche Detective e crea il grafico di comportamento in quella Regione.

- Invia le e-mail di invito agli account membri.
- Accetta automaticamente gli inviti per gli account membri.

Per informazioni su come configurare e utilizzare GitHub gli script, vedere. the section called “Script di Amazon Detective Python”

Abilitazione di un account membro che non è abilitato

Dopo che un account membro ha accettato un invito, Amazon Detective verifica il numero di account membri. Il numero massimo di account membri per un grafico di comportamento è 1.200. Se il grafico di comportamento contiene già 1.200 account membri, non è possibile abilitare nuovi account. Se Detective non è in grado di abilitare l'account membro, imposta lo stato dell'account membro su Non abilitato.

Gli account membri che non sono abilitati non contribuiscono con i dati al grafico di comportamento.

Detective abilita automaticamente gli account in quanto il grafico di comportamento è in grado di gestirli.

Puoi anche provare ad abilitare manualmente gli account membri che sono account membri non abilitati. Ad esempio, potresti rimuovere gli account membri esistenti per ridurre il volume di dati. Invece di attendere il processo automatico che abilita gli account, puoi provare ad abilitare gli account membro con stato Non abilitato.

Console

L'elenco degli account membri include un'opzione per abilitare gli account membri selezionati il cui stato è Non abilitato.

Abilitare un account membro che non è abilitato

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. In I miei account membro, seleziona la casella di controllo per ogni account membro da abilitare.

   Puoi abilitare solo gli account membri con lo stato Non abilitato.
4. Scegli Abilita account.

Detective determina se l'account membro può essere abilitato. Se l'account membro può essere abilitato, lo stato cambia in Abilitato.

Detective API/CLI

Puoi utilizzare una API chiamata o abilitare un account AWS Command Line Interface per singolo membro che non è abilitato. Per ottenere il grafico ARN del comportamento da utilizzare nella richiesta, usa l'`ListGraphs`operazione.

Abilitare un account membro che non è abilitato

- DetectiveAPI: Usa l'`StartMonitoringMember`APIoperazione. È necessario fornire il grafico del comportamentoARN. Per identificare l'account membro, utilizza l'identificatore AWS dell'account.
- AWS CLI: Esegui il `start-monitoring-member`comando.

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account ID>
```

Per esempio:

```
start-monitoring-member --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --account-id 444455556666
```

Rimozione degli account dei membri da un grafico comportamentale

L'account amministratore può rimuovere gli account dei membri invitati da un grafico comportamentale in qualsiasi momento.

Detective rimuove automaticamente gli account dei membri che vengono chiusi AWS, ad eccezione delle regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali).

Quando un account membro invitato viene rimosso da un grafico di comportamento, si verifica quanto segue.

- L'account membro viene rimosso da I miei account membro.
- Amazon Detective interrompe l'importazione dei dati dall'account rimosso.

Detective non rimuove alcun dato esistente dal grafico di comportamento, che aggrega i dati tra gli account membri.

Console

Puoi utilizzare il AWS Management Console per rimuovere gli account dei membri invitati dal tuo grafico comportamentale.

Rimuovere gli account membri (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Nell'elenco di account, seleziona la casella di controllo accanto a ciascun account membro da rimuovere.

   Non puoi rimuovere il tuo account dall'elenco.
4. Scegli Azioni. Quindi scegli Disabilita account.

Detective API/CLI

Puoi usare il Detective API o il AWS Command Line Interface per rimuovere gli account dei membri invitati dal tuo grafico del comportamento. Per ottenere il grafico ARN del tuo comportamento da utilizzare nella richiesta, usa l'`ListGraphs`operazione.

Per rimuovere gli account dei membri invitati dal tuo grafico comportamentale (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`DeleteMembers`operazione. Specificate il grafico ARN e l'elenco degli identificatori degli account dei membri da rimuovere.
- AWS CLI: alla riga di comando, esegui il comando `delete-members`.

  ```
  aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
   graph ARN>
  ```

  Esempio:

  ```
  aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
   arn:aws:detective:us-east-1:111122223333:graph:123412341234
  ```

Python script

Detective fornisce uno script open source in GitHub. È possibile utilizzare questo script per rimuovere un elenco specifico di account membri dai grafici di comportamento di un account amministratore in un elenco specifico di Regioni.

Per informazioni su come configurare e utilizzare GitHub gli script, vedere. the section called “Script di Amazon Detective Python”

Per gli account membri: gestione degli inviti e delle iscrizioni al grafico di comportamento

Amazon Detective addebita a ciascun account membro i dati importati per ogni grafico di comportamento a cui contribuisce.

La pagina Gestione dell'account consente agli account membri di visualizzare gli account amministratore per i grafici di comportamento di cui sono membri.

Gli account membri invitati a un grafico di comportamento possono visualizzare e rispondere ai relativi inviti. Possono anche rimuovere il proprio account dal grafico.

Per quanto riguarda il grafico di comportamento dell'organizzazione, gli account dell'organizzazione non controllano se il loro account è un account membro. L'account amministratore di Detective sceglie gli account dell'organizzazione da abilitare o disabilitare come account membri.

Indice

IAMPolitica richiesta per un account membro

Prima che un account membro possa visualizzare e gestire gli inviti, è necessario allegare la IAM politica richiesta al relativo account principale. Il principale può essere un utente o un ruolo esistente oppure puoi crearne uno nuovo da utilizzare per Detective.

Idealmente, all'account amministratore deve essere allegato IAM dall'amministratore la politica richiesta.

La IAM politica dell'account membro consente l'accesso alle azioni dell'account membro in Amazon Detective. L'e-mail di invito a contribuire a un grafico comportamentale include il testo di tale IAM politica.

Per utilizzare questa politica, *<behavior graph ARN>* sostituiscila con il graficoARN.

```
{
  "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":"*"
   }
 ]
}
```

Tieni presente che gli account dell'organizzazione nel grafico di comportamento dell'organizzazione non ricevono inviti e non possono dissociare il loro account dal grafico. Se non appartengono ad altri grafici di comportamento, richiedono solo l'autorizzazione `ListInvitations`. `ListInvitations` consente loro di visualizzare l'account amministratore per il grafico di comportamento. Le autorizzazioni per gestire gli inviti e annullare le iscrizioni si applicano solo alle iscrizioni su invito.

Visualizzazione dell'elenco degli inviti del grafico di comportamento

Dalla console Amazon DetectiveAPI, Detective o AWS Command Line Interface un account membro può vedere gli inviti relativi al grafico del comportamento.

Visualizzazione degli inviti del grafico di comportamento (console)

Puoi visualizzare gli inviti con un grafico comportamentale da. AWS Management Console

Visualizzare gli inviti del grafico di comportamento (console)

1. Accedi alla AWS Management Console. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.

Nella pagina Gestione dell'account, I miei account amministratore contiene gli inviti del grafico di comportamento aperti e accettati nella Regione corrente. Per un account dell'organizzazione, I miei account amministratore contiene anche il grafico di comportamento dell'organizzazione.

Se il tuo account è attualmente nel periodo di prova gratuita, la pagina mostra anche il numero di giorni rimanenti della prova.

L'elenco non contiene gli inviti che hai rifiutato, gli abbonamenti per cui ti sei cancellato o gli abbonamenti rimossi dall'amministratore.

Ogni invito mostra il numero di account amministratore, la data di accettazione dell'invito e lo stato corrente dell'invito.

- Per gli inviti a cui non hai risposto, lo stato è Invitato.
- Per gli inviti che hai accettato, lo stato è Abilitato o Non abilitato.

  Se lo stato è Abilitato, il tuo account contribuisce con i dati al grafico di comportamento.

  Se lo stato è Non abilitato, l'account non fornisce dati al grafico di comportamento.

  Lo stato del tuo account è inizialmente impostato su Non abilitato mentre il Detective verifica se l'hai GuardDuty abilitato e, in tal caso, se il tuo account potrebbe far sì che il volume di dati per il grafico del comportamento superi la quota di Detective.

Se il tuo account non fa aumentare la quota del grafico di comportamento, Detective aggiorna lo stato in Abilitato. Altrimenti, lo stato rimane Non abilitato.

Se il grafico di comportamento è in grado di adattarsi al volume di dati del tuo account, Detective lo aggiorna automaticamente su Abilitato. Ad esempio, l'account amministratore potrebbe rimuovere gli account di altri membri in modo che il tuo account possa essere abilitato. L'account amministratore può anche abilitare l'account manualmente.

Visualizzazione degli inviti con grafico comportamentale (DetectiveAPI, AWS CLI)

Puoi elencare gli inviti del grafico comportamentale del Detective API o del AWS Command Line Interface.

Per recuperare un elenco di inviti aperti e accettati ai grafici comportamentali (Detective,) API AWS CLI

- DetectiveAPI: Usa l'`ListInvitations`operazione.
- AWS CLI: alla riga di comando, esegui il comando `list-invitations`.

```
aws detective list-invitations
```

Risposta a un invito del grafico di comportamento

Dopo aver accettato un invito, il Detective controlla il numero di account dei membri. Il numero massimo di account membri per un grafico di comportamento è 1.200. Se il grafico di comportamento contiene già 1.200 account membri, non è possibile abilitare nuovi account.

Dopo aver accettato l'invito, Detective sarà abilitato nel tuo account. Detective verifica se il volume di dati rientra nella quota di Detective. Il volume di dati che fluiscono in un grafico di comportamento deve essere inferiore al massimo consentito da Detective. Se l'attuale volume importato supera il limite di 10 TB al giorno, non puoi aggiungere altri account e Detective disabiliterà l'ulteriore acquisizione di dati. La console Detective visualizza una notifica per indicare che il volume di dati è troppo grande e lo stato rimane Non abilitato.

Se rifiuti l'invito, questo viene rimosso dal tuo elenco di inviti e Detective non utilizzerà i dati del tuo account nel grafico di comportamento.

Risposta a un invito del grafico di comportamento (console)

Puoi usare il AWS Management Console per rispondere all'e-mail di invito, che include un link alla console Detective. Puoi rispondere solo a un invito con lo stato Invitato.

Rispondere a un invito del grafico di comportamento (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. In I miei account di amministratore, per accettare l'invito e iniziare a contribuire con i dati al grafico di comportamento, scegli Accetta invito.

   Per rifiutare l'invito e rimuoverlo dall'elenco, scegli Rifiuta.

Rispondere a un invito con grafico comportamentale (DetectiveAPI, AWS CLI)

Puoi rispondere agli inviti del grafico comportamentale del Detective API o del AWS Command Line Interface.

Accettare un invito al grafico comportamentale (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`AcceptInvitation`operazione. È necessario specificare il graficoARN.
- AWS CLI: alla riga di comando, esegui il comando `accept-invitation`.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

  Esempio:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Per rifiutare un invito a un grafico comportamentale (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`RejectInvitation`operazione. È necessario specificare il graficoARN.
- AWS CLI: alla riga di comando, esegui il comando `reject-invitation`.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

Esempio:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Rimozione dell'account da un grafico di comportamento

Dopo aver accettato un invito, puoi rimuovere il tuo account da un grafico di comportamento in qualsiasi momento. Quando rimuovi il tuo account da un grafico di comportamento, Amazon Detective interrompe l'importazione dei dati dal tuo account nel grafico di comportamento. I dati esistenti rimangono nel grafico di comportamento.

Solo gli account invitati possono rimuovere il proprio account da un grafico di comportamento. Gli account dell'organizzazione non possono rimuovere il proprio account dal grafico di comportamento dell'organizzazione.

Rimozione dell'account da un grafico di comportamento (console)

Puoi usare il AWS Management Console per rimuovere il tuo account da un grafico comportamentale.

Rimuovere l'account da un grafico di comportamento (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. In I miei account di amministratore, per il grafico di comportamento a cui desideri rinunciare, scegli Abbandona.

Rimuovere il proprio account da un grafico comportamentale (DetectiveAPI, AWS CLI)

Puoi usare il Detective API o il AWS Command Line Interface per rimuovere il tuo account da un grafico comportamentale.

Per rimuovere il tuo account da un grafico comportamentale (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`DisassociateMembership`operazione. È necessario specificare il graficoARN.

- AWS CLI: alla riga di comando, esegui il comando disassociate-membership.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

Esempio:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Effetto delle operazioni dell'account sui grafici di comportamento

Queste operazioni hanno i seguenti effetti sui dati e sull'accesso ad Amazon Detective.

Detective disabilitato

Quando un account amministratore disabilita Detective, si verifica quanto segue:

- Il grafico di comportamento viene rimosso.
- Detective interrompe l'importazione dei dati dall'account amministratore e dagli account membri per quel grafico di comportamento.

Account membro rimosso dal grafico di comportamento

Quando un account membro viene rimosso da un grafico di comportamento, Detective interrompe l'importazione dei dati da quell'account.

I dati esistenti nel grafico di comportamento non vengono modificati.

Per gli account invitati, l'account viene rimosso dall'elenco I miei account membri.

Per gli account dell'organizzazione nel grafico di comportamento dell'organizzazione, lo stato dell'account cambia in Non membro.

L'account del membro lascia l'organizzazione

Quando un account membro lascia un'organizzazione, si verifica quanto segue:

- L'account viene rimosso dall'elenco I miei account membro per il grafico di comportamento dell'organizzazione.

- Detective interrompe l'importazione dei dati dall'account.

I dati esistenti nel grafico di comportamento non vengono modificati.

AWS account sospeso

Quando un account amministratore viene sospeso AWS, l'account perde l'autorizzazione a visualizzare il grafico del comportamento in Detective. Detective smette di importare i dati nel grafico di comportamento.

Quando un account membro viene sospeso AWS, Detective interrompe l'acquisizione dei dati relativi a quell'account.

Dopo 90 giorni, l'account viene chiuso o riattivato. Quando un account amministratore viene riattivato, le relative autorizzazioni di Detective vengono ripristinate. Detective riprende l'importazione dei dati dall'account. Quando un account membro viene riattivato, Detective riprende l'importazione dei dati dall'account.

AWS account chiuso

Quando un AWS account viene chiuso, il Detective risponde alla chiusura come segue.

- Per un account amministratore, Detective elimina il grafico di comportamento.
- Per un account membro, Detective rimuove l'account dal grafico di comportamento.

AWS conserva i dati relativi alla policy dell'account per 90 giorni dalla data di entrata in vigore della chiusura dell'account amministratore. Al termine del periodo di 90 giorni, elimina AWS definitivamente tutti i dati relativi alla politica dell'account.

- Per conservare i risultati per più di 90 giorni, puoi archiviare le policy. Puoi anche utilizzare un'azione personalizzata con una EventBridge regola per archiviare i risultati in un bucket S3.
- Finché AWS conserva i dati della politica, quando riapri l'account chiuso, AWS riassegna l'account come amministratore del servizio e recupera i dati della politica di servizio per l'account.
- Per ulteriori informazioni, consulta Chiusura di un account.

> **Important**
>
> Per i clienti delle regioni: AWS GovCloud (US)

- Prima di chiudere il tuo account, effettua il backup ed elimina le risorse dell'account. Dopo aver chiuso l'account, non avrai più accesso ad essi.

Utilizzo degli script di Detective Python per gestire gli account

Amazon Detective fornisce un set di script Python open source nel repository. GitHub [amazon-detective-multiaccount-scripts](https://github.com/aws-samples/amazon-detective-multiaccount-scripts) Gli script richiedono Python 3.

Puoi utilizzarli per completare le attività seguenti:

- Abilita Detective per un account amministratore in tutte le Regioni.

  Quando abiliti Detective, puoi assegnare i valori dei tag al grafico di comportamento.
- Aggiungi gli account membri ai grafici di comportamento di un account amministratore in tutte le Regioni.
- Facoltativamente, invia le e-mail di invito agli account membri. Puoi anche configurare la richiesta per non inviare e-mail di invito.
- Rimuovi gli account membri dai grafici di comportamento di un account amministratore in tutte le Regioni.
- Disabilita Detective per un account amministratore in tutte le Regioni. Quando un account amministratore disabilita Detective, il grafico di comportamento dell'account amministratore in ciascuna Regione viene disabilitato.

Panoramica dello script `enableDetective.py`

Lo script `enableDetective.py` svolge le seguenti funzioni:

1. Abilita Detective per un account amministratore in ogni Regione specificata, se l'account amministratore non ha già abilitato Detective in quella Regione.

   Quando utilizzi lo script per abilitare Detective, puoi assegnare i valori dei tag al grafico di comportamento.
2. Facoltativamente, invia gli inviti dall'account amministratore agli account membri specificati per ogni grafico di comportamento.

I messaggi e-mail di invito utilizzano il contenuto predefinito dei messaggi e non possono essere personalizzati.

Puoi anche configurare la richiesta per non inviare e-mail di invito.

3. Accetta automaticamente gli inviti per gli account membri.

   Poiché lo script accetta automaticamente gli inviti, gli account membri possono ignorare questi messaggi.

   Ti consigliamo di contattare direttamente gli account membri per avvisarli che gli inviti vengono accettati automaticamente.

Panoramica dello script `disableDetective.py`

Lo script `disableDetective.py` elimina gli account dei membri specificati dai grafici di comportamento dell'account amministratore nelle Regioni specificate.

Fornisce inoltre un'opzione per disabilitare Detective per l'account amministratore nelle Regioni specificate.

Autorizzazioni richieste per gli script

Gli script richiedono un AWS ruolo preesistente nell'account amministratore e in tutti gli account dei membri che aggiungi o rimuovi.

> **Note**
>
> Il nome del ruolo deve essere lo stesso in tutti gli account.

IAMle migliori pratiche consigliate dalla politica consistono nell'utilizzare i ruoli con meno ambito. Per eseguire il flusso di lavoro dello script che prevede la creazione di un grafico, la creazione di membri e l'aggiunta di membri al grafico, le autorizzazioni richieste sono:

- investigatore: CreateGraph
- investigatore: CreateMembers
- investigatore: DeleteGraph

- investigatore: DeleteMembers
- investigatore: ListGraphs
- investigatore: ListMembers
- investigatore: AcceptInvitation

Relazione di attendibilità del ruolo

La relazione di attendibilità tra i ruoli deve consentire all'istanza o alle credenziali locali di assumere il ruolo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Se non disponi di un ruolo comune che includa le autorizzazioni richieste, devi creare un ruolo con almeno tali autorizzazioni in ogni account membro. È inoltre necessario creare il ruolo nell'account amministratore.

Quando crei il ruolo, assicurati di completare le seguenti operazioni:

- Usa lo stesso nome di ruolo in ogni account.
- Aggiungi le autorizzazioni richieste sopra (consigliate) o seleziona la politica AmazonDetectiveFullAccessgestita.
- Aggiungi il blocco di relazioni di attendibilità tra ruoli come discusso in precedenza.

Per automatizzare questo processo, puoi utilizzare il `EnableDetective.yaml` AWS CloudFormation modello. Poiché il modello crea solo risorse globali, può essere eseguito in qualsiasi Regione.

Configurazione dell'ambiente di esecuzione per gli script Python

È possibile eseguire gli script da un'EC2istanza o da un computer locale.

Avvio e configurazione di un'istanza EC2

Un'opzione per eseguire gli script è eseguirli da un'istanza. EC2

Per avviare e configurare un'istanza EC2

1. Avvia un'EC2istanza nel tuo account amministratore. Per informazioni dettagliate su come avviare un'EC2istanza, consulta la sezione Getting Started with Amazon EC2 Linux Instances nella Amazon EC2 User Guide.
2. Allega all'istanza un IAM ruolo con le autorizzazioni necessarie per consentire all'istanza di effettuare chiamate all'`AssumeRole`interno dell'account amministratore.

   Se hai utilizzato il `EnableDetective.yaml` AWS CloudFormation modello, è `EnableDetective` stato creato un ruolo di istanza con un profilo denominato.

   Altrimenti, per informazioni sulla creazione di un ruolo di istanza, consulta il post del blog Sostituisci o collega facilmente un IAM ruolo a un'EC2istanza esistente utilizzando la EC2 console.
3. Installa il software richiesto:
   - APT: `sudo apt-get -y install python3-pip python3 git`
   - RPM: `sudo yum -y install python3-pip python3 git`
   - Boto (versione minima 1.15): `sudo pip install boto3`
4. Clona il repository sull'istanza. EC2

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

Configurazione di un computer locale per eseguire gli script

È inoltre possibile eseguire gli script dal computer locale.

Configurare un computer locale per eseguire gli script

1. Assicurati di aver configurato sul tuo computer locale le credenziali per il tuo account amministratore che dispone dell'autorizzazione per chiamare `AssumeRole`.
2. Installa il software richiesto:

   - Python 3
   - Boto (versione minima 1.15)
   - GitHub script

Piattaforma	Istruzioni di configurazione
Windows	1. Installa Python 3 (https://www.python.org/downloads/windows/). 2. Apri un prompt dei comandi. 3. Per installare Boto, esegui: `pip install boto3` 4. Scarica il codice sorgente dello script da () GitHub . https://github.com/aws-samples/amazon-detective-multiaccount-scripts
Mac	1. Installa Python 3 (https://www.python.org/downloads/mac-osx/). 2. Apri un prompt dei comandi. 3. Per installare Boto, esegui: `pip install boto3` 4. Scarica il codice sorgente dello script da (). GitHub https://github.com/aws-samples/amazon-detective-multiaccount-scripts
Linux	1. Per installare Python 3, esegui uno dei comandi riportati: • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. Per installare Boto, esegui: `sudo pip install boto3`

Piattaforma	Istruzioni di configurazione
	3. Clona il codice sorgente dello script da https://github.com/aws-samples/amazon-detective-multiaccount-scripts.

Creazione di un elenco `.csv` di account membri da aggiungere o rimuovere

Per identificare gli account membro da aggiungere o rimuovere dai grafici di comportamento, fornisci un file `.csv` contenente l'elenco degli account.

Ogni account viene riportato su una riga separata. Ogni voce dell'account membro contiene l'ID AWS dell'account e l'indirizzo e-mail dell'utente root dell'account.

Fai riferimento al file di esempio seguente:

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Esecuzione di `enableDetective.py`

È possibile eseguire lo `enableDetective.py` script da un'EC2istanza o dal computer locale.

Per eseguire **`enableDetective.py`**

1. Copia il `.csv` file nella `amazon-detective-multiaccount-scripts` directory dell'EC2istanza o del computer locale.
2. Passare alla directory `amazon-detective-multiaccount-scripts`.
3. Eseguire lo script `enableDetective.py`.

