aws

사용 설명서

Amazon Detective

Amazon Detective: 사용 설명서

Table of Contents

Amazon Detective란 무엇인가요?

Amazon Detective는 사용자가 보안 조사 결과 또는 의심스러운 활동의 근본 원인을 분석 및 조사하고 신속하게 식별하는 데 도움이 됩니다. Detective는AWS리소스에서 로그 데이터를 자동으로 수집합니다. 그런 다음 기계 학습, 통계 분석 및 그래프 이론을 사용하여 더 빠르고 효율적으로 보안 조사를 수행할 수 있도록 시각화를 생성합니다. Detective의 사전 구축된 데이터 집계, 요약 및 컨텍스트는 가능한 보안 문제의 특성과 범위를 신속하게 분석하고 확인하는 데 도움이 됩니다.

Detective를 사용하면 최대 1년 분량의 과거 이벤트 데이터에 액세스할 수 있습니다. 이 데이터는 선택한 기간 동안의 활동 유형 및 양의 변화를 보여주는 일련의 시각화를 통해 제공됩니다. Detective는 이러한 변경 사항을 GuardDuty 조사 결과와 연결합니다. Detective의 소스 데이터에 대한 자세한 내용은 the section called “동작 그래프에 사용된 소스 데이터” 섹션을 참조하세요.

Amazon Detective를 사용하면 데이터를 자동으로 집계하고 시각적 도구를 제공하여 더 빠르고 효율적인 보안 조사를 수행할 수 있습니다. 잠재적 문제를 신속하게 분석하고 보안 위협의 범위를 결정할 수 있습니다.

주제

Amazon Detective의 기능

다음은 Amazon Detective가AWS환경에서 의심스러운 활동을 조사하고 리소스를 분석하여 보안 문제의 근본 원인을 식별하는 데 도움이 되는 몇 가지 주요 방법입니다.

탐지 결과 그룹

탐지 결과 그룹을 사용하면 잠재적 보안 이벤트와 관련된 여러 활동을 검사할 수 있습니다. 조사 결과 그룹을 사용하여 심각도가 높은 GuardDuty 조사 결과의 근본 원인을 분석할 수 있습니다. 위협 행위자가AWS환경을 손상시키려고 하는 경우 일반적으로 여러 보안 조사 결과와 비정상적인 동작을 생성하는 일련의 작업을 수행합니다.

Detective의 결과 그룹 페이지에는 동작 그래프에서 추출된 모든 관련 결과 그룹이 표시됩니다. 조사 결과 그룹을 활용하여 보안 조사 결과의 근본 원인을 분석하는 방법에 대한 자세한 내용은 Detective에서 조사 결과 그룹 분석을 참조하세요.

Detective는 보안 문제를 더 빠르고 철저하게 조사하는 데 도움이 되는 각 결과 그룹의 대화형 시각화를 제공합니다. 시각화는 보안 인시던트와 관련된 엔터티와 조사 결과를 표시하도록 설계되어 연결 및 근본 원인을 더 쉽게 이해할 수 있습니다.는 적은 노력으로 문제를 더 빠르고 철저하게 조사할 수 있도록 도와줍니다. 조사 결과 그룹 시각화 패널에는 조사 결과 그룹과 관련된 조사 결과 및 개체가 표시됩니다.

조사 결과를 분류하기 위한 탐지 조사

Detective 조사를 사용하면 손상 지표를 사용하여 IAM 사용자 및 IAM 역할을 조사할 수 있으며, 이를 통해 리소스가 보안 인시던트와 관련이 있는지 확인할 수 있습니다. 손상 지표(IOC)는 네트워크, 시스템 또는 환경에서 관찰된 아티팩트로, 높은 수준의 신뢰도로 악의적인 활동이나 보안 인시던트를 식별할 수 있습니다. Detective 조사를 통해 효율성을 극대화하고, 보안 위협에 집중하고, 발생률 대응 기능을 강화할 수 있습니다.

Detective 조사는 기계 학습 모델과 위협 인텔리전스를 사용하여 가장 중요하고 의심스러운 문제만 표시하므로 상위 수준의 조사에 집중할 수 있습니다.AWS환경의 리소스를 자동으로 분석하여 손상 또는 의심스러운 활동의 잠재적 지표를 식별합니다. 이를 통해 패턴을 식별하고 보안 이벤트의 영향을 받는 리소스를 이해하여 위협 식별 및 완화에 대한 선제적 접근 방식을 제공할 수 있습니다.