```
enableDetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
disable_email
```

Quando esegui lo script, sostituisci i seguenti valori:

`administratorAccountID`

L' AWS ID dell'account dell'amministratore.

roleName

Il nome del AWS ruolo da assumere nell'account amministratore e in ogni account membro.

inputFileName

Il nome del file `.csv` contenente l'elenco degli account membri da aggiungere ai grafici di comportamento dell'account amministratore.

tagValueList

(Facoltativo) Un elenco di valori di tag separati da virgole da assegnare a un nuovo grafico di comportamento.

Per ogni valore di tag, il formato è *key*=*value*. Per esempio:

```
--tags Department=Finance,Geo=Americas
```

regionList

(Facoltativo) Un elenco separato da virgole di Regioni in cui aggiungere gli account membri al grafico di comportamento dell'account amministratore. Per esempio:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

L'account amministratore potrebbe non avere già abilitato Detective in una Regione. In tal caso, lo script abilita Detective e crea un nuovo grafico di comportamento per l'account amministratore.

Se non fornisci un elenco di Regioni, lo script agirà su tutte le Regioni supportate da Detective.

`--disable_email`

(Facoltativo) Se inclusa, Detective non invia e-mail di invito agli account membri.

Esecuzione di **`disableDetective.py`**

È possibile eseguire lo `disableDetective.py` script da un'EC2istanza o dal computer locale.

Per eseguire **`disableDetective.py`**

1. Copia i file `.csv` nella directory `amazon-detective-multiaccount-scripts`.

2. Per utilizzare il file `.csv` per eliminare gli account membri elencati dai grafici di comportamento dell'account amministratore in un elenco specificato di Regioni, esegui lo script `disableDetective.py` come segue:

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --disabled_regions regionList
```

3. Per disabilitare Detective per l'account amministratore in tutte le Regioni, esegui lo script `disableDetective.py` con il flag `--delete-master`.

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --disabled_regions regionList --delete_master
```

Quando esegui lo script, sostituisci i seguenti valori:

`administratorAccountID`

L' AWS ID dell'account dell'amministratore.

`roleName`

Il nome del AWS ruolo da assumere nell'account amministratore e in ogni account membro.

`inputFileName`

Il nome del file `.csv` contenente l'elenco degli account membri da rimuovere dai grafici di comportamento dell'account amministratore.

Devi fornire un file `.csv` anche se stai disabilitando Detective.

`regionList`

(Facoltativo) Un elenco separato da virgole di Regioni in cui completare una delle seguenti operazioni:

- Rimuovi gli account membri dai grafici di comportamento dell'account amministratore.
- Se il flag `--delete-master` è incluso, disabilita Detective.

Per esempio:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

Se non fornisci un elenco di Regioni, lo script agirà su tutte le Regioni supportate da Detective.

Integrazione di Amazon Detective con Amazon Security Lake

Amazon Security Lake è un servizio di data lake di sicurezza completamente gestito. Puoi utilizzare Security Lake per centralizzare automaticamente i dati di sicurezza provenienti da AWS ambienti, provider SaaS, fonti locali, fonti cloud e fonti di terze parti in un data lake creato appositamente e archiviato nel tuo account. AWS Security Lake ti aiuta ad analizzare i dati di sicurezza in modo da ottenere un quadro più completo del tuo livello di sicurezza in tutta l'organizzazione. Con Security Lake, puoi anche migliorare la protezione di carichi di lavoro, applicazioni e dati.

Amazon Detective è ora integrato con Security Lake, il che significa che puoi interrogare e recuperare i dati dei log non elaborati archiviati da Security Lake.

Grazie a questa integrazione, puoi raccogliere log ed eventi dalle seguenti origini supportate in modo nativo da Security Lake. Detective supporta fino alla versione sorgente 2 (OCSF 1.1.0).

- AWS CloudTrail gestione degli eventi versione 1.0 e successive
- Amazon Virtual Private Cloud (Amazon VPC) Flow Logs versione 1.0 e successive
- Registro di controllo di Amazon Elastic Kubernetes Service (Amazon EKS) versione 2.0. — Per utilizzare i log di controllo di Amazon EKS come fonte, è necessario `ram:ListResources` aggiungere le autorizzazioni IAM. Per maggiori dettagli, consulta Aggiungere le autorizzazioni IAM richieste al tuo account.

Per i dettagli su come Security Lake converte automaticamente i log e gli eventi provenienti da AWS servizi supportati nativamente nello schema OCSF, consulta la Amazon Security Lake User Guide.

Dopo aver integrato Detective con Security Lake, Detective inizia a estrarre i log non elaborati da Security Lake relativi agli eventi di AWS CloudTrail gestione e ai log di flusso di Amazon VPC. Per ulteriori dettagli, consulta Esecuzione di query sui log non elaborati.

Abilitare l'integrazione di Detective con Security Lake

Per integrare Detective con Security Lake, devi completare i seguenti passaggi.

1. Prima di iniziare

Utilizza un account di gestione di Organizations per designare un amministratore delegato di Security Lake per la tua organizzazione. Assicurati che Security Lake sia abilitato e verifica che Security Lake stia raccogliendo log ed eventi dagli eventi di AWS CloudTrail gestione e dai log di flusso di Amazon Virtual Private Cloud (Amazon VPC).

In linea con la Security Reference Architecture, Detective consiglia di utilizzare un account Log Archive e di non utilizzare un account Security Tooling per l'implementazione di Security Lake.

2. Creazione di un abbonato a Security Lake

   Per utilizzare i log e gli eventi di Amazon Security Lake, devi essere abbonato a Security Lake. Segui questa procedura per concedere l'accesso alle query a un amministratore dell'account Detective.

3. Aggiungere le autorizzazioni richieste AWS Identity and Access Management (IAM) alla tua identità IAM.
   - Aggiungi queste autorizzazioni per creare l'integrazione di Detective con Security Lake:
     - Associa queste autorizzazioni AWS Identity and Access Management (IAM) alla tua identità IAM. Per i dettagli, consulta la sezione Aggiungi le autorizzazioni IAM richieste al tuo account.
     - Aggiungi questa policy IAM al principio IAM che intendi utilizzare per assegnare il ruolo AWS CloudFormation di servizio. Per maggiori dettagli, consulta la sezione Aggiungi permessi al tuo principale IAM.
   - Se hai già integrato Detective con Security Lake, per utilizzare l'integrazione collega queste autorizzazioni (IAM) alla tua identità IAM. Per i dettagli, consulta la sezione Aggiungere le autorizzazioni IAM richieste al tuo account.
4. Accettare l'invito Resource Share ARN e abilitare l'integrazione

Utilizza il AWS CloudFormation modello per configurare i parametri necessari per creare e gestire l'accesso alle query per gli abbonati a Security Lake. Per i passaggi dettagliati per creare uno stack, consulta Creare uno stack utilizzando il modello. AWS CloudFormation Dopo aver creato lo stack, abilita l'integrazione.

Per una dimostrazione di come integrare Amazon Detective con Amazon Security Lake utilizzando la console Detective, guarda il seguente video: Integrazione di Amazon Detective con Amazon Security Lake- How to Setup -->

Prima di iniziare a integrare Detective con Security Lake

Questo argomento descrive i passaggi preliminari come la delega di un amministratore di Security Lake per l'organizzazione, l'attivazione di Security Lake per l'account amministratore di Detective e la verifica che Security Lake stia raccogliendo log ed eventi.

Security Lake si integra AWS Organizations per gestire la raccolta dei log su più account di un'organizzazione. Per utilizzare Security Lake per un'organizzazione, l'account di AWS Organizations gestione deve prima designare un amministratore delegato di Security Lake per l'organizzazione. L'amministratore delegato di Security Lake deve quindi abilitare Security Lake e consentire la raccolta di log ed eventi per gli account membri dell'organizzazione.

Prima di integrare Security Lake con Detective, assicurati che Security Lake sia abilitato per l'account amministratore di Detective. È necessario innanzitutto configurare le impostazioni del data lake e configurare la raccolta dei log abilitando Security Lake tramite la console Security Lake. Per i passaggi dettagliati su come abilitare Security Lake, consulta Nozioni di base nella Guida per l'utente di Amazon Security Lake.

Inoltre, verifica che Security Lake stia raccogliendo log ed eventi dagli eventi di AWS CloudTrail gestione e dai log di flusso di Amazon Virtual Private Cloud (Amazon VPC). Per ulteriori dettagli sulla raccolta dei log in Security Lake, consulta Raccolta di dati dai AWS servizi nella Guida per l'utente di Amazon Security Lake.

Fase 1: Creare un abbonato a Security Lake in Detective

Questo argomento spiega come utilizzare la console Detective per creare un abbonato a Security Lake.

Per utilizzare i log e gli eventi di Amazon Security Lake, devi essere abbonato a Security Lake. Un abbonato può interrogare e accedere ai dati raccolti da Security Lake. Un abbonato con accesso alle query può interrogare AWS Lake Formation le tabelle direttamente in un bucket Amazon Simple Storage Service (Amazon S3) utilizzando servizi come Amazon Athena. Per diventare un abbonato, l'amministratore di Security Lake ti deve fornire un accesso da abbonato che ti consenta di eseguire query sul data lake. Per informazioni su come l'amministratore esegue questa operazione, consulta Creazione di un abbonato con accesso alle query nella Guida per l'utente di Amazon Security Lake.

Segui questi passaggi per creare un abbonato a Security Lake al fine di concedere l'accesso alle query a un account amministratore di Detective.

Creare un abbonato Detective in Security Lake

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, scegli Integrazioni.
3. Nel riquadro degli abbonati di Security Lake, prendi nota dei valori ID account e ID esterno.

   Chiedi all'amministratore di Security Lake di usarli IDs per:

   - Creare un abbonato Detective in Security Lake per tuo conto.
   - Configurare l'abbonato in modo che abbia accesso alle query.
   - Per garantire che l'abbonato della query di Security Lake sia creato con le autorizzazioni di Lake Formation, seleziona Lake Formation come Metodo di accesso ai dati nella console di Security Lake.

   Quando l'amministratore di Security Lake crea un abbonato per tuo conto, Security Lake genera un ARN di condivisione delle risorse Amazon. Chiedi all'amministratore di inviarti questo ARN.
4. Immetti l'ARN di condivisione delle risorse fornito dall'amministratore di Security Lake nel riquadro degli abbonati di Security Lake.
5. Dopo aver ricevuto l'ARN di condivisione delle risorse dall'amministratore di Security Lake, inseriscilo nella casella ARN di condivisione delle risorse nel riquadro degli abbonati di Security Lake.

Passaggio 2: aggiungere le autorizzazioni IAM richieste al tuo account in Detective

Questo argomento spiega i dettagli della politica di autorizzazione AWS Identity and Access Management (IAM) che devi aggiungere alla tua identità IAM.

Per abilitare l'integrazione di Detective con Security Lake, devi allegare la seguente politica di autorizzazioni AWS Identity and Access Management (IAM) alla tua identità IAM.

Collega la seguente policy in linea al ruolo. Se desideri utilizzare il tuo bucket Amazon S3 per archiviare i risultati delle query Athena, sostituisci `athena-results-bucket` con il nome del tuo bucket Amazon S3. Se desideri che Detective generi automaticamente un bucket Amazon S3 per archiviare il risultato delle query Athena, puoi rimuovere tutte le `S3ObjectPermissions` dalla policy IAM.

Se non disponi delle autorizzazioni necessarie per allegare questa policy alla tua identità IAM, contatta il tuo AWS amministratore. Se disponi delle autorizzazioni richieste ma si verifica un problema, consulta Risoluzione dei messaggi di errore di accesso negato nella Guida per l'utente IAM.

```
{
  "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"
        ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetTemplateSummary",
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "securitylake.amazonaws.com"
          ]
```

```
            }
          }
        }
      ]
    }
```

Fase 3: Accettazione dell'invito Resource Share ARN

Questo argomento spiega i passaggi per accettare l'invito Resource Share ARN utilizzando un AWS CloudFormation modello, passaggio obbligatorio prima di abilitare l'integrazione di Detective con Security Lake.

Per accedere ai log dei dati non elaborati da Security Lake, è necessario accettare un invito alla condivisione delle risorse dall'account Security Lake creato dall'amministratore di Security Lake. Sono inoltre necessarie le autorizzazioni AWS Lake Formation per configurare la condivisione delle tabelle tra account. Inoltre, devi creare un bucket Amazon Simple Storage Service (Amazon S3) in grado di ricevere log di query non elaborati.

Nel passaggio successivo, utilizzerai un AWS CloudFormation modello per creare uno stack per: accettare l'invito Resource Share ARN, creare le risorse Crawler di AWS Glue necessarie e AWS Lake Formation concedere le autorizzazioni di amministratore.

Per accettare l'invito Resource Share ARN e abilitare l'integrazione

1. Crea un nuovo CloudFormation stack utilizzando il CloudFormation modello. Per ulteriori dettagli, consulta Creazione di uno stack mediante il modello AWS CloudFormation.
2. Dopo aver finito di creare lo stack, scegli Abilita integrazione per abilitare l'integrazione di Detective con Security Lake.

Creazione di uno stack mediante il modello AWS CloudFormation

Detective fornisce un AWS CloudFormation modello che è possibile utilizzare per impostare i parametri necessari per creare e gestire l'accesso alle query per gli abbonati a Security Lake.

Fase 1: Creare un ruolo AWS CloudFormation di servizio

È necessario creare un ruolo AWS CloudFormation di servizio per creare uno stack utilizzando il AWS CloudFormation modello. Se non disponi delle autorizzazioni necessarie per creare un ruolo di servizio, contatta l'amministratore dell'account amministratore di Detective. Per ulteriori informazioni sul ruolo di servizio AWS CloudFormation , consulta [Ruolo di servizio AWS CloudFormation](#).

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegliere Ruoli e quindi Crea ruolo.
3. In Seleziona tipo di entità attendibile, scegli Servizio AWS .
4. Scegli AWS CloudFormation. Quindi, seleziona Next (Successivo).
5. Inserisci un nome per il ruolo. Ad esempio, `CFN-DetectiveSecurityLakeIntegration`.
6. Collega la seguente policy in linea al ruolo. `<Account ID>`Sostituiscila con l'ID AWS del tuo account.

```
{
    "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/*"
        }
    ]
}
```

Passaggio 2: aggiunta di autorizzazioni al tuo principale IAM.

Avrai bisogno delle seguenti autorizzazioni per creare uno stack utilizzando il ruolo CloudFormation di servizio creato nel passaggio precedente. Aggiungi la seguente policy IAM al principale IAM che intendi utilizzare per passare il CloudFormation ruolo di servizio. Assumerai questo principale IAM per creare lo stack. Se non disponi delle autorizzazioni necessarie per aggiungere la policy IAM, contatta l'amministratore dell'account amministratore di Detective.

> **Note**
>
> Nella seguente policy, il termine `CFN-DetectiveSecurityLakeIntegration` utilizzato si riferisce al ruolo creato nella fase precedente del ruolo di servizio `Creating an AWS CloudFormation`. Se è diverso, modificalo con il nome del ruolo che hai inserito nel passaggio precedente.

```
{
    "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:*"
        }
    ]
}
```

Fase 3: Specificazione di valori personalizzati nella console AWS CloudFormation

1. Vai alla AWS CloudFormation console da Detective.
2. (Facoltativo) Immissione di un Nome stack. Il nome dello stack viene compilato automaticamente. Puoi modificare il nome dello stack con un nome che non sia in conflitto con i nomi degli stack esistenti.
3. Immetti i seguenti parametri:

   - AthenaResultsBucket— Se non inserisci valori, questo modello genera un bucket Amazon S3. Se desideri utilizzare il tuo bucket, inserisci un nome di bucket per memorizzare i risultati della query Athena. Se utilizzi il tuo bucket, assicurati che il bucket si trovi nella stessa Regione dell'ARN di condivisione delle risorse. Se usi il tuo bucket, assicurati che i `LakeFormationPrincipals` scelti dispongano delle autorizzazioni per scrivere e leggere oggetti dal bucket. Per ulteriori informazioni sulle autorizzazioni del bucket, consulta [Risultati della query e query recenti](#) nella Guida per l'utente di Amazon Athena.
   - DTRegion— Questo campo è precompilato. Non modificare i valori in questo campo.
   - LakeFormationPrincipals— Inserisci l'ARN dei principali IAM (ad esempio, l'ARN del ruolo IAM) a cui desideri concedere l'accesso per utilizzare l'integrazione di Security Lake, separati da virgole. Questi potrebbero essere i tuoi analisti e ingegneri della sicurezza che utilizzano Detective.

     Puoi utilizzare solo i principali IAM a cui hai precedentemente associato le autorizzazioni IAM nel passaggio [`Step 2: Add the required IAM permissions to your account`]
   - ResourceShareARN — Questo campo è precompilato. Non modificare i valori in questo campo.
4. Autorizzazioni

   Ruolo IAM: seleziona il ruolo creato nella fase `Creating an AWS CloudFormation Service Role`. Facoltativamente, puoi lasciarlo vuoto se il ruolo IAM dispone di tutte le autorizzazioni richieste nella fase `Creating an AWS CloudFormation Service Role`.

5. Controlla tutte le caselle Confermo, quindi fai clic sul pulsante Crea stack. Per maggiori dettagli, consulta le seguenti risorse IAM che verranno create.

```
* ResourceShareAcceptorCustomResourceFunction
    - ResourceShareAcceptorLambdaRole
    - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
    - SsmParametersLambdaRole
    - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
    - GlueDatabaseLambdaRole
    - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
    - GlueTablesLambdaRole
    - GlueTablesLogsAccessPolicy
```

Fase 4: Aggiungere la policy dei bucket di Amazon S3 ai principi IAM in `LakeFormationPrincipals`

(Facoltativo) Se consenti a questo modello di generare automaticamente `AthenaResultsBucket` per tuo conto, devi collegare la seguente policy ai principali IAM in `LakeFormationPrincipals`.