Detective 조사를 실행하여 Detective 콘솔에서 Detective 조사 시작을 사용할 수 있습니다. 프로그래밍 방식으로 조사를 실행하려면 Detective API의 StartInvestigation 작업을 사용합니다.AWS Command Line Interface(AWS CLI)를 사용하여 조사를 실행하려면 start-investigation 명령을 실행합니다.

Amazon Security Lake와의 Detective 통합

Detective는 Amazon Security Lake와 통합되므로 Security Lake에 저장된 원시 로그 데이터를 쿼리하고 검색할 수 있습니다. 이 통합을 통해 Security Lake가 기본적으로 지원하는 다음 소스에서 로그와 이벤트를 수집할 수 있습니다.

- AWS CloudTrail관리 이벤트 버전 1.0 이상
- Amazon Virtual Private Cloud(Amazon VPC) 흐름 로그 버전 1.0 이상
- Amazon Elastic Kubernetes Service(Amazon EKS) 감사 로그 버전 2.0

Detective를 Security Lake와 통합한 후 Detective는AWS CloudTrail관리 이벤트 및 Amazon VPC 흐름 로그와 관련하여 Security Lake에서 원시 로그를 가져오기 시작합니다. 원시 로그를 쿼리하여 Detective에서 로그와 이벤트를 볼 수 있습니다.

VPC 흐름 볼륨 조사

Detective를 사용하면 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 및 Kubernetes 포드의 Virtual Private Cloud(VPC) 네트워크 흐름에 대한 활동 세부 정보를 대화형으로 검사할 수 있습니다.Amazon EC2 Detective는 모니터링된 계정에서 VPC 흐름 로그를 자동으로 수집하고, EC2 인스턴스별로 집계하고, 이러한 네트워크 흐름에 대한 시각적 요약 및 분석을 제공합니다.

EC2 인스턴스의 경우 전체 VPC 흐름량의 활동 세부 정보에는 선택한 시간 범위 동안의 EC2 인스턴스와 IP 주소 간의 상호 작용이 표시됩니다.

Kubernetes 포드의 경우 전체 VPC 흐름량은 모든 대상 IP 주소에 대해 Kubernetes 포드에 할당된 IP 주소로 들어오고 나가는 전체 바이트 볼륨을 표시합니다.

Amazon Detective 액세스

Amazon Detective는 대부분에서 사용할 수 있습니다AWS 리전. Detective를 현재 사용할 수 있는 리전 목록은의 Amazon Detective 엔드포인트 및 할당량을 참조하세요AWS 일반 참조. 에 대한 관리에AWS 리전대한 자세한AWS 계정내용은 AWS Account Management참조 안내서의 계정에서 사용할 수 있는 지정을 참조AWS 리전하세요.

각 리전에서 다음 방법 중 하나로 Detective를 사용할 수 있습니다.

AWS Management Console

는 리소스를 생성하고 관리하는AWS데 사용할 수 있는 브라우저 기반 인터페이스AWS Management Console입니다. 해당 콘솔의 일부로 Amazon Detective 콘솔은 Detective 계정, 데이터 및 리소스에 대한 액세스를 제공합니다. Detective 콘솔을 사용하여 모든 Detective 작업을 수행할 수 있습니다. 즉, 잠재적 보안 위협을 검토하고 보안 결과의 근본 원인을 분석, 조사 및 식별할 수 있습니다.

AWS명령줄 도구

AWS명령줄 도구를 사용하면 시스템의 명령줄에서 명령을 실행하여 Detective 작업 및AWS작업을 수행할 수 있습니다. 명령줄을 사용하는 것이 콘솔을 사용하는 것보다 더 빠르고 편리할 수 있습니다. 작업을 수행하는 스크립트를 작성할 때도 명령줄 도구가 유용합니다.

AWS는AWS Command Line Interface(AWS CLI)와의 두 가지 명령줄 도구 세트를 제공합니다AWS Tools for PowerShell. 설치 및 사용에 대한 자세한 내용은 AWS Command Line Interface사용 설명서를AWS CLI참조하세요. Tools for PowerShell 설치 및 사용에 대한 자세한 내용은 AWS Tools for PowerShell사용 설명서를 참조하세요.