```
{
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}
```

Sostituisci `athena-results-bucket` con il nome. `AthenaResultsBucket` Lo si `AthenaResultsBucket` può trovare sulla AWS CloudFormation console:

1. Apri la AWS CloudFormation console in https://console.aws.amazon.com/cloudformazione.
2. Fai clic sullo stack.

3. Seleziona la scheda Risorse.
4. Cerca l'ID logico `AthenaResultsBucket` e copiane l'ID fisico.

Modifica della configurazione dell'integrazione di Detective

Se desideri modificare uno qualsiasi dei parametri che hai usato per integrare Detective con Security Lake, puoi modificarli e quindi abilitare nuovamente l'integrazione. Puoi modificare il AWS CloudFormation modello per riattivare questa integrazione per i seguenti scenari:

- Per aggiornare l'abbonamento a Security Lake, puoi creare un nuovo abbonato oppure l'amministratore di Security Lake può aggiornare l'origine dati per l'abbonamento esistente.
- Specificare un bucket Amazon S3 diverso in cui archiviare i log di query non elaborati.
- Specificare principali di Lake Formation differenti.

Quando riabiliti l'integrazione di Detective con Security Lake, puoi modificare l'ARN di condivisione delle risorse e visualizzare le autorizzazioni IAM. Per modificare le autorizzazioni IAM, puoi accedere alla console IAM da Detective. Puoi anche modificare i valori che hai inserito in precedenza nel AWS CloudFormation modello. È necessario eliminare lo CloudFormation stack esistente e ricrearlo per riattivare l'integrazione.

Riabilitare l'integrazione di Detective con Security Lake

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, scegli Integrazioni.
3. Puoi modificare l'integrazione utilizzando uno di questi passaggi:
   - Nel riquadro Security Lake, scegli Modifica.
   - Nel riquadro Security Lake, scegli Visualizza. Nella pagina della vista, scegli Modifica.
4. Inserisci un nuovo ARN di condivisione delle risorse per accedere alle origini dati in una Regione.
5. Se desideri modificare le autorizzazioni IAM, visualizza le autorizzazioni IAM correnti e passa alla console IAM.
6. Modifica i valori nel CloudFormation modello.
   1. Elimina lo stack esistente prima di crearne uno nuovo. Se non elimini lo stack esistente, la creazione di un nuovo stack nella stessa Regione avrà esito negativo. Per ulteriori dettagli, consulta Eliminazione di una pila CloudFormation .

1. Crea una nuova CloudFormation pila. Per ulteriori dettagli, consulta [Creazione di uno stack mediante il modello AWS CloudFormation](#).

7. Scegli Abilita integrazione.

AWS Regioni supportate per l'integrazione di Detective con Security Lake

Puoi integrare Detective con Security Lake nelle seguenti AWS regioni.

Nome della regione	Regione	Endpoint	Protocollo;
Stati Uniti orientali (Ohio)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
US West (N. California)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
Asia Pacifico (Mumbai)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo;
Asia Pacifico (Tokyo)	ap-northe ast-1	securitylake.ap-northeast-1 .amazonaws.com	HTTPS
Canada (Central)	ca-central-1	securitylake.ca-central-1.a mazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	securitylake.eu-central-1.a mazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	securitylake.eu-west-1.amaz onaws.com	HTTPS
Europe (London)	eu-west-2	securitylake.eu-west-2.amaz onaws.com	HTTPS
Europe (Paris)	eu-west-3	securitylake.eu-west-3.amaz onaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	securitylake.eu-north-1.ama zonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	securitylake.sa-east-1.amaz onaws.com	HTTPS

Query sui log non elaborati in Detective

Dopo aver integrato Detective con Security Lake, Detective inizia a estrarre i log non elaborati da Security Lake relativi agli eventi di AWS CloudTrail gestione e ai log di flusso di Amazon Virtual Private Cloud (Amazon VPC).

> **Note**
>
> Non sono previsti costi supplementari per le query sui log non elaborati in Detective. I costi di utilizzo per altri AWS Servizi, incluso Amazon Athena, si applicano ancora alle tariffe pubblicate.

AWS CloudTrail gli eventi di gestione sono disponibili per i seguenti profili:

- AWS conto
- AWS utente
- AWS ruolo
- AWS ruolo Sessione
- EC2 Istanza Amazon
- Bucket Amazon S3
- Indirizzo IP
- Cluster Kubernetes
- Pod Kubernets
- Soggetto Kubernets
- Ruolo IAM
- Sessione come ruolo IAM
- Utente IAM

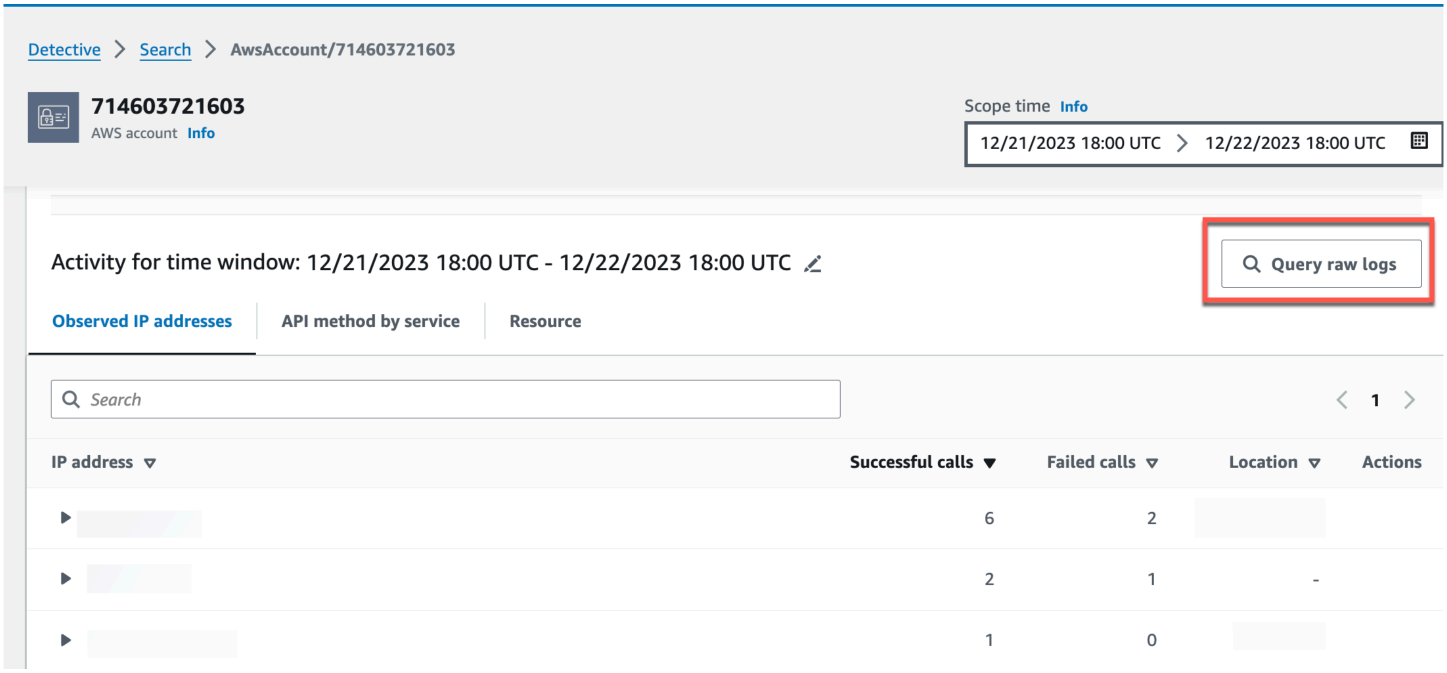
I FLow log di Amazon VPC sono disponibili per i seguenti profili:

- EC2 Istanza Amazon
- Pod Kubernetes

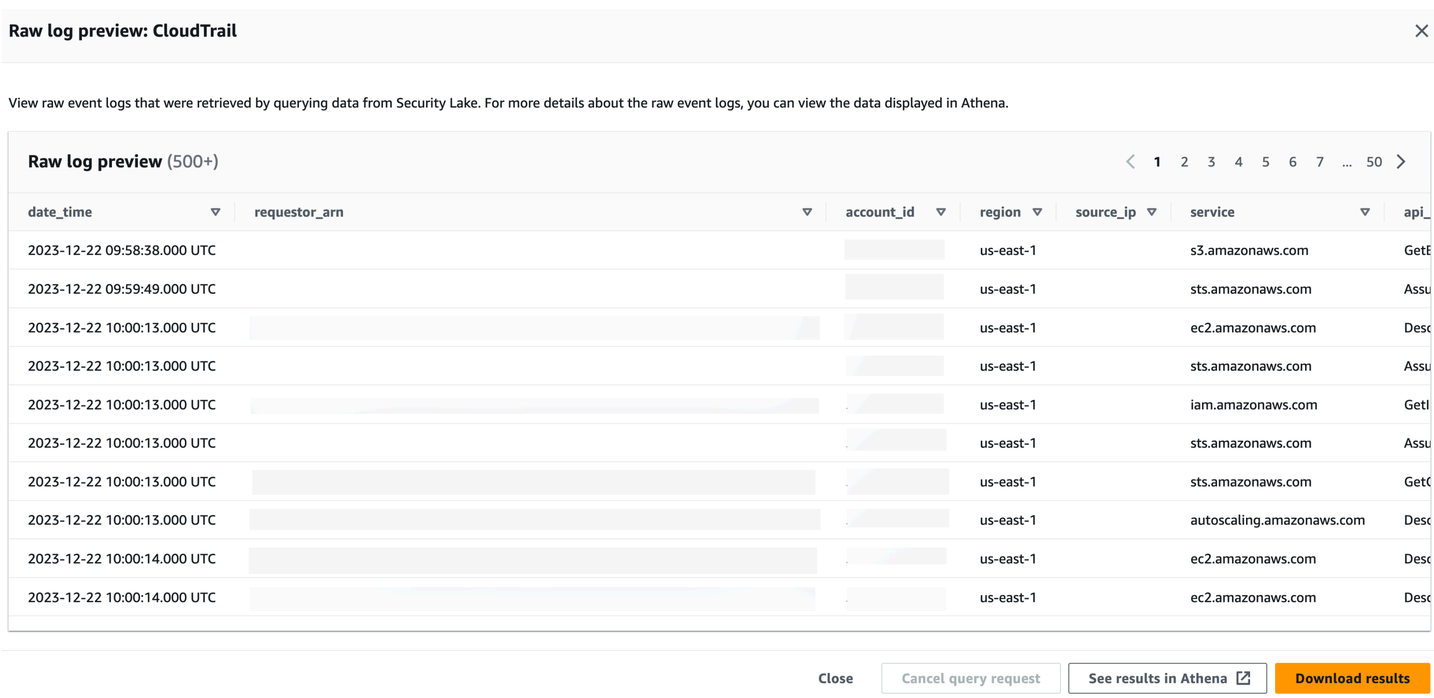
Per una dimostrazione di come integrare Amazon Detective con Amazon Security Lake utilizzando la console Detective, guarda il seguente video: [Integrazione di Amazon Detective con Amazon Security Lake- How to Use]() -->

Per eseguire query sui log non elaborati per un account AWS

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel pannello di navigazione, scegli Ruoli e cerca un `AWS account.`
3. Nella sezione Volume globale delle chiamate API, scegli Visualizza i dettagli per il periodo di validità.
4. Da qui, puoi iniziare a interrogare i log non elaborati.



Nella tabella di anteprima dei log non elaborati, è possibile visualizzare i log e gli eventi recuperati interrogando i dati da Security Lake. Per maggiori dettagli sui log degli eventi non elaborati, puoi visualizzare i dati visualizzati in Amazon Athena.



Dalla tabella Interroga log non elaborati, puoi annullare la richiesta di query, visualizzare i risultati in Amazon Athena e scaricare i risultati come file con valori separati da virgole (.csv).

Se vedi i log in Detective ma la query non ha prodotto risultati, ciò potrebbe accadere per i seguenti motivi.

- I log non elaborati possono diventare disponibili in Detective prima di essere visualizzati nelle tabelle di log di Security Lake. Riprova più tardi.
- È possibile che in Security Lake manchino dei log . Se hai atteso per un periodo di tempo prolungato, significa che i log non sono presenti in Security Lake. Contatta l'amministratore di Security Lake per risolvere il problema.

Esempi

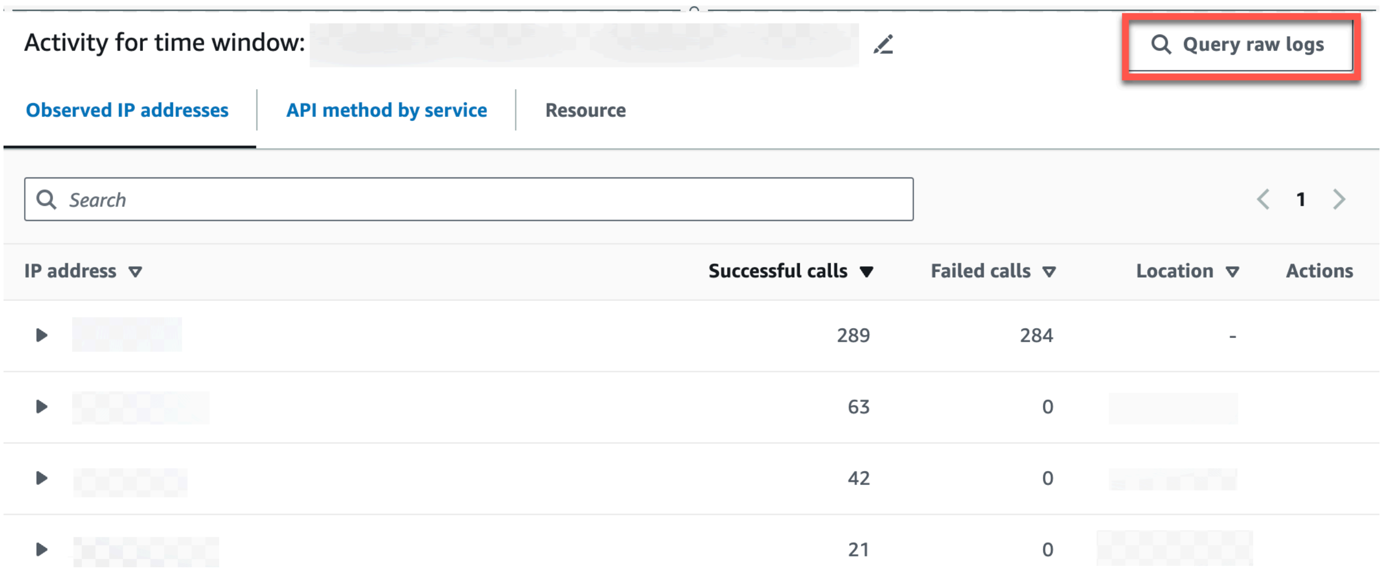
- [Interrogazione dei log non elaborati per un ruolo AWS]
- [Interrogazione di log non elaborati per un cluster Amazon EKS]
- [Interrogazione di log non elaborati per un'istanza Amazon EC2]

Interrogazione dei log non elaborati per un ruolo AWS

Se vuoi comprendere l'attività di un AWS ruolo in una nuova geolocalizzazione, puoi farlo all'interno della console Detective.

Per eseguire query sui log non elaborati per un ruolo AWS

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Dalla pagina Detective Summary, sezione Geolocalizzazioni appena osservate, annota il AWS ruolo.
3. Nel pannello di navigazione, scegli Ruoli e cerca `AWS role`.
4. Per il AWS ruolo, espandi la risorsa per visualizzare le chiamate API specifiche emesse da quell'indirizzo IP da quella risorsa.
5. Scegli l'icona a forma di lente di ingrandimento accanto alla chiamata API che desideri esaminare per aprire la tabella Anteprima dei log non elaborati.

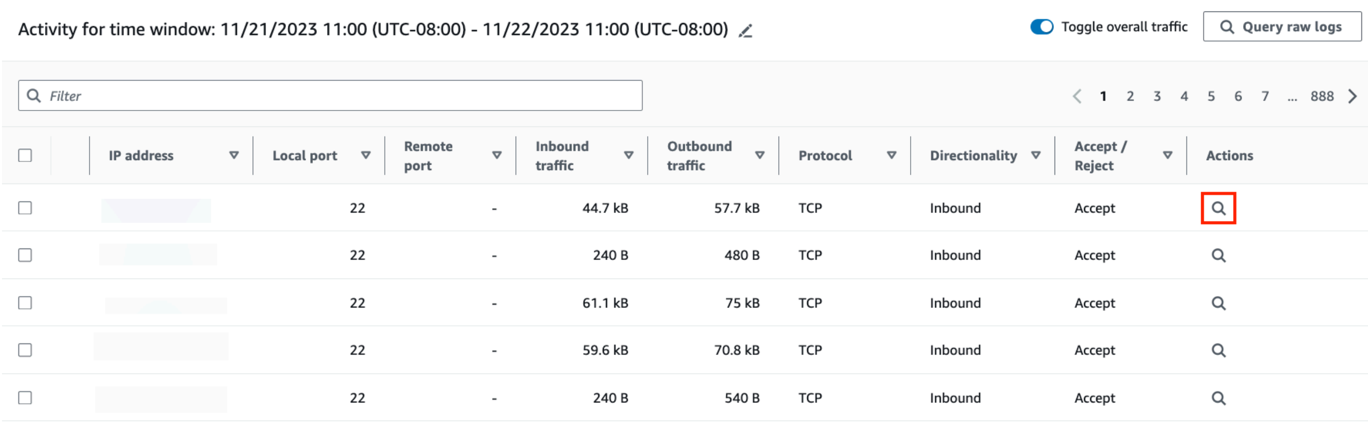


Interrogazione di log non elaborati per un cluster Amazon EKS

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Dalla pagina Detective Summary, sezione Cluster di container con il maggior numero di pod creati, accedi a un cluster Amazon EKS.
3. Nella pagina dei dettagli del cluster Amazon EKS, seleziona la scheda Attività dell'API Kubernets.
4. Nella sezione Attività complessiva dell'API Kubernets che coinvolge questo cluster Amazon EKS, scegli Visualizza dettagli per l'ambito temporale.
5. Da qui, puoi iniziare a interrogare i log non elaborati.

Interrogazione di log non elaborati per un'istanza Amazon EC2

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel pannello di navigazione, scegli Ruoli e cerca un `Amazon EC2 instance`.
3. Nella sezione Volume complessivo del flusso VPC, scegli l'icona a forma di lente di ingrandimento accanto alla chiamata API che desideri esaminare per aprire la tabella Anteprima dei log non elaborati.
4. Da qui, puoi iniziare a interrogare i log non elaborati.



Nella tabella di anteprima dei log non elaborati, è possibile visualizzare i log e gli eventi recuperati interrogando i dati da Security Lake. Per maggiori dettagli sui log degli eventi non elaborati, puoi visualizzare i dati visualizzati in Amazon Athena.

Dalla tabella Interroga log non elaborati, puoi annullare la richiesta di query, visualizzare i risultati in Amazon Athena e scaricare i risultati come file con valori separati da virgole (.csv).

Disattivazione dell'integrazione di Detective con Security Lake

Se disabiliti l'integrazione di Detective con Security Lake, non potrai più interrogare i dati di log ed eventi da Security Lake.

Disabilitare l'integrazione di Detective con Security Lake

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, scegli Integrazioni.
3. Elimina lo stack esistente. Per ulteriori dettagli, consulta Eliminazione di una pila CloudFormation .
4. Nel riquadro Disabilita integrazione Security Lake, scegli Disabilita.

Eliminazione di una pila CloudFormation

Se non elimini lo stack esistente, la creazione di un nuovo stack nella stessa Regione avrà esito negativo. È possibile eliminare uno CloudFormation stack utilizzando la CloudFormation console o la AWS CLI.

Per eliminare lo AWS CloudFormation stack (Console)

1. Apri la AWS CloudFormation console in https://console.aws.amazon.com/cloudformation.
2. Nella pagina Stacks della CloudFormation console, seleziona lo stack che desideri eliminare. Lo stack deve essere attualmente in esecuzione.
3. Nel riquadro dei dettagli dello stack, scegliere Delete (Elimina).
4. Selezionare Delete stack (Elimina stack) quando richiesto.

> **Note**
>
> Una volta iniziata, l'operazione di eliminazione dello stack non può essere interrotta. Lo stack procede allo stato `DELETE_IN_PROGRESS`.

Dopo l'eliminazione dello stack, lo stack sarà nello stato `DELETE_COMPLETE`.

Risoluzione dei problemi relativi agli errori di eliminazione dello stack

Se visualizzi un errore di autorizzazione nel messaggio `Failed to delete stack` dopo aver fatto clic `Delete` sul pulsante, il tuo ruolo IAM non dispone dell' CloudFormation autorizzazione per eliminare uno stack. Contatta l'amministratore del tuo account per eliminare lo stack.

Per eliminare lo CloudFormation stack (AWS CLI)

Immettete il seguente comando nell' AWS interfaccia CLI:

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
      arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

`CFN-DetectiveSecurityLakeIntegration` è il ruolo di servizio creato nella fase `Creating an AWS CloudFormation Service Role`.

Previsione e monitoraggio dei costi del Detective

Per aiutarti a tenere traccia delle tue attività di Detective, la pagina Utilizzo mostra la quantità di dati importati e il costo previsto.

- Per gli account amministratore, la pagina Utilizzo mostra il volume dei dati e il costo previsto nell'intero grafico di comportamento.
- Per gli account membri, la pagina Utilizzo mostra il volume di dati e il costo previsto per l'account in base ai grafici del comportamento a cui contribuiscono.

Detective supporta anche AWS CloudTrail la registrazione.

Indice

Informazioni sulla versione di prova gratuita per i grafici di comportamento

Amazon Detective offre una prova gratuita di 30 giorni per ogni account in ogni Regione. La prova gratuita per un account inizia la prima volta che si verifica una delle seguenti azioni.

- Un account abilita Detective manualmente e diventa l'account amministratore per un grafico di comportamento.
- Un account è designato come account amministratore di Detective per un'organizzazione in AWS Organizations e ha Detective abilitato per la prima volta.
- Se l'account amministratore di Detective aveva già attivato Detective prima di essere designato, l'account non avvia una nuova prova gratuita di 30 giorni.
- Un account accetta un invito a diventare un account membro in un grafico di comportamento ed è abilitato come account membro.
- Un account dell'organizzazione viene abilitato come account membro dall'account amministratore di Detective.

La prova gratuita dura 30 giorni da quel momento. All'account non viene addebitato alcun dato elaborato durante quel periodo. Al termine del periodo di prova, Detective inizia a fatturare all'account i dati con cui contribuisce ai grafici di comportamento. Per ulteriori informazioni su come tenere traccia dell'attività di Detective, monitorare l'utilizzo e visualizzare i costi previsti, consulta Previsione e monitoraggio dei costi del Detective. Per ulteriori informazioni sui prezzi, consulta Prezzi di Detective.

Lo stesso periodo di 30 giorni viene utilizzato per tutti i grafici di comportamento della Regione. Ad esempio, un account è abilitato come account membro per un grafico di comportamento. Inizia la prova gratuita di 30 giorni. Dopo 10 giorni, l'account viene abilitato per un secondo grafico di comportamento nella stessa Regione. Per il secondo grafico di comportamento, l'account riceve 20 giorni di dati gratuiti.

La versione di prova gratuita offre diversi vantaggi:

- Gli account amministratore possono esplorare le caratteristiche e le funzionalità di Detective per verificarne il valore.
- Gli account amministratore e gli account membri possono monitorare la quantità di dati e il costo stimato prima che Detective inizi a fatturarli. Consulta the section called “Utilizzo e costi dell'account amministratore” e the section called “Monitoraggio dell'utilizzo dell'account membro”.

Versione di prova gratuita per origini dati facoltative

Detective offre una prova gratuita di 30 giorni anche per le origini dati facoltative. Questa versione di prova gratuita è separata dalla versione di prova gratuita fornita per le origini dati principali di Detective quando Detective viene abilitato per la prima volta.

> **Note**
>
> Se un cliente disabilita un pacchetto di origini dati opzionale entro 7 giorni dall'abilitazione, Detective esegue un ripristino automatico una tantum della versione di prova gratuita per quel pacchetto di origini dati, se viene nuovamente abilitato.

Per abilitare o disabilitare un'origine dati facoltativa, consulta Tipi di origini dati facoltativi in Detective.

Monitoraggio dell'utilizzo di un account amministratore di Detective

Amazon Detective fattura a ciascun account i dati utilizzati in ogni grafico di comportamento a cui appartiene l'account. Detective applica una tariffa fissa a più livelli per GB per tutti i dati indipendentemente dall'origine.

Per gli account amministratore, la pagina Utilizzo della console di Detective consente di visualizzare il volume di dati importati per origine dati o per account nei 30 giorni precedenti. Gli account amministratore visualizzano anche un costo previsto per un periodo tipico di 30 giorni per il rispettivo account e per l'intero grafico di comportamento.

Visualizzazione delle informazioni sull'utilizzo di Detective

1. Accedi alla AWS Management Console. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Utilizzo.
3. Scegli una scheda per selezionare tra la visualizzazione dell'utilizzo per origine dati o per account.

Volume di dati importati per ogni account

Volume acquisito per account membro riporta gli account attivi nel grafico di comportamento. Non riporta gli account dei membri che sono stati rimossi.

Per ogni account, l'elenco dei volumi importati fornisce le seguenti informazioni.

- L'identificatore AWS dell'account e l'indirizzo e-mail dell'utente root.
- La data in cui l'account ha iniziato a fornire dati al grafico di comportamento.

  Per l'account amministratore, questa è la data in cui l'account ha abilitato Detective.

  Per gli account membro, questa è la data in cui un account è stato abilitato come account membro dopo aver accettato l'invito.
- Il volume di dati importati dall'account nei 30 giorni precedenti. Il totale include tutti i tipi di origine.
- Se l'account si trova nel periodo di prova gratuito. Per gli account che si trovano nel periodo di prova gratuito, l'elenco mostra il numero di giorni rimanenti.

Se nessuno degli account è nel periodo di prova gratuito, la colonna relativa allo stato della prova gratuita non viene visualizzata.

Costi previsti per il grafico di comportamento

Costo previsto di questo account mostra il costo previsto per 30 giorni di dati per l'account amministratore. Il costo previsto si basa sul volume medio giornaliero per ogni account amministratore.

> **Important**
>
> Questo importo è solo un costo previsto. Proietta il costo totale dei dati dell'account amministratore per un periodo di tempo tipico di 30 giorni. Si basa sull'utilizzo dei 30 giorni precedenti. Per informazioni, consulta the section called "Come Detective calcola il costo previsto".

Costo previsto per il grafico di comportamento

Costo previsto di tutti gli account mostra un costo mostra un costo totale previsto per 30 giorni di dati per l'intero grafico di comportamento. Il costo previsto si basa sul volume medio giornaliero per ogni account.

> **Important**
>
> Questo importo è solo un costo previsto. Proietta il costo totale dei dati del grafico di comportamento per un periodo di tempo tipico di 30 giorni. Si basa sull'utilizzo dei 30 giorni precedenti. Il costo previsto non include gli account membri che sono stati rimossi dal grafico di comportamento. Per informazioni, consulta the section called "Come Detective calcola il costo previsto".

Volume di dati importati dai pacchetti di origine

Seleziona Per pacchetto sorgente per visualizzare il volume di dati importati elencato dai diversi pacchetti sorgente abilitati nel grafico di comportamento.

Tutti gli account possono visualizzare questi dati per i propri account. Un account amministratore può visualizzare pannelli aggiuntivi che elencano l'utilizzo per pacchetto sorgente per ciascun membro. Non riporta gli account dei membri che sono stati rimossi.

Core Detective

I pannelli principali di Detective mostrano il volume di dati acquisiti dalle fonti principali di Detective (CloudTrail log, log di VPC flusso e GuardDuty risultati) negli ultimi 30 giorni.

Log di verifica EKS

EKSi pannelli dei registri di controllo mostrano il volume di dati acquisiti dalle fonti dei registri di EKS controllo negli ultimi 30 giorni. I pannelli per questo pacchetto sorgente sono disponibili solo se i log di EKS controllo sono abilitati per il grafico del comportamento.

Monitoraggio dell'utilizzo di un account membro Detective

Amazon Detective fattura a ciascun account i dati utilizzati in ogni grafico di comportamento a cui appartiene l'account. Detective applica una tariffa fissa a più livelli per GB per tutti i dati indipendentemente dall'origine.

Per gli account membri, la pagina Utilizzo mostra il volume di dati e il costo previsto per 30 giorni solo per quell'account.

Visualizzazione delle informazioni sull'utilizzo di Detective

1. Accedi alla AWS Management Console. Quindi apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Utilizzo.

Volume importato per ogni grafico di comportamento

Volume acquisito di questo account riporta i grafici del comportamento a cui contribuisce l'account membro. Non include gli abbonamenti per cui ti sei cancellato o gli abbonamenti rimossi dall'account amministratore.

Per ciascun grafico del comportamento, l'elenco include le seguenti informazioni.

- Il numero di account dell'account amministratore

- Il volume di dati importati dall'account membro nei 30 giorni precedenti. Il totale include tutti i tipi di origine.
- La data in cui l'account membro è stato abilitato per il grafico di comportamento.

Costo previsto nei grafici del comportamento

Costo previsto di questo account mostra il costo previsto per 30 giorni di dati per l'account membro in tutti i grafici del comportamento a cui contribuisce. Il costo previsto si basa sul volume medio giornaliero per ogni account membro.

> **Important**
>
> Questo importo è solo un costo previsto. Proietta il costo totale dei dati dell'account amministratore per un periodo di tempo tipico di 30 giorni. Si basa sull'utilizzo dei 30 giorni precedenti. Per informazioni, consulta the section called “Come Detective calcola il costo previsto”.

Come Amazon Detective calcola il costo previsto

Per calcolare i valori di costo previsti visualizzati nella pagina Utilizzo, Detective effettua le seguenti operazioni.

1. Per ottenere il costo previsto per un singolo account in un grafico del comportamento, Detective effettua le seguenti operazioni.
   a. Calcola il volume medio giornaliero. Aggiunge il volume di dati di tutti i giorni attivi e quindi lo divide per il numero di giorni in cui l'account è stato attivo.

      Se l'account è stato abilitato più di 30 giorni fa, il numero di giorni è 30. Se l'account è stato abilitato meno di 30 giorni fa, allora è il numero di giorni trascorsi dalla data di accettazione.

      Ad esempio, se l'account è stato abilitato 12 giorni fa, Detective aggiunge il volume importato per quei 12 giorni e poi lo divide per 12.
   b. Moltiplica la media giornaliera dell'account per 30. Si tratta dell'utilizzo previsto per 30 giorni dell'account.
   c. Utilizza il modello di prezzo corrispondente per calcolare il costo previsto per 30 giorni per l'utilizzo previsto per 30 giorni.

2. Per ottenere il costo totale previsto per un grafico di comportamento, Detective effettua le seguenti operazioni:
    a. Combina l'utilizzo previsto per 30 giorni di tutti gli account nel grafico di comportamento.
    b. Utilizza il modello di prezzo corrispondente per calcolare il costo previsto per 30 giorni per l'utilizzo totale previsto per 30 giorni.
3. Per ottenere il costo totale previsto per un account membro tra grafici del comportamento, Detective effettua le seguenti operazioni:
    a. Combina l'utilizzo previsto per 30 giorni di tutti gli account nel grafico del comportamento.
    b. Utilizza il modello di prezzo corrispondente per calcolare il costo previsto per 30 giorni per l'utilizzo totale previsto per 30 giorni.
4. Se utilizzi un Amazon VPC condiviso, Detective calcola il costo previsto in base all'attività di monitoraggio. Consigliamo di esaminare i costi previsti per le indagini specifiche dell'ambiente.
    a. Se un account membro di Detective dispone di un Amazon VPC condiviso e ci sono altri account non Detective che utilizzano il VPC condiviso, Detective monitorerà tutto il traffico proveniente da quel VPC. L'utilizzo e il costo aumenteranno e Detective fornirà la visualizzazione di tutto il flusso di traffico all'interno del VPC.
    b. Se hai un'istanza EC2 all'interno di un Amazon VPC condiviso e il proprietario condiviso non è un membro di Detective, Detective non monitorerà alcun traffico proveniente dal VPC e l'utilizzo e i costi diminuiranno. Se desideri visualizzare il flusso di traffico all'interno del VPC, devi aggiungere il proprietario dell'Amazon VPC come membro del grafico di Detective.

Sicurezza in Amazon Detective

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro.

  I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS.

  Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon Detective, consulta Servizi AWS coperti dal programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione descrive come applicare il modello di responsabilità condivisa quando si utilizza Detective. I seguenti argomenti illustrano come configurare Detective per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse da Detective.

Indice

Protezione dei dati in Amazon Detective

Il AWS modello di responsabilità condivisa modello di di si applica alla protezione dei dati in Amazon Detective. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutte le Cloud AWS. L'utente è responsabile del mantenimento del controllo sui contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza per Servizi AWS che usi. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consultare il AWS Modello di responsabilità condivisa e post sul GDPR blog sul AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS credenziali e configura singoli utenti con AWS IAM Identity Center oppure AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Usa l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi di acquisizione AWS attività, vedi Lavorare con i CloudTrail sentieri in AWS CloudTrail Guida per l'utente.
- Utilizzo AWS soluzioni di crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se sono necessari FIPS 140-3 moduli crittografici convalidati per l'accesso AWS tramite un'interfaccia a riga di comando o unAPI, utilizza un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Detective o altri Servizi AWS utilizzando la consoleAPI, AWS CLI, oppure AWS SDKs. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

Detective crittografa tutti i dati che elabora e archivia a riposo e in transito.

Indice

Gestione delle chiavi per Amazon Detective

Poiché Detective non memorizza dati personali dei clienti, utilizza Chiavi gestite da AWS.

Questo tipo di chiave KMS può essere utilizzato su più account. Consulta la descrizione delle chiavi AWS possedute nella Guida per AWS Key Management Service gli sviluppatori.

Questo tipo di chiave KMS ruota automaticamente ogni anno (circa 365 giorni). Vedi la descrizione della rotazione delle chiavi nella Guida per gli AWS Key Management Service sviluppatori.

Identity and Access Management per Amazon Detective

AWS Identity and Access Management (IAM) è un programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse del Detective. IAMè un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Indice

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi in Detective.

Utente del servizio: se utilizzi il servizio Detective per eseguire il tuo processo, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità di Detective utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Detective, consulta Risoluzione dei problemi relativi all'identità e all'accesso di Amazon Detective.

Amministratore del servizio: se sei il responsabile delle risorse Detective presso la tua azienda, probabilmente disponi dell'accesso completo a Detective. Il tuo compito è determinare le funzionalità e le risorse di Detective a cui gli utenti del servizio devono accedere. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM Detective, consultaCome funziona Amazon Detective con IAM.

IAMamministratore — Se sei un IAM amministratore, potresti voler saperne di più su come scrivere politiche per gestire l'accesso a Detective. Per visualizzare esempi di politiche basate sull'identità del Detective che puoi utilizzare, consultaIAM. Esempi di policy basate sull'identità per Amazon Detective

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta AWS Signature Version 4 per API le richieste nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'AWS IAM Identity Center utente e Autenticazione a AWS più fattori IAM nella Guida per l'IAMutente.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Utenti e gruppi IAM

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per IAM gli utenti nella Guida per l'IAMutente.

IAMRuoli

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. Per assumere temporaneamente un IAM ruolo in AWS Management Console, puoi passare da un utente a un IAM ruolo (console). È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Metodi per assumere un ruolo nella Guida per l'IAMutente.

IAMi ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, consulta Creare un ruolo per un provider di identità di terze parti (federazione) nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione

utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- Sessioni di accesso inoltrato (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
- Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o effettuano AWS API richieste. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate sulle identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Definire le IAM autorizzazioni personalizzate con le politiche gestite dal cliente nella Guida per l'utente. IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scegliere tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite contenute IAM in una policy basata sulle risorse.

Liste di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioniACLs, consulta la [panoramica di Access control list (ACL)](#) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. [Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM](#)
- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.
- Criteri di controllo delle risorse (RCPs): RCPs sono JSON criteri che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le IAM politiche allegate a ciascuna risorsa di tua proprietà. RCPLimita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente

root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations eRCPs, incluso un elenco di Servizi AWS tale supportoRCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

Come funziona Amazon Detective con IAM

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Amazon Detective. Inoltre, non possono eseguire attività utilizzando AWS Management Console AWS CLI, o AWS API. Un amministratore Detective deve disporre di politiche AWS Identity and Access Management (IAM) che concedano a IAM utenti e ruoli il permesso di eseguire API operazioni specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi collegare queste policy al principale che richiedono tali autorizzazioni.

Detective utilizza politiche IAM basate sull'identità per concedere le autorizzazioni per i seguenti tipi di utenti e azioni:

- Account amministratore: l'account amministratore è il proprietario di un grafico di comportamento, che utilizza i dati del proprio account. L'account amministratore può invitare gli account membri a contribuire con i propri dati al grafico di comportamento. L'account amministratore può anche utilizzare il grafico comportamentale per la valutazione e l'analisi dei risultati e delle risorse associati a tali account.

È possibile impostare le policy per consentire agli utenti diversi dall'account amministratore di eseguire diversi tipi di attività. Ad esempio, un utente con un account amministratore potrebbe avere solo le autorizzazioni per gestire gli account membri. Un altro utente potrebbe avere solo le autorizzazioni per utilizzare il grafico di comportamento per le indagini.

- Account membri: un account membro è un account invitato a contribuire con i dati a un grafico di comportamento. Un account membro risponde a un invito. Dopo aver accettato un invito, un account membro può rimuovere il proprio account dal grafico di comportamento.

Per avere una panoramica generale del Servizi AWS funzionamento di Detective e altriIAM, consulta [Creazione delle politiche nella JSON scheda della](#) Guida per l'IAMutente.

Policy basate su identità di Detective

Con le policy IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Detective supporta operazioni, risorse e chiavi di condizione specifiche.

Per maggiori informazioni su tutti gli elementi utilizzati in una JSON policy, consulta [IAMJSONPolicy Elements Reference](#) nella Guida per l'IAMutente.

Azioni

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le istruzioni della policy devono includere un elemento `Action` o un elemento `NotAction`. L'elemento `Action` elenca le azioni consentite dalla policy. L'elemento `NotAction` elenca le operazioni non consentite.

Le operazioni definite per Detective riflettono le attività che è possibile eseguire utilizzando Detective. Le operazioni delle policy in Detective hanno il seguente prefisso: `detective:`.

Ad esempio, per concedere l'autorizzazione a utilizzare l'`CreateMembers`APIoperazione per invitare gli account dei membri a visualizzare un grafico comportamentale, includi l'`detective:CreateMembers`azione nella loro politica.

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Ad esempio, per un account membro, la politica include l'insieme di operazioni relative alla gestione di un invito:

```
"Action": [
      "detective:ListInvitations",
      "detective:AcceptInvitation",
      "detective:RejectInvitation",
      "detective:DisassociateMembership
]
```

Per specificare più operazioni, è possibile utilizzare i caratteri jolly (*). Ad esempio, per gestire i dati utilizzati nel grafico di comportamento, gli account amministratore in Detective devono poter eseguire le seguenti attività:

- Visualizza l'elenco di account membri (`ListMembers`).
- Ottieni informazioni sugli account membri selezionati (`GetMembers`).
- Invita gli account membri a visualizzare il loro grafico di comportamento (`CreateMembers`).
- Rimuovi i membri dal grafico di comportamento (`DeleteMembers`).

Invece di elencare queste operazioni separatamente, puoi concedere l'accesso a tutte le operazioni che terminano con la parola `Members`. La policy a tal fine potrebbe includere la seguente operazione:

```
"Action": "detective:*Members"
```

Per visualizzare un elenco di operazioni di Detective, consulta [Operazioni definite da Amazon Detective]() nella Guida di riferimento per l'autorizzazione del servizio.

Risorse

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo [Amazon Resource Name (ARN)](). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per ulteriori informazioni sul formato diARNs, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Per Detective, l'unico tipo di risorsa è il grafico di comportamento. La risorsa del grafico del comportamento in Detective ha quanto segueARN:

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

Ad esempio, un grafico di comportamento ha i seguenti valori:

- La Regione per il grafico di comportamento è `us-east-1`.
- L'ID account per l'account amministratore è `111122223333`.
- L'ID del grafico di comportamento è `027c7c4610ea4aacaf0b883093cab899`.

Per identificare questo grafico comportamentale in un'`Resource`istruzione, dovresti usare quanto segueARN:

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

Per specificare più risorse in una istruzione `Resource`, separa gli ARN con le virgole.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Ad esempio, lo stesso AWS account può essere invitato a diventare un account membro in più di un grafico comportamentale. Nella policy per quell'account membro, l'istruzione `Resource` elencherebbe i grafici di comportamento a cui sono stati invitati.

```
"Resource": [
      "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

Alcune operazioni di Detective, come la creazione di un grafico di comportamento, la visualizzazione di grafici di comportamento e la visualizzazione degli inviti al grafico di comportamento, non vengono eseguite su un grafico di comportamento specifico. Per queste operazioni, l'istruzione `Resource` deve utilizzare il carattere jolly (*).

```
"Resource": "*"
```

Per le operazioni dell'account amministratore, Detective verifica sempre che l'utente che effettua la richiesta appartenga all'account amministratore per il grafico di comportamento interessato. Per le operazioni dell'account membro, Detective verifica sempre che l'utente che effettua la richiesta appartenga all'account membro. Anche se una IAM policy concede l'accesso a un grafico comportamentale, se l'utente non appartiene all'account corretto, l'utente non può eseguire l'azione.

Per tutte le azioni eseguite su uno specifico grafico comportamentale, la IAM policy deve includere il graficoARN. Il grafico ARN può essere aggiunto in un secondo momento. Ad esempio, quando un account abilita per la prima volta Detective, la IAM policy iniziale fornisce l'accesso a tutte le azioni del Detective, utilizzando la jolly per il graficoARN. Ciò consente all'utente di iniziare immediatamente a gestire gli account membri e a condurre indagini nel proprio grafico di comportamento. Dopo aver creato il grafico del comportamento, puoi aggiornare la politica per aggiungere il graficoARN.

Chiavi di condizione

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano [operatori di condizione](), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica`OR`. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

Detective non definisce il proprio set di chiavi di condizione. Supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta AWS Global Condition Context Keys nella Guida IAM per l'utente.

Per scoprire con quali operazioni e risorse puoi utilizzare una chiave di condizione, consulta Operazioni definite da Amazon Detective.

Esempi

Per visualizzare esempi di policy basate su identità di Detective, consulta Esempi di policy basate sull'identità per Amazon Detective.

Policy basate sulle risorse di Detective (non supportate)

Detective non supporta policy basate su risorse.

Autorizzazione basata sui tag del grafici di comportamento di Detective

A ciascun grafico di comportamento possono essere assegnati valori di tag. È possibile utilizzare questi valori di tag nelle istruzioni condizionali per gestire l'accesso al grafico.

L'istruzione condizionale per un valore di tag utilizza il formato seguente.

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

Ad esempio, utilizza il codice seguente per consentire o negare un'azione quando il valore del tag `Department` è `Finance`.

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

Per esempi di policy che utilizzano i valori dei tag di risorsa, consulta the section called “Account amministratore: limitazione dell'accesso in base ai valori di tag”.

IAMRuoli da Detective

Un IAMruolo è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Detective

Puoi utilizzare credenziali temporanee per accedere con la federazione, assumere un IAM ruolo o assumere un ruolo tra account. È possibile ottenere credenziali di sicurezza temporanee chiamando AWS STS API operazioni come o. AssumeRoleGetFederationToken

Detective supporta l'uso di credenziali temporanee.

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. I ruoli collegati ai servizi vengono visualizzati nell'IAMaccount e sono di proprietà del servizio. Un IAM amministratore può visualizzare ma non modificare le autorizzazioni per i ruoli collegati al servizio.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi di Detective, consulta the section called “Uso di ruoli collegati ai servizi”.

Ruoli di servizio (non supportati)

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli di servizio vengono visualizzati nell'IAMaccount e sono di proprietà dell'account. Ciò significa che un IAM amministratore può modificare le autorizzazioni per questo ruolo. Tuttavia, il farlo potrebbe pregiudicare la funzionalità del servizio.

Detective non supporta i ruoli del servizio.

Esempi di policy basate sull'identità per Amazon Detective

Per impostazione predefinita, IAM gli utenti e i ruoli non sono autorizzati a creare o modificare le risorse del Detective. Inoltre, non possono eseguire attività utilizzando AWS Management Console AWS CLI, o AWS API.

Un IAM amministratore deve creare IAM politiche che concedano a utenti e ruoli l'autorizzazione a eseguire API operazioni specifiche sulle risorse specifiche di cui ha bisogno. L'amministratore associa quindi tali politiche agli IAM utenti o ai gruppi che richiedono tali autorizzazioni.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta Creazione di politiche JSON nella scheda nella Guida per l'utente. IAM

Argomenti

Best practice per le policy

Le policy basate sulle identità determinano se qualcuno può creare, accedere o eliminare risorse Detective nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere le autorizzazioni agli utenti e ai carichi di lavoro, utilizza le policy gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative nella Guida per l'IAMutente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo

le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM

- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle politiche con IAM Access Analyzer nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, consulta Secure API access with MFA nella Guida IAM per l'utente.

Per ulteriori informazioni sulle best practice inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida IAM per l'utente.

Utilizzo della console Detective

Per utilizzare la console Amazon Detective, l'utente o il ruolo deve avere accesso alle azioni pertinenti, che corrispondono alle azioni corrispondenti inAPI.

Per abilitare Detective e diventare un account amministratore per un grafico di comportamento, all'utente o al ruolo deve essere concessa l'autorizzazione per l'operazione `CreateGraph`.

Per utilizzare la console Detective per eseguire operazioni dell'account amministratore, all'utente o al ruolo deve essere concessa l'autorizzazione per l'operazione `ListGraphs`. Ciò concede l'autorizzazione a recuperare i grafici di comportamento di cui il relativo account è amministratore. È inoltre necessario concedergli l'autorizzazione a eseguire operazioni specifiche dell'account amministratore.

Le operazioni più basilari dell'account amministratore consistono nel visualizzare un elenco degli account membri in un grafico di comportamento e nell'utilizzare il grafico di comportamento per le indagini.

- Per visualizzare l'elenco degli account membri in un grafico di comportamento, è necessario concedere al principale l'autorizzazione per l'operazione `ListMembers`.
- Per condurre un'indagine in un grafico di comportamento, è necessario concedere al principale l'autorizzazione per l'operazione `SearchGraph`.

Per utilizzare la console Detective per eseguire operazioni dell'account membro, all'utente o al ruolo deve essere concessa l'autorizzazione per l'operazione `ListInvitations`. Ciò concede l'autorizzazione a visualizzare gli inviti del grafico di comportamento. È quindi possibile concedergli l'autorizzazione per operazioni specifiche dell'account membro.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una policy che consenta IAM agli utenti di visualizzare le policy in linea e gestite associate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI AWS API

```
{
    "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": "*"
        }
    ]
}
```

Account amministratore: gestione degli account membri in un grafico di comportamento

Questa policy di esempio è diretta agli utenti con account amministratore che sono responsabili solo della gestione degli account membri utilizzati nel grafico di comportamento. La policy, inoltre, consente all'utente di visualizzare le informazioni di utilizzo e di disattivare Detective. La policy non concede l'autorizzazione per utilizzare il grafico di comportamento per le indagini.

```
{"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:027c7c4610ea4aacaf0b883093cab899"
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Account amministratore: utilizzo di un grafico di comportamento per le indagini

Questa policy di esempio è diretta agli utenti con account amministratore che utilizzano il grafico di comportamento solo per le indagini. Non possono visualizzare o modificare l'elenco degli account dei membri nel grafico di comportamento.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":["detective:SearchGraph"],
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
   },
   {
    "Effect":"Allow",
    "Action":["detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Account membro: gestione degli inviti e delle iscrizioni al grafico di comportamento

Questa policy di esempio è diretta agli utenti che appartengono a un account membro. Nell'esempio, l'account membro appartiene a due grafici di comportamento. La policy concede l'autorizzazione a rispondere agli inviti e rimuovere l'account membro dal grafico di comportamento.