AWS SDK

AWS는 Java, Go, Python, C++ 및 .NET과 같은 다양한 프로그래밍 언어 및 플랫폼을 위한 라이브러리 및 샘플 코드로 구성된 SDKs를 제공합니다. SDKs를 사용하면 Detective 및 기타에 프로그래밍 방식으로 편리하게 액세스할 수 있습니다AWS 서비스. SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 포함합니다.AWS SDKs. AWS

Amazon Detective REST API

Amazon Detective REST API를 사용하면 Detective 계정, 데이터 및 리소스에 포괄적이고 프로그래밍 방식으로 액세스할 수 있습니다. 이 API를 사용하면 HTTPS 요청을 Detective로 직접 보낼 수 있습니다. 그러나AWS명령줄 도구 및 SDKs와 달리이 API를 사용하려면 애플리케이션에서 요청에 서명하기 위한 해시 생성과 같은 하위 수준의 세부 정보를 처리해야 합니다. 이 API에 대한 자세한 내용은 Detective API 참조를 참조하세요.

Amazon Detective 요금

다른AWS제품과 마찬가지로 Amazon Detective 사용에 대한 계약이나 최소 약정은 없습니다.

Detective 요금은 여러 차원을 기반으로 하며 소스에 관계없이 모든 데이터에 대해 GB당 계층형 고정 요금이 부과됩니다. 자세한 내용은 Amazon Detective 요금을 참조하세요.

Detective 사용 비용을 이해하고 예측하는 데 도움이 되도록 Detective는 계정에 대한 예상 사용 비용을 제공합니다. Amazon Detective 콘솔에서 이러한 추정치를 검토하고 Amazon Detective API를 사용하여 액세스할 수 있습니다. 서비스 사용 방법에 따라 Security Lake 통합 및 Detective 조사와 같은 특정 Detective 기능과AWS 서비스함께 다른를 사용하는 데 추가 비용이 발생할 수 있습니다.

Detective를 처음 활성화하면가 Detective의 30일 무료 평가판에 자동으로 등록AWS 계정됩니다. 여기에는AWS Organizations에서 조직의 일부로 활성화된 개별 계정도 포함됩니다. 무료 평가판 기간 동안 해당에서 Detective를 사용하는 데는 요금이 부과되지 않습니다AWS 리전.

무료 평가판이 종료된 후 Detective 사용 비용을 이해하고 예측하는 데 도움이 되도록 Detective는 평가판 사용 중 Detective 사용에 따른 예상 사용 비용을 제공합니다. 사용량 데이터에는 무료 평가판이 종료될 때까지 남은 시간도 표시됩니다. Amazon Detective 콘솔에서 Detective 계정의 사용 관련 데이터를 검토하고 Amazon Detective API를 사용하여 액세스할 수 있습니다.

Detective는 어떻게 작동하나요?

Detective는AWS CloudTrail및 Amazon VPC 흐름 로그에서 로그인 시도, API 호출 및 네트워크 트래픽과 같은 시간 기반 이벤트를 자동으로 추출합니다. 또한 GuardDuty에서 탐지한 조사 결과를 수집합니다.

Detective는 이러한 이벤트를 기반으로 기계 학습과 시각화를 사용하여 리소스 동작과 시간 경과에 따른 리소스 동작 간의 상호 작용에 대한 통합된 대화형 보기를 생성합니다. 이 동작 그래프를 탐색하여 실패한 로그인 시도 또는 의심스러운 API 직접 호출과 같은 잠재적으로 악의적인 작업을 검사할 수 있습니다. 이러한 작업이AWS계정 및 Amazon EC2 인스턴스와 같은 리소스에 미치는 영향도 확인할 수 있습니다. 다음과 같이 다양한 작업에 맞게 동작 그래프의 범위와 타임라인을 조정할 수 있습니다.

- 규범을 벗어나는 모든 활동을 신속하게 조사합니다.
- 보안 문제를 나타낼 수 있는 패턴을 식별합니다.
- 조사 결과의 영향을 받는 모든 리소스를 이해합니다.

Detective 맞춤형 시각화는 계정 정보의 기준을 제공하고 요약합니다. 이러한 조사 결과는 “이 역할을 위한 비정상적인 API 직접 호출입니까?” 또는 “이 인스턴스에서 트래픽이 급증할 것으로 예상됩니까?”와 같은 질문에 답하는 데 도움이 될 수 있습니다.

Detective를 사용하면 데이터를 구성하거나 자체 쿼리 및 알고리즘을 개발, 구성 또는 조정할 필요가 없습니다. 선결제 비용은 없으며 분석된 이벤트에 대해서만 비용을 지불합니다. 추가 소프트웨어를 배포하거나 구독할 다른 피드는 없습니다.