```
{"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:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
```

```
    "Effect":"Allow",
    "Action":["detective:ListInvitations"],
    "Resource":"*"
  }
 ]
}
```

Account amministratore: limitazione dell'accesso in base ai valori di tag

La seguente policy consente all'utente di utilizzare un grafico di comportamento per verificare se il tag `SecurityDomain` del grafico di comportamento corrisponde al tag `SecurityDomain` dell'utente.

```
{
    "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":"*"
    } ]
}
```

La seguente policy impedisce agli utenti di utilizzare un grafico di comportamento per verificare se il valore del tag `SecurityDomain` per il grafico di comportamento è `Finance`.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
```

```
        }
    } ]
}
```

AWS politiche gestite per Amazon Detective

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AmazonDetectiveFullAccess

È possibile allegare la policy `AmazonDetectiveFullAccess`alle identità IAM.

Questa policy concede autorizzazioni amministrative che consentono a un principale l'accesso completo a tutte le operazioni di Amazon Detective. Puoi collegare questa policy a un principale prima che abiliti Detective per il suo account. Deve inoltre essere collegato al ruolo utilizzato per eseguire gli script Python di Detective per creare e gestire un grafico del comportamento.

I principali con queste autorizzazioni possono gestire gli account membri, aggiungere tag al loro grafico del comportamento e utilizzare Detective per le indagini. Possono anche archiviare GuardDuty i risultati. Il criterio fornisce le autorizzazioni necessarie alla console Detective per visualizzare i nomi degli account che si trovano in AWS Organizations.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `detective`: consente ai principali l'accesso completo alle operazioni di Detective.
- `organizations`: consente ai principali di recuperare informazioni sugli account di un'organizzazione da AWS Organizations . Se un account appartiene a un'organizzazione, queste autorizzazioni consentono alla console di Detective di visualizzare i nomi degli account oltre ai numeri di account.
- `guardduty`— Consente ai presidi di ottenere e archiviare i GuardDuty risultati dall'interno di Detective.
- `securityhub`: consente ai principali di ottenere i risultati di Centrale di sicurezza dall'interno di Detective.

```
{
    "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 politica gestita: AmazonDetectiveMemberAccess

Puoi collegare la policy `AmazonDetectiveMemberAccess` anche alle tue entità IAM.

Questa policy fornisce ai membri l'accesso ad Amazon Detective e l'accesso in ambito alla console.

Con questa policy, puoi:

- Visualizzare gli inviti all'iscrizione al grafico di Detective e accetta o rifiuta tali inviti.
- Scoprire come la tua attività in Detective contribuisce ai costi di utilizzo di questo servizio nella pagina Utilizzo.
- Annullare la tua appartenenza a un grafico.

Questa policy concede le autorizzazioni di sola lettura che consentono l'accesso in ambito alla console di Detective.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `detective`: consente ai membri di accedere a 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": "*"
    }
  ]
}
```

AWS Policy gestita: AmazonDetectiveInvestigatorAccess

Puoi collegare la policy `AmazonDetectiveInvestigatorAccess` anche alle tue entità IAM.

Questa policy fornisce ai responsabili delle indagini l'accesso al servizio Detective e l'accesso in ambito alle dipendenze dell'interfaccia utente della console Detective. Questa policy concede le autorizzazioni per abilitare le indagini di Detective per gli utenti IAM e i ruoli IAM. Puoi indagare per identificare gli indicatori di compromissione, come i risultati, utilizzando un report di indagine, che fornisce analisi e approfondimenti sugli indicatori di sicurezza. Il report è classificato in base alla gravità, determinata utilizzando l'analisi comportamentale e il machine learning di Detective. Puoi utilizzare il report per dare priorità alla riparazione delle risorse.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `detective`: consente ai responsabili delle indagini di accedere alle operazioni di Detective, di abilitare le indagini di Detective e di abilitare il riepilogo dei gruppi di risultati.

- `guardduty`— Consente ai presidi di ottenere e archiviare i GuardDuty risultati dall'interno di Detective.
- `securityhub`: consente ai principali di ottenere i risultati di Centrale di sicurezza dall'interno di Detective.
- `organizations`— Consente ai dirigenti di recuperare informazioni sugli account di un'organizzazione da. AWS Organizations Se un account appartiene a un'organizzazione, queste autorizzazioni consentono alla console di Detective di visualizzare i nomi degli account oltre ai numeri di account.

```
{
  "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 politica gestita: AmazonDetectiveOrganizationsAccess

Puoi collegare la policy `AmazonDetectiveOrganizationsAccess` anche alle tue entità IAM.

Questa policy concede l'autorizzazione per abilitare e gestire Amazon Detective all'interno di un'organizzazione. È possibile abilitare Detective in tutta l'organizzazione e determinare l'account amministratore delegato per Detective.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `detective`: consente ai principali di accedere alle operazioni di Detective.
- `iam`: specifica che un ruolo collegato ai servizi viene creato quando Detective chiama `EnableOrganizationAdminAccount`.
- `organizations`— Consente ai responsabili di recuperare informazioni sugli account di un'organizzazione da. AWS Organizations Se un account appartiene a un'organizzazione, queste autorizzazioni consentono alla console di Detective di visualizzare i nomi degli account oltre ai numeri di account. Consente l'integrazione di un AWS servizio, consente la registrazione e l'annullamento della registrazione dell'account membro specificato come amministratore delegato e consente ai responsabili di recuperare gli account amministratore delegato in altri servizi di sicurezza come Amazon Detective, Amazon, Amazon GuardDuty Macie e. 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"
          ]
        }
      }
    }
  ]
}
```

AWS Policy gestita: AmazonDetectiveServiceLinkedRole

Non è possibile allegare la policy `AmazonDetectiveServiceLinkedRole` alle entità IAM. Questa policy è collegata a un ruolo collegato ai servizi che consente a Detective di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta the section called “Uso di ruoli collegati ai servizi”.

Questa policy concede le autorizzazioni amministrative che consentono al ruolo collegato ai servizi di recuperare le informazioni sull'account per un'organizzazione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `organizations`: recupera le informazioni sull'account di un'organizzazione.

```
{
  "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "organizations:DescribeAccount",
              "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

Detective: aggiornamenti alle policy AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Detective da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti .

Modifica	Descrizione	Data
AmazonDetectiveInvestigatorAccess: aggiornamento a policy esistenti	Sono state aggiunte operazioni di riepilogo dei gruppi di risultati e indagini di Detective alla policy `AmazonDetectiveInvestigatorAccess`. Queste operazioni consentono di avviare, recuperare e aggiornare le indagini di Detective e ottenere un riepilogo dei gruppi di risultati all'interno di Detective.	26 novembre 2023
AmazonDetectiveFullAccess e AmazonDetectiveInvestigatorAccess: aggiornamenti alle policy esistenti	Detective ha aggiunto operazioni `GetFindings` di Centrale di sicurezza alle policy `AmazonDetectiveFullAccess` e `AmazonDetectiveInvestigatorAccess`. Queste operazioni consentono di ottenere i risultati di Centrale di sicurezza dall'interno di Detective.	16 maggio 2023
AmazonDetectiveOrganizationsAccess: nuova policy	Detective ha aggiunto la policy `AmazonDetectiveOrganizationsAccess`. Questa policy concede l'autorizzazione per abilitare e gestire Detective all'interno di un'organizzazione	2 marzo 2023
AmazonDetectiveMemberAccess: nuova policy	Detective ha aggiunto la policy `AmazonDetectiveMemberAccess`.	17 gennaio 2023

Modifica	Descrizione	Data
	Questa policy fornisce ai membri l'accesso a Detective e l'accesso in ambito alle dipendenze dell'interfaccia utente della console.	
AmazonDetectiveFullAccess: aggiornamenti a una policy esistente	Detective ha aggiunto GuardDuty `GetFindings` delle azioni alla `AmazonDetectiveFullAccess` polizza. Queste azioni consentono di ottenere GuardDuty risultati dall'interno del Detective.	17 gennaio 2023
AmazonDetectiveInvestigatorAccess: nuova policy	Detective ha aggiunto la policy `AmazonDetectiveInvestigatorAccess` . Questa policy consente al principale di condurre indagini in Detective.	17 gennaio 2023
AmazonDetectiveServiceLinkedRole: nuova policy	Detective ha aggiunto una nuova policy per il suo ruolo collegato ai servizi. La policy consente al ruolo collegato ai servizi di recuperare informazioni sugli account in un'organizzazione.	16 dicembre 2021
Detective ha iniziato a tenere traccia delle modifiche	Detective ha iniziato a tenere traccia delle modifiche alle sue politiche AWS gestite.	10 maggio 2021

Utilizzo dei ruoli collegati ai servizi per Detective

Amazon Detective utilizza AWS Identity and Access Management ruoli collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente a Detective. I ruoli collegati ai servizi sono predefiniti dal Detective e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per conto dell'utente.

Un ruolo collegato ai servizi semplifica la configurazione di Detective perché consente di evitare l'aggiunta manuale delle autorizzazioni necessarie. Detective definisce le autorizzazioni dei relativi ruoli collegati ai servizi e, salvo diversamente definito, solo Detective potrà assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di Detective perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione relativa ai Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli un Sì con un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per Detective

Detective utilizza il ruolo collegato al servizio denominato AWSServiceRoleForDetective: consente al Detective di accedere alle AWS Organizations informazioni per tuo conto.

Il ruolo AWSServiceRoleForDetective collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `detective.amazonaws.com`

Il ruolo AWSServiceRoleForDetective collegato al servizio utilizza la policy gestita. `AmazonDetectiveServiceLinkedRolePolicy`

Per dettagli sugli aggiornamenti della `AmazonDetectiveServiceLinkedRolePolicy` politica, consulta gli aggiornamenti di Amazon Detective alle politiche AWS gestite. Per ricevere avvisi automatici sulle modifiche a questa politica, iscriviti al feed RSS nella pagina della cronologia dei documenti di Detective.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Detective

Non è necessario creare manualmente un ruolo collegato ai servizi. Quando si designa l'account amministratore di Detective per un'organizzazione nella AWS Management Console, nella o nell' AWS API AWS CLI, Detective crea il ruolo collegato al servizio per l'utente.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando si definisce l'account amministratore di Detective per un'organizzazione, Detective crea il ruolo collegato ai servizi per tuo conto.

Modifica di un ruolo collegato ai servizi per Detective

Detective non consente di modificare il ruolo AWSServiceRoleForDetective collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Detective

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio Detective utilizza tale ruolo quando provi a eliminare le risorse, è possibile che l'eliminazione non riesca. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse del Detective utilizzate da AWSServiceRoleForDetective

1. Rimuovi l'account amministratore di Detective. Per informazioni, consulta the section called “Designazione dell'account amministratore di Detective”.
2. Ripeti la procedura in ogni Regione in cui hai designato l'account amministratore di Detective.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSServiceRoleForDetective collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi di Detective

Detective supporta l'utilizzo di ruoli collegati ai servizi in tutte le Regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Risoluzione dei problemi relativi all'identità e all'accesso di Amazon Detective

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi comuni che potresti riscontrare lavorando con Detective eIAM. Se riscontri problemi di accesso negato o difficoltà simili quando lavori con AWS Identity and Access Management(IAM), consulta IAM gli argomenti sulla risoluzione dei problemi nella Guida per l'IAMutente.

Non sono autorizzato a eseguire un'operazione in Detective

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'errore di esempio seguente si verifica quando l'`mateojackson`IAMutente tenta di utilizzare la console per accettare un invito a diventare un account membro per un grafico comportamentale, ma non dispone `detective:AcceptInvitation` delle autorizzazioni.

```
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 questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa `arn:aws:detective:us-east-1:444455556666:graph:567856785678` utilizzando l'azione `detective:AcceptInvitation`.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a Detective.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Detective. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse da Detective

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l’assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se Detective supporta queste funzionalità, consulta Come funziona Amazon Detective con IAM.
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un IAM utente di un altro Account AWS di tua proprietà nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a persone Account AWS di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.

- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM IAM

Convalida della conformità per Amazon Detective

Amazon Detective rientra nell'ambito del programma di AWS garanzia. Per ulteriori informazioni, vedere Health Information Trust Alliance Common Security Framework (HITRUST) CSF .

Per un elenco dei AWS servizi nell'ambito di programmi di conformità specifici, vedere AWSServizi nell'ambito del programma di conformità AWS . Per informazioni generali, vedere Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact Scaricamento dei . AWS

AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide rapide su sicurezza e conformità Guide introduttive alla sicurezza e alla conformità illustrano le considerazioni relative all'architettura e forniscono i passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- Valutazione delle risorse in base alle regole contenute nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente di verificare la conformità agli standard e alle best practice del settore della sicurezza. AWS

Resilienza in Amazon Detective

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Oltre all'infrastruttura AWS globale, Detective utilizza la resilienza integrata in Amazon DynamoDB e Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3). Per ulteriori informazioni, consulta la pagina Resilienza e disaster recovery in Amazon DynamoDB e Resilience in Amazon Simple Storage Service.

L'architettura di Detective è inoltre resistente al fallimento di una singola zona di disponibilità. Questa resilienza è integrata in Detective e non richiede alcuna configurazione.

Sicurezza dell'infrastruttura in Amazon Detective

Come servizio gestito, Amazon Detective; è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well‐Architected Framework.

Utilizzi API le chiamate AWS pubblicate per accedere a Detective; attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS) come (Ephemeral Diffie-Hellman) o DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale. IAM In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Le migliori pratiche di sicurezza per Detective

Detective fornisce una serie di funzionalità di sicurezza che occorre valutare durante lo sviluppo e l'implementazione delle policy di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

Per Detective, le best practice di sicurezza sono associate alla gestione degli account in un grafico di comportamento.

Le migliori pratiche per gli account degli amministratori di Detective

Quando inviti degli account dei membri al tuo grafico comportamentale da Detective, invita solo gli account che hai supervisionato.

Limita l'accesso al grafico di comportamento. Gli utenti con AmazonDetectiveFullAccessquesta policy possono concedere l'accesso a tutte le azioni del Detective. I principali con queste autorizzazioni possono gestire gli account membri, aggiungere tag al loro grafico del comportamento e utilizzare Detective per le indagini. Quando un utente ha accesso a un grafico di comportamento, può visualizzare tutti i risultati relativi agli account membri. Tali risultati potrebbero rivelare informazioni di sicurezza sensibili.

Best practice per gli account membri

Quando ricevi un invito a visualizzare un grafico di comportamento, assicurati di verificare la fonte dell'invito.

Controlla l' AWS identificatore dell'account amministratore che ha inviato l'invito. Assicurati di sapere a chi appartiene l'account e verifica che l'account che ha inviato l'invito abbia un motivo legittimo per monitorare i tuoi dati di sicurezza.

Registrazione delle API chiamate di Amazon Detective con AWS CloudTrail

Detective è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Detective. CloudTrail cattura tutte le API chiamate al Detective come eventi. Le chiamate acquisite includono chiamate dalla console Detective e chiamate in codice alle API operazioni del Detective.

- Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Detective.
- Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi.

Utilizzando le informazioni raccolte da CloudTrail, puoi determinare quanto segue:

- La richiesta effettuata a Detective
- L'indirizzo IP dal quale è stata effettuata la richiesta
- L'utente che ha effettuato la richiesta
- Quando è stata effettuata
- Dettagli aggiuntivi relativi alla richiesta

Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

Informazioni investigative in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Detective, tale attività viene registrata in un CloudTrail evento, insieme ad altri eventi di AWS servizio, nella Cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS . Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Detective, crea una traccia. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3.

Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni AWS . Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Puoi anche configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione di Amazon SNS Notifications per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

CloudTrail registra tutte le operazioni del Detective, che sono documentate nel Detective API Reference.

Ad esempio, le chiamate alle `DeleteMembers` operazioni `CreateMembersAcceptInvitation`, e generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM)
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato
- Se la richiesta è stata effettuata da un altro AWS servizio

Per ulteriori informazioni, consulta l'CloudTrail userIdentityelemento.

Informazioni sulle voci dei file di log di Detective

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro.

Un evento rappresenta una singola richiesta da un'origine. Gli eventi includono informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle API chiamate pubbliche, quindi le voci non vengono visualizzate in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`AcceptInvitation`azione.


```
      {
            "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
            "Username": "JaneRoe",
            "EventTime": 1571956406.0,
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS: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\":\"AROAJZARKEP6WKJ5JHSUS
\",\"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": []
        },
```

Regioni e quote di Amazon Detective

Quando usi Amazon Detective, tieni presente le seguenti quote.

Regioni ed endpoint di Detective

Per visualizzare l'elenco delle aree Regioni AWS in cui è disponibile Detective, consulta Endpoints del servizio Detective.

Quote di Detective

Detective ha le seguenti quote, che non possono essere configurate.