누가 Detective를 사용하나요?

계정이 Detective를 활성화하면 동작 그래프의 관리자 계정이 됩니다. 동작 그래프는 하나 이상의AWS계정에서 추출 및 분석된 데이터의 연결된 집합입니다. 관리자 계정은 멤버 계정을 초대하여 관리자 계정의 동작 그래프에 데이터를 제공합니다.

Detective도와 통합됩니다AWS Organizations. 조직 관리 계정은 조직의 Detective 관리자 계정을 지정합니다. Detective 관리자 계정을 사용하면 조직 동작 그래프에서 조직 계정을 멤버 계정으로 사용할 수 있습니다.

Detective가 동작 그래프 계정의 소스 데이터를 사용하는 방법에 대한 자세한 내용은 the section called “동작 그래프에 사용된 소스 데이터” 섹션을 참조하세요.

관리자 계정이 동작 그래프를 관리하는 방법에 대한 자세한 내용은 계정 관리 섹션을 참조하세요. 멤버 계정이 동작 그래프 초대와 멤버십을 관리하는 방법에 대한 자세한 내용은 the section called “멤버 계정의 경우: 초대 및 멤버십 관리” 섹션을 참조하세요.

관리자 계정은 동작 그래프에서 생성된 분석 및 시각화를 사용하여AWS리소스와 GuardDuty 조사 결과를 조사합니다. GuardDuty 및와 Detective 통합을 사용하면 이러한 서비스의 GuardDuty 결과에서 Detective 콘솔로 직접 피벗AWS Security Hub CSPM할 수 있습니다.

Detective 조사는 관련AWS리소스와 관련된 활동에 초점을 맞춥니다. Detective의 조사 프로세스에 대한 개요는 Detective 사용 설명서의 Amazon Detective를 조사에 사용하는 방법을 참조하세요.

관련 서비스

에서 데이터, 워크로드 및 애플리케이션을 더욱 안전하게 보호하려면 Amazon Detective와AWS 서비스함께 다음을 사용하는 것이AWS좋습니다.

AWS Security Hub CSPM

AWS Security Hub CSPM는AWS리소스의 보안 상태를 포괄적으로 파악하고 보안 업계 표준 및 모범 사례를 기준으로AWS환경을 확인하는 데 도움이 됩니다. 이는 부분적으로 여러AWS 서비스(Detective 포함) 및 지원되는AWS파트너 네트워크(APN) 제품의 보안 조사 결과를 사용, 집계, 구성 및 우선 순위를 지정하여 이를 수행합니다. Security Hub CSPM을 사용하면 보안 추세를 분석하고AWS환경 전체에서 우선순위가 가장 높은 보안 문제를 식별할 수 있습니다.

Security Hub CSPM에 대한 자세한 내용은 AWS Security Hub CSPM사용 설명서를 참조하세요.

Amazon GuardDuty

Amazon GuardDuty는 Amazon S3 및 CloudTrail 관리 이벤트AWS로그에 대한AWS CloudTrail데이터 이벤트 로그와 같은 특정 유형의 로그를 분석하고 처리하는 보안 모니터링 서비스입니다. 악성 IP 주소 및 도메인 목록과 같은 위협 인텔리전스 피드와 기계 학습을 사용하여AWS환경 내에서 예기치 않고 잠재적으로 승인되지 않은 악의적인 활동을 식별합니다.

GuardDuty에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서를 참조하세요.

Amazon Security Lake

Amazon Security Lake는 완전 관리형 보안 데이터 레이크 서비스입니다. Security Lake를 사용하여AWS환경, SaaS 공급자, 온프레미스 소스, 클라우드 소스 및 타사 소스의 보안 데이터를AWS계정에 저장된 전용 데이터 레이크로 자동으로 중앙 집중화할 수 있습니다. Security Lake를 사용하

면 보안 데이터를 분석할 수 있으므로 조직 전체의 보안 상태를 더 완벽하게 이해할 수 있습니다. Security Lake를 사용하면 워크로드, 애플리케이션 및 데이터에 대한 보호도 개선할 수 있습니다.

Security Lake에 대한 자세한 내용은 Amazon Security Lake 사용 설명서를 참조하세요. Detective와 Security Lake를 함께 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요Security Lake와 Detective 통합.

추가AWS보안 서비스에 대한 자세한 내용은 의 보안, 자격 증명 및 규정 준수를AWS참조하세요.