Risorsa	Quota	Commenti
Numero di account membro	1.200	Il numero di account membri che un account amministratore può aggiungere a un grafico di comportamento.
Volume dei dati del grafico di comportamento: avviso sul volume	9 TB al giorno	Se il volume di dati del grafico di comportamento è superiore a 9 TB al giorno, Detective visualizza un avviso che indica che il grafico di comportamento si sta avvicinando al volume massimo consentito.
Volume di dati del grafico di comportamento: nessun nuovo account	10 TB al giorno	Se il volume di dati del grafico di comportamento supera i 10 TB al giorno, non è possibile aggiungere un nuovo account membro al grafico.
Volume di dati del grafico di comportamento: interromp i l'importazione dei dati nel grafico di comportamento	15 TB al giorno	Se il volume di dati del grafico di comportamento è superiore a 15 TB al giorno, Detective interrompe l'importa zione dei dati nel grafico di comportam ento.

Risorsa	Quota	Commenti
		La quota di 15 TB al giorno riflette sia il normale volume di dati che i picchi. Per riabilitare l'importazione dei dati, è necessario contattare Supporto.

Internet Explorer 11 non è supportato

Non è possibile utilizzare Detective con Internet Explorer 11.

Gestione dei tag per un grafico di comportamento

Un tag è un'etichetta opzionale che puoi definire e assegnare alle AWS risorse, inclusi alcuni tipi di risorse da Detective. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio in base allo scopo, al proprietario, all'ambiente o ad altri criteri. Ad esempio, è possibile utilizzare i tag per applicare politiche, allocare i costi, distinguere tra versioni delle risorse o identificare risorse che supportano determinati requisiti o flussi di lavoro di conformità.

Puoi assegnare tag al tuo grafico di comportamento. È quindi possibile utilizzare i valori dei tag nelle IAM politiche per gestire l'accesso alle funzioni del grafico comportamentale in Detective. Per informazioni, consulta the section called “Autorizzazione basata sui tag del grafici di comportamento di Detective”.

Puoi anche utilizzare i tag come strumento per la rendicontazione dei costi. Ad esempio, per tenere traccia dei costi associati alla sicurezza, puoi assegnare lo stesso tag al grafico del comportamento del Detective, alla risorsa dell' AWS Security Hub hub e ai GuardDuty rilevatori Amazon. Inoltre AWS Cost Explorer, puoi quindi cercare quel tag per visualizzare una visione consolidata dei costi di tali risorse.

Visualizzazione dei tag per un grafico comportamentale

Puoi gestire i tag per il tuo grafico di comportamento dalla pagina Generale.

Console

Visualizzare l'elenco dei tag assegnati al grafico di comportamento

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, in Settings (Impostazioni), scegliere General (Generali).

Detective API, AWS CLI

Puoi usare il Detective API o il AWS Command Line Interface per ottenere l'elenco dei tag per il tuo grafico del comportamento.

Per ottenere l'elenco dei tag per un grafico del comportamento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`ListTagsForResource`operazione. Devi fornire il grafico ARN del tuo comportamento.

- AWS CLI: alla riga di comando, esegui il comando `list-tags-for-resource`.

  ```
  aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
  ```

  Esempio

  ```
  aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
  ```

Aggiungere tag a un grafico del comportamento

Console

Dall'elenco dei tag nella pagina Generale, è possibile aggiungere valori di tag al grafico di comportamento.

Aggiungere un tag al grafico di comportamento

1. Scegli Aggiungi nuovo tag.
2. Per Chiave, inserisci il nome del tag.
3. In Valore, immetti il valore del tag.

Detective API, AWS CLI

Puoi usare il Detective API o il AWS CLI per aggiungere valori di tag al tuo grafico del comportamento.

Per aggiungere tag a un grafico del comportamento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'[`TagResource`]operazione. Fornisci il grafico del comportamento ARN e i valori dei tag da aggiungere.
- AWS CLI: alla riga di comando, esegui il comando `tag-resource`.

  ```
  aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior graph ARN> --tags '{"TagName":"TagValue"}'
  ```

  Esempio

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

Rimuovere i tag da un grafico comportamentale

Console

Per rimuovere un tag dall'elenco nella pagina Generale, scegli l'opzione Rimuovi per quel tag.

Detective API, AWS CLI

Puoi usare il Detective API o il AWS CLI per rimuovere i valori dei tag dal tuo grafico del comportamento.

Per rimuovere i tag da un grafico del comportamento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Usa l'`UntagResource`operazione. Fornisci il grafico ARN del comportamento e i nomi dei tag da rimuovere.
- AWS CLI: alla riga di comando, esegui il comando `untag-resource`.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys
 "TagName"
```

Esempio

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Disabilitazione di Amazon Detective

L'account amministratore per un grafico di comportamento può disabilitare Amazon Detective dalla console Detective, dall'API Detective o dalla AWS Command Line Interface. Quando disabiliti Detective, il grafico di comportamento e i dati di Detective associati vengono eliminati.

Una volta eliminato, il grafico di comportamento non può più essere ripristinato.

Indice

Disabilitazione di Detective (console)

Puoi disabilitare Amazon Detective dalla AWS Management Console.

Per disabilitare Amazon Detective (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Generale.
3. Nella pagina Generale, in Disattiva Amazon Detective, scegli Disabilita Amazon Detective.
4. Quando richiesto, digita **`disable`** per confermare.
5. Scegli Disattiva Amazon Detective.

Disattivazione di Detective (Detective API, AWS CLI)

Puoi disabilitare Amazon Detective dall'API Detective o dalla AWS Command Line Interface. Per ottenere l'ARN del grafico del comportamento da utilizzare nella richiesta, utilizza l'operazione `ListGraphs`.

Per disabilitare Detective (Detective API, AWS CLI)

- API Detective: usa l'operazione `DeleteGraph`. È necessario specificare l'ARN del grafico.
- AWS CLI: alla riga di comando, esegui il comando `delete-graph`.

```
aws detective delete-graph --graph-arn <graph ARN>
```

Esempio:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Disattivazione di Detective in tutte le regioni (script Python attivo) GitHub

Detective fornisce uno script open source GitHub che consente di disabilitare Detective per un account amministratore in un elenco specificato di regioni.

Per informazioni su come configurare e utilizzare GitHub gli script, vedere. the section called “Script di Amazon Detective Python”

Cronologia dei documenti per la Guida per l'utente di Detective

Nella tabella seguente vengono descritte le modifiche importanti apportate alla documentazione dall'ultima versione di Detective. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile sottoscrivere un feed RSS.

- Ultimo aggiornamento della documentazione: 20 febbraio 2025

Modifica	Descrizione	Data
Aggiunto il supporto per i rilevamenti delle sequenze di GuardDuty attacco di Amazon	Detective ha aggiunto il supporto per la ricerca dei tipi associati a GuardDuty Extended Threat Detection . GuardDutyrileva una sequenza di attacco quando una sequenza specifica di più azioni, come le attività delle API e il rilevamento dei GuardDuty risultati, si allinea a un'attività potenzialmente sospetta. Per informazioni su Extended Threat Detection e sui tipi di ricerca delle sequenze di attacco, consulta Extended Threat Detection nella Amazon GuardDuty User Guide.	20 febbraio 2025
È stato aggiunto il supporto per la ricerca di Amazon GuardDuty IAM	Detective ha aggiunto il supporto per un nuovo tipo di GuardDuty ricerca che avvisa l'utente quando le credenziali utente con restrizioni, create	4 febbraio 2025

	per gli utenti elencati Account AWS nel proprio ambiente, vengono utilizzate per effettuare richieste a. Servizi AWS Per ulteriori informazioni, consulta Policy:IAMUser/ShortTermRootCredentialUsagenella Amazon GuardDuty User Guide.	
Nuova caratteristica	Aggiunto il layout della sequenza temporale a Detective Finding Group Visualization. Sono state introdotte la funzionalità del pulsante di riproduzione e il filtraggio dei risultati basato sulla gravità. Questi miglioramenti possono aiutarvi a comprendere meglio la progressione degli eventi, a dare priorità ai problemi critici e a condurre indagini di sicurezza più efficienti.	27 dicembre 2024

Aggiunto il supporto per i GuardDuty risultati di Amazon	Detective ha aggiunto il supporto per i seguenti tre GuardDuty tipi di risultati che ti avvisano quando vengono eseguiti comandi sospetti su un' EC2 istanza Amazon o un carico di lavoro di container all'interno del tuo AWS ambiente: • Discovery:Runtime/SuspiciousCommand • Persistence:Runtime/SuspiciousCommand • PrivilegeEscalation:Runtime/SuspiciousCommand	6 novembre 2024
Aggiunto il supporto per i GuardDuty risultati di Amazon	Detective ora fornisce supporto per i seguenti tipi di risultati GuardDuty di Runtime Monitoring. • `Execution:Runtime/SuspiciousShell` • `PriviliegeEscalation:Runtime/ElevationToRoot`	27 agosto 2024

Aggiunto il supporto per i GuardDuty risultati di Amazon	Detective ora fornisce supporto per la protezione GuardDuty da malware per S3. Questo ti aiuta a scansionare gli oggetti appena caricati nei bucket Amazon S3 alla ricerca di potenziali malware e caricamenti sospetti e ad agire per isolarli prima che vengano inseriti nei processi downstream.	9 luglio 2024
Funzionalità aggiornate	Detective ha aggiunto un nuovo layout radiale al pannello di visualizzazione del gruppo di risultati, per fornire una migliore visualizzazione e una più facile interpretazione dei dati.	26 giugno 2024
Nuove versioni dei sorgenti di Security Lake	Oltre alla versione sorgente 1 (OCSF 1.0.0-rc.2), Detective ora acquisisce i dati dalla versione sorgente 2 (OCSF 1.1.0) per le sorgenti Security Lake supportate da Detective.	15 maggio 2024
Nuova fonte di log di Security Lake	Puoi utilizzare l'integrazione di Detective con Security Lake per raccogliere log ed eventi da Amazon EKS Audit Logs.	15 maggio 2024

Aggiornamento della documentazione	Il contenuto dell'Amazon Detective Administration Guide è ora consolidato nella Amazon Detective User Guide. Amazon Detective Administr ation Guide raggiungerà la fine del supporto standard l'8 maggio 2024.	15 aprile 2024
Aggiunto il supporto per i GuardDuty risultati di Amazon	Detective ora fornisce supporto per i seguenti tipi di risultati GuardDuty di Runtime Monitoring. • `Execution:Runtime/MaliciousFileExecuted` • `Execution:Runtime/SuspiciousTool` • `DefenseEvasion:Runtime/PtraceAntiDebugging` • `Execution:Runtime/SuspiciousCommand` • `DefenseEvasion:Runtime/SuspiciousCommand`	5 aprile 2024
Rimosso il requisito di GuardDuty iscrizione ad Amazon	Non è più necessario essere un GuardDuty cliente per abilitare Amazon Detective. Il requisito che doveva essere GuardDuty abilitato nel tuo account per 48 ore prima di abilitare Detective è stato rimosso.	2 febbraio 2024

Aggiunto il supporto per i GuardDuty risultati di Amazon	Detective estende il supporto per i tipi di risultati GuardDuty EC2 di Runtime Monitoring a ECS e EC2 alle risorse.	30 gennaio 2024
Funzionalità aggiornate	Ora puoi eseguire un'indagi ne investigativa dalla pagina Investigazioni per una risorsa specifica su cui vuoi indagare. Detective suggerisce le risorse in base alla sua attività nei risultati e nei gruppi di ricerca. Detective Investigations ti consente di esaminare gli utenti e i ruoli IAM con indicatori di compromis sione, che possono aiutarti a determinare se una risorsa è coinvolta in un incidente di sicurezza.	16 gennaio 2024
Funzionalità aggiornate	Ora puoi eseguire un'indagi ne da Detective dalla pagina Indagini su una risorsa consigliata. Detective suggerisce le risorse in base alla sua attività nei risultati e nei gruppi di ricerca. Detective Investigations ti consente di esaminare gli utenti e i ruoli IAM con indicatori di compromissione, che possono aiutarti a determinare se una risorsa è coinvolta in un incidente di sicurezza.	26 dicembre 2023

Modifiche nel modo in cui Detective legge il flusso di traffico per la condivisione VPCs	Se utilizzi un Amazon VPC condiviso, potresti notare cambiamenti nel traffico monitorato da Detective. Ti consigliamo di esaminare le modifiche nei Dettagli dell'atti vità per il volume globale dei flussi VPC per comprende re i potenziali effetti sulla copertura e di esaminare Come Amazon Detective calcola il costo previsto per comprendere l'impatto sui costi del servizio.	20 dicembre 2023
Disponibilità regionale	Sono state aggiunte le regioni Europa (Stoccolma), Europa (Parigi) e Canada (Centrale) all'elenco delle AWS regioni in cui è disponibile l'integrazione tra Detective e Security Lake.	8 dicembre 2023
Nuova caratteristica	Indagini di Detective consentono di esaminare gli utenti IAM e i ruoli IAM con indicatori di compromis sione, che possono aiutarti a determinare se una risorsa è coinvolta in un incidente di sicurezza.	26 novembre 2023

Nuova caratteristica	Per impostazione predefinita, Detective genera automaticamente riepiloghi dei gruppi di risultati basati sull'intelligenza artificiale generativa (IA generativa). Un riepilogo di gruppi di risultati analizza rapidamente le relazioni tra i risultati e le risorse interessate, quindi riassume le potenziali minacce in linguaggio naturale.	26 novembre 2023
Nuova caratteristica	L'integrazione di Detective con Security Lake ti consente di eseguire query e recuperare i dati dei log non elaborati archiviati da Security Lake. Utilizzando questa integrazione, puoi raccogliere log ed eventi dagli eventi di CloudTrail gestione e dai log di flusso di Amazon Virtual Private Cloud (Amazon VPC).	26 novembre 2023
Aggiunte informazioni sulla policy gestita al capitolo sulla sicurezza	Sono state aggiunte operazioni di riepilogo dei gruppi di risultati e indagini di Detective alla policy `AmazonDetectiveInvestigatorAccess` .	26 novembre 2023
Visualizzazione di una panoramica dei risultati	Se un risultato è correlato a un'attività più ampia, Detective ora avvisa di passare a quel gruppo di risultati.	18 settembre 2023

Endpoint e quote di Amazon Detective	Detective è ora disponibile nella Regione Israele (Tel Aviv).	25 agosto 2023
Visualizzazione migliorata dei gruppi di risultati	La visualizzazione dei gruppi di risultati di Detective ora include gruppi di risultati con risultati aggregati che rendono più efficiente l'analisi delle prove, delle entità e dei risultati correlati.	8 agosto 2023
Gruppi di risultati migliorati	I gruppi di risultati ora includono i risultati delle vulnerabilità di Amazon Inspector.	13 giugno 2023
Aggiunto supporto per Amazon GuardDuty Lambda Protection	Detective ora fornisce supporto per GuardDuty Lambda Protection.	26 maggio 2023
Aggiunti risultati AWS di sicurezza come nuovo pacchetto opzionale di sorgenti dati.	Detective ora fornisce risultati AWS di sicurezza come pacchetto di sorgenti dati opzionale. Questo pacchetto di origini dati facoltativi consente a Detective di importare dati da Centrale di sicurezza e di aggiungerli al grafico di comportamento.	16 maggio 2023
Aggiunto supporto per i tipi di risultati di Amazon GuardDuty EKS Runtime Monitoring	Detective ora fornisce supporto per i tipi di risultati di GuardDuty EKS Runtime Monitoring.	3 maggio 2023

[È stato aggiunto il supporto per i tipi di ricerca di Amazon GuardDuty RDS Protection](#)	Detective ora fornisce supporto per i tipi di ricerca GuardDuty di RDS Protection.	20 aprile 2023
[Aggiunto il supporto per altri tipi di GuardDuty ricerca Amazon](#)	Detective ora fornisce profili per i seguenti tipi di GuardDuty reperti aggiuntivi: `DefenseEvasion:EC2UnusualDNSResolver` `DefenseEvasion:EvasionEC2UnusualDoHActivity` `DefenseEvasion: DefenseEvasionEC2UnusualDoTActivity`	12 aprile 2023
[Aggiunti nuovi pannelli nella console di Detective per aiutare gli utenti a selezionare la policy gestita da AWS appropriata per il caso d'uso specifico.](#)	Detective offre policy gestite per scegliere in modo sicuro le autorizzazioni di cui si ha bisogno.	3 aprile 2023
[Visualizzazione del traffico di flusso VPC per i cluster EKS](#)	Aggiunta una nuova sezione per il traffico di flusso di Amazon Virtual Private Cloud (Amazon VPC) con i cluster Amazon Elastic Kubernetes Service (Amazon EKS).	2 marzo 2023

Il gruppo di risultati ora include una rappresentazione visiva dinamica del grafico di comportamento di Detective	Il gruppo di risultati di Detective ora include una rappresentazione visiva dinamica del grafico di comportamento di Detective per enfatizzare la relazione tra entità e i risultati all'interno del gruppo di risultati.	28 febbraio 2023
Esporta i dati dalla pagina Riepilogo di Detective e dalla pagina dei risultati di ricerca. I dati vengono esportati in formato CSV (valori separati da virgola).	Detective ora offre la possibili tà di esportare i dati nel browser dalla console Detective.	7 febbraio 2023
Aggiunto il volume globale di flussi VPC per i carichi di lavoro EKS di Amazon EKS	Detective ora aggiunge riepiloghi visivi e analisi sui log di flusso di Amazon Virtual Private Cloud (VPC) dai carichi di lavoro Amazon Elastic Kubernetes Service Amazon EKS.	19 gennaio 2023
Aggiunte informazioni sulla policy gestita al capitolo sulla sicurezza	Il Detective ora supporta le azioni GuardDuty per ottenere risultati attravers o la AmazonDetectiveFul lAccess polizza. Il capitolo sulla sicurezza ora fornisce dettagli sulle seguenti nuove politiche gestite per Detective : AmazonDetectiveMem berAccess e AmazonDet ectiveInvestigatorAccess.	17 gennaio 2023

Aggiunta la conservazione dei dati	Con Detective puoi accedere fino a un anno di dati storici degli eventi.	20 dicembre 2022
Aggiunta l'opzione per regolare il periodo di validità nella pagina di riepilogo.	Detective ora offre la possibilità di modificare il periodo di validità in modo da visualizzare l'attività per qualsiasi periodo di 24 ore nei 365 giorni precedenti.	5 ottobre 2022
Ricerca di un risultato o di un'entità	Detective ora consente le ricerche senza dover fare distinzione tra maiuscole e minuscole.	3 ottobre 2022
Aggiunta la possibilità di impostare il timestamp dell'ambito	Detective ora offre un modo per configurare la preferenza del formato di timestamp dell'ambito. Questa preferenza verrà applicata a tutti i timestamp di Detective.	3 ottobre 2022
Aggiunti termini relativi ai gruppi di risultati	Detective ora supporta gruppi di risultati che collegano i risultati correlati in un'unica visualizzazione per indagare su potenziali attività dannose nel tuo ambiente. Da un profilo del gruppo di risultati, puoi passare ai profili di entità e alle panoramiche dei risultati relative a quel gruppo.	3 agosto 2022

Aggiunti nuovi profili associati ai log di controllo di Amazon EKS	Detective ora fornisce profili che consentono di esaminare le attività associate alle seguenti entità relative ai container: cluster Amazon EKS, immagini di container , pod Kubernetes e soggetti Kubernetes.	26 luglio 2022
Aggiunta una nuova origine dati facoltativa	Detective ora supporta i log di controllo EKS come pacchetto di origini dati facoltative. Un account amministratore può abilitare questa nuova origine dati per il grafico di comportamento esistente. Nei grafici creati dopo questa data questa origine dati sarà abilitata per impostazione predefinita. Gli amministratori possono disabilitare questa origine dati manualmente in qualsiasi momento.	26 luglio 2022
Nuovo ruolo collegato ai servizi e policy gestita per Detective	Detective ha ora un ruolo collegato ai servizi, `AWSServiceRoleForDetective` . Il ruolo collegato ai servizi viene utilizzato per accedere ai dati di Organizations per tuo conto. Il ruolo utilizza una nuova policy gestita da `AmazonDetectiveServiceLinkedRolePolicy` .	16 dicembre 2021

[Aggiunta integrazione con AWS Organizations]()	Detective è ora integrato con Organizations. L'account di gestione dell'organizzazione designa un account amministr atore di Detective per l'organiz zazione. L'account amministr atore di Detective può visualizzare tutti gli account dell'organizzazione e abilitarl i come account membri nel grafico di comportamento dell'organizzazione.	16 dicembre 2021
[I profili di risultati sono stati sostituiti con le panoramiche dei risultati]()	I profili dei risultati conteneva no visualizzazioni che analizzavano l'attività della risorsa coinvolta. La nuova panoramica dei risultati contiene i dettagli dei risultati acquisiti GuardDuty e un elenco delle entità coinvolte. Dalla panoramica dei risultati , è possibile passare ai profili delle entità correlate.	20 settembre 2021
[È stato rimosso il limite ai tipi di ricerca supportati GuardDuty]()	Detective non è più limitato a una serie selezionata di tipi di GuardDuty reperti. Detective raccoglie automaticamente i dettagli dei risultati per tutti i tipi di risultati e fornisce l'accesso ai profili delle entità per le entità correlate.	20 settembre 2021

Collegamento ai dettagli dei risultati dal pannello del profilo dei risultati associato	In un profilo di entità, quando si sceglie un risultato nell'elenco dei risultati associati, i dettagli del risultato vengono visualizzati nel pannello a destra. Il periodo di validità è impostato sulla finestra dell'ora del risultato.	20 settembre 2021
Aggiunti i bucket S3 ai tipi di entità disponibili in Detective	Detective ora fornisce profili per i bucket S3. I profili dei bucket S3 forniscono dettagli sui principali che hanno interagito con il bucket S3 e sulle operazioni API che hanno eseguito sul bucket S3.	20 settembre 2021
Nuova opzione per generare Detective URLs in Splunk	Il progetto Splunk Trumpet ti consente di inviare AWS contenuti a Splunk. Il progetto ora consente di aggiungere Detective URLs per accedere ai profili e ai GuardDuty risultati.	8 settembre 2021

[Sostituito AKIDs nei dettagli dell'attività per account e ruoli]()	Nei profili degli account, i dettagli dell'attività per il volume complessivo delle chiamate API ora mostrano gli utenti o i ruoli anziché gli identificatori delle chiavi di accesso (AKIDs). Nei profili di ruolo, i dettagli dell'atti vità per il volume complessi vo delle chiamate API ora mostrano le sessioni di AKIDs ruolo anziché. Per le attività che si sono svolte prima di questa modifica, il chiamante viene elencato come Risorsa sconosciuta.	14 luglio 2021

Aggiunto il servizio di chiamata alle informazioni sulle chiamate API	Nella console Detective, le informazioni sulle chiamate API ora includono il servizio che ha emesso la chiamata. È stata aggiunta una colonna Servizio agli elenchi nelle pagine Volume globale delle chiamate API, Chiamate API appena osservate e Chiamate API con maggiore volume. Nei dettagli dell'attività per Volume globale delle chiamate API e Geolocalizzazioni appena osservate, i metodi API sono raggruppati in base ai servizi che li hanno emessi. Per le attività che si sono verificat e prima di questa modifica, i metodi API sono raggruppati in Servizio sconosciuto.	14 luglio 2021
Nuova scheda Interazione delle risorse per utenti, ruoli e sessioni di ruolo	La scheda Interazione delle risorse per utenti, ruoli e sessioni di ruolo contiene informazioni sull'attività di assunzione dei ruoli che ha coinvolto tali entità. Per le sessioni di ruolo, questa è una nuova scheda. Per utenti e ruoli, questa è una scheda esistente con nuovi contenuti.	29 giugno 2021

Aggiornati i valori per le quote di volume dei dati del grafico di comportamento	Sono state aumentate le quote di volume di dati per i grafici di comportamento. Con 3,24 TB al giorno, Detective emette un avviso. Con 3,6 TB al giorno, non è possibile aggiungere nuovi account. Con 4,5 TB al giorno, Detective interromp e l'importazione dei dati nel grafico di comportamento.	10 giugno 2021
Aggiunti valori di tag alle opzioni dello script Python	Quando si utilizza lo script Python di Detective `enableDetective.py` per abilitare Detective, puoi assegnare i valori dei tag al grafico di comportamento.	19 maggio 2021
Aggiunta l'abilitazione automatica degli account membri che superano il controllo del volume di dati	Quando gli account membri accettano un invito, il loro stato è Accettato (Non abilitato) fino a quando Detective non verifica che i loro dati non facciano sì che il volume di dati del grafico di comportam ento superi la quota. Se il volume di dati non è un problema, Detective modifica automaticamente lo stato in Accettato (Abilitato). Tieni presente che gli account membri esistenti che si trovano nello stato Accettato (Non abilitati) non possono essere abilitati automatic amente.	12 maggio 2021

Aggiunte informazioni sulla policy gestita al capitolo sulla sicurezza	Una nuova sezione del capitolo sulla sicurezza fornisce dettagli sulle policy gestite per Detective. Detective attualmente fornisce un'unica policy gestita, `AmazonDetectiveFullAccess` .	10 maggio 2021
Modificati i valori del volume di dati nell'elenco degli account membri	Nella pagina di gestione dell'account, l'elenco degli account membri ora mostra il volume di dati giornaliero per ogni account membro. In precedenza l'elenco mostrava il volume come percentuale del volume totale consentito.	29 aprile 2021
Opzioni riviste per la gestione degli account membri	Il menu Gestisci account è stato sostituito con un menu Operazioni. Combinate le opzioni per aggiungere singoli account e aggiungere account da un file .csv. L'opzione Abilita account è stata spostata da Gestisci account in un'opzione separata accanto a Operazioni.	5 aprile 2021
Aggiunti tag del grafico di comportamento e autorizzazioni basati sui tag	Quando abiliti Detective, puoi aggiungere tag al grafico di comportamento. Puoi gestire i tag per un grafico di comportamento dalla pagina Generale. Detective supporta anche l'autorizzazione basata sui valori dei tag.	31 marzo 2021

Aggiunto il supporto per altri tipi di GuardDuty ricerca Amazon	Detective ora fornisce profili per i seguenti tipi di GuardDuty reperti aggiuntivi: `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 marzo 2021
Sono state aggiunte differenze per AWS GovCloud (US) le regioni	Detective è ora disponibile nelle AWS GovCloud (US) Regioni. Negli AWS GovCloud Stati Uniti orientali e AWS GovCloud negli Stati Uniti occidentali, Detective non invia e-mail di invito agli account dei membri. Detective, inoltre, non rimuove automaticamente gli account membri che vengono chiusi in AWS.	24 marzo 2021

[Aggiunte le schede per filtrare l'elenco degli account membri in base allo stato dell'account membro]()	L'elenco degli account membri ora mostra delle schede che puoi utilizzare per filtrare l'elenco in base allo stato dell'account membro. È possibile visualizzare tutti gli account membro, quelli con lo stato Accettato (Abilitato) o quelli con uno stato diverso da Accettato (Abilitato).	16 marzo 2021
[Aggiunto il supporto per altri tipi di GuardDuty ricerca Amazon]()	Detective ora fornisce profili per i seguenti tipi di GuardDuty reperti aggiuntivi: `Backdoor:EC2/C&CActivity.B` `Impact:EC2/PortSweep` ,, `Impact:EC2/WinRMBruteForce` , e `PrivilegeEscalation:IAMUser/AdministrativePermissions`	4 marzo 2021
[Aggiunta l'opzione allo script Python per sopprimere le e-mail di invito]()	Lo script `enableDetective.py` di Detective ora offre un'opzione `--disable_email` . Quando includi questa opzione, Detective non invia e-mail di invito agli account membri.	26 febbraio 2021
[Il termine "account principale" è stato modificato in "account amministratore"]()	Il termine "account principale" viene modificato in "account amministratore". Il termine è cambiato anche nella console e nell'API di Detective.	25 febbraio 2021

Il termine "account principale" è stato modificato in "account amministratore"	Il termine "account principale" viene modificato in "account amministratore". Il termine è cambiato anche nella console e nell'API di Detective.	25 febbraio 2021
Aggiunti dettagli sull'attività per il volume dei flussi VPC del pannello del profilo da e verso l'indirizzo IP del risultato	Il pannello del profilo Volume del flusso VPC da e verso l'indirizzo IP del risultato ora visualizza i dettagli delle attività. I dettagli delle attività sono disponibili solo se il risultato è associato a un singolo indirizzo IP. I dettagli delle attività mostrano il volume per ogni combinazione di porte, protocollo e direzione.	25 febbraio 2021
Aggiunta l'opzione API per non inviare e-mail di invito agli account membri	Quando si utilizza l'API Detective per aggiungere account membri, gli account amministratore possono scegliere di non inviare e-mail di invito agli account membri.	25 febbraio 2021
Nuovi dettagli delle attività per il pannello di profilo Volume globale delle chiamate API sui profili degli indirizzi IP	Ora puoi visualizzare i dettagli delle attività per gli indirizzi IP dal pannello di profilo Volume globale delle chiamate API. I dettagli dell'attività mostrano il numero di chiamate riuscite e non riuscite per ogni risorsa che ha emesso la chiamata dall'indirizzo IP.	23 febbraio 2021

Nuovo pannello del profilo del volume globale di flussi VPC sui profili degli indirizzi IP	Il profilo dell'indirizzo IP ora contiene il pannello del profilo Volume globale di flussi VPC. Il pannello del profilo mostra il volume del traffico del flusso VPC da e verso l'indirizzo IP. È possibile visualizzare i dettagli dell'attività per mostrare il volume di ogni EC2 istanza con cui l'indirizzo IP ha comunicato.	21 gennaio 2021
Aggiunta la pagina Riepilogo di Detective	La pagina Detective Summary contiene visualizzazioni per guidare gli analisti verso le entità di interesse in base alla geolocalizzazione, al numero di chiamate API e al volume di traffico Amazon. EC2	21 gennaio 2021
Aggiornata l'opzione per passare da Amazon GuardDuty a Detective	In GuardDuty, l'opzione Investigate in Detective viene spostata dal menu Azioni al pannello dei dettagli del ritrovamento. Visualizza un elenco di entità correlate. Se il tipo di risultato è supportato, l'elenco include anche il risultato. Puoi quindi decidere di passare a un profilo di entità o a un profilo di risultato.	15 gennaio 2021

[Aggiunta l'opzione per impostare la finestra dei dettagli dell'attività sul periodo di validità predefinito]()	Nei dettagli dell'attività per Volume globale delle chiamate API e Volume globale dei flussi VPC, puoi impostare la finestra temporale per i dettagli dell'attività sul periodo di validità predefinito per il profilo.	15 gennaio 2021
[Aggiunta la gestione di intervalli di tempo ad alto volume per le entità]()	È stato aggiunto un nuovo avviso per indicare quando un'entità ha uno o più intervall i di tempo ad alto volume. Una nuova pagina Entità ad alto volume riporta tutti gli intervalli ad alto volume per il periodo di validità corrente.	18 dicembre 2020
[La quota degli account membri è stata aumentata a 1.200]()	Gli account master possono ora invitare fino a 1.200 account membri al proprio grafico di comportamento. In precedenza, questa quota era 1.000.	11 dicembre 2020
[Valori aggiunti per le quote di volume dei dati del grafico di comportamento]()	Aggiornate le informazioni sulle quote di volume dei dati del grafico di comportamento per aggiungere i valori di quota specifici.	11 dicembre 2020

È stata aggiunta la selezione dell'intervallo di tempo per i dettagli delle attività nel pannello di profilo del volume complessivo di chiamate API	Nel pannello Volume globale di flussi API, ora puoi visualizzare i dettagli dell'attività per qualsiasi intervallo di tempo selezionato. Il pannello mostra inizialmente un'opzione per visualizzare i dettagli dell'attività per il periodo di validità.	29 settembre 2020
Aggiunta la selezione dell'intervallo di tempo per i dettagli dell'attività nel pannello del profilo Volume globale di flussi VPC	Nel pannello Volume globale di flussi VPC, puoi visualizzare i dettagli dell'attività per un singolo intervallo di tempo dal grafico. Per visualizzare i dettagli dell'intervallo di tempo, scegli l'intervallo di tempo.	25 settembre 2020
Nuova sessione di ruolo ed entità utente federate	Detective ora consente di esplorare e indagare sull'autenticazione federata. Puoi vedere quali risorse hanno assunto ogni ruolo e quando sono avvenute tali autenticazioni.	17 settembre 2020
Aggiornamenti alla gestione del periodo di validità	È stata rimossa l'opzione per bloccare o sbloccare il periodo di validità. Adesso è sempre bloccata. Nel profilo di un risultato, viene visualizzato un avviso se il periodo di validità è diverso dalla finestra temporale del risultato.	4 settembre 2020

L'intestazione del profilo rimane visibile mentre scorri un profilo	Nei profili, il tipo, l'identificatore e il periodo di validità ora rimangono visibili mentre si scorrono i pannelli del profilo su una scheda. Quando le schede non sono visibili, puoi utilizzare l'elenco a discesa delle schede nel percorso di navigazione per passare a una scheda diversa.	4 settembre 2020
La ricerca mostra sempre i risultati della ricerca	Quando si esegue una ricerca, ora vengono visualizzati i risultati nella pagina Cerca. Dai risultati, è possibile passare a un risultato specifico o al profilo di una entità.	27 agosto 2020
Aggiunto ai criteri consentiti per le ricerche	I criteri consentiti per le ricerche sono stati ampliati. È possibile cercare AWS utenti e AWS ruoli per nome. Puoi usare l'ARN per cercare risultati, AWS ruoli, AWS utenti e EC2 istanze.	27 agosto 2020
Collegamenti ad altre console dai pannelli dei profili	Nel pannello del EC2 profilo dei dettagli dell' EC2 istanza, l'identificatore dell'istanza è collegato alla EC2 console Amazon. Nei pannelli del profilo Dettagli e Dettagli ruolo, il nome utente e il nome del ruolo sono collegati alla console IAM.	14 agosto 2020

Dettagli dell'attività per i dati del flusso VPC	Il pannello del profilo Volume globale di flussi VPC ora fornisce l'accesso ai dettagli dell'attività. I dettagli dell'atti vità mostrano il flusso di traffico tra gli indirizzi IP e un' EC2 istanza durante un periodo di tempo selezionato.	23 luglio 2020
Gli account membri possono ora vederne l'utilizzo e i costi previsti	Gli account membri possono ora visualizzare le informazi oni sul proprio utilizzo. Per gli account membri, la pagina Utilizzo mostra la quantità di dati importati in ogni grafico di comportamento a cui contribui scono. Gli account membri possono inoltre visualizzare il costo previsto per 30 giorni.	26 maggio 2020
La prova gratuita è ora disponibile per account anziché per grafico di comportamento	Ogni account Amazon Detective ora riceve una prova gratuita separata all'inter no di ciascuna Regione. La prova gratuita inizia quando l'account abilita Detective o la prima volta che l'account viene abilitato come account membro.	26 maggio 2020

Nuovi script Python open source su GitHub	Il nuovo amazon-detective-multiaccount-scriptsrepository GitHub fornisce script Python open source che è possibile utilizzare per gestire i grafici comportamentali tra le regioni. È possibile abilitare Detective , aggiungere account membri, rimuovere account membri e disabilitare Detective.	21 gennaio 2020
Introduzione di Amazon Detective	Detective utilizza il machine learning e le visualizzazioni dedicate per aiutarti ad analizzare e indagare sui problemi di sicurezza nei carichi di lavoro di Amazon Web Services (AWS).	2 dicembre 2019