Amazon Detective 개념 및 용어

다음은 Amazon Detective 및 해당 작동 방식을 이해하는 데 중요한 용어 및 개념입니다.

관리자 계정

동작 그래프를AWS 계정소유하고 조사를 위해 동작 그래프를 사용하는 입니다.

관리자 계정은 멤버 계정을 초대하여 동작 그래프에 해당 데이터를 제공합니다. 자세한 내용은 the section called “초대된 멤버 계정 관리” 단원을 참조하십시오.

조직 동작 그래프의 경우 관리자 계정은 조직 관리 계정이 지정하는 Detective 관리자 계정입니다. 자세한 내용은 the section called “Detective 관리자 계정 지정” 단원을 참조하십시오. Detective 관리자 계정은 조직 동작 그래프에서 모든 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 자세한 내용은 the section called “조직 멤버 계정 관리” 단원을 참조하십시오.

관리자 계정은 동작 그래프의 데이터 사용량을 확인하고 동작 그래프에서 멤버 계정을 제거할 수도 있습니다.

자율 시스템 구성(ASO)

자율 시스템을 할당받은 직함이 지정 조직입니다. 이 자율 시스템은 유사한 라우팅 로직 및 정책을 사용하는 이기종 네트워크 또는 네트워크 집합입니다.

동작 그래프

하나 이상의AWS 계정와 연결된 수신 소스 데이터에서 생성된 연결된 데이터 세트입니다.

각 동작 그래프는 동일한 구조의 조사 결과, 엔터티 및 관계를 사용합니다.

위임된 관리자 계정(AWS Organizations)

조직에서 서비스의 위임된 관리자 계정은 조직의 서비스 사용을 관리할 수 있습니다.

Detective에서는 Detective 관리자 계정이 조직 관리 계정이 아닌 한 Detective 관리자 계정도 위임된 관리자 계정입니다. 조직 관리 계정은 위임된 관리자 계정일 수 없습니다.

Detective에서는 자체 위임이 허용됩니다. 조직 관리 계정은 자신의 계정을 Detective의 위임된 관리자로 위임할 수 있지만 이는 Detective의 범위에서만 등록되거나 기억되며 조직은 등록되지 않습니다.

Detective 관리자 계정

조직 관리 계정이 리전의 조직 동작 그래프에 대한 관리자 계정으로 지정한 계정입니다. 자세한 내용은 the section called “Detective 관리자 계정 지정” 단원을 참조하십시오.

Detective는 조직 관리 계정이 자신의 계정이 아닌 다른 계정을 선택할 것을 권장합니다.

계정이 조직 관리 계정이 아닌 경우 Detective 관리자 계정은 Organizations에서 Detective에 대한 위임된 관리자 계정이기도 합니다.

Detective 소스 데이터

다음 유형의 피드에서 처리되고 구조화된 버전의 정보입니다.

- 로그 및 Amazon VPC 흐름AWS CloudTrail로그와 같은AWS서비스의 로그
- GuardDuty 조사 결과

Detective는 Detective 소스 데이터를 사용하여 동작 그래프를 채웁니다. 또한 Detective는 해당 분석을 지원하기 위해 Detective 소스 데이터의 사본을 저장합니다.

엔터티

수집된 데이터에서 추출한 항목입니다.

각 엔터티에는 엔터티가 나타내는 객체 유형을 식별하는 유형이 있습니다. 개체 유형의 예로는 IP 주소, Amazon EC2 인스턴스 및AWS사용자가 있습니다.

개체는 관리하는AWS리소스 또는 리소스와 상호 작용한 외부 IP 주소일 수 있습니다.

각 엔터티의 소스 데이터는 엔터티 속성을 채우는 데에도 사용됩니다. 속성 값은 소스 레코드에서 직접 추출하거나 여러 레코드에서 집계할 수 있습니다.

결과

Amazon GuardDuty에서 감지한 보안 문제입니다.

조사 결과 그룹

동일한 이벤트 또는 보안 문제와 관련이 있을 수 있는 조사 결과, 엔터티 및 증거 컬렉션입니다. Detective는 내장된 기계 학습 모델을 기반으로 조사 결과 그룹을 생성합니다.

Detective 증거

Detective는 지난 45일 이내에 수집된 동작 그래프의 데이터를 기반으로 조사 결과 그룹과 관련된 추가 증거를 식별합니다. 이 증거는 심각도 값이 정보용인 조사 결과로 제시됩니다. 증거는 조사 결과 그룹 내에서 볼 때 잠재적으로 의심스러울 수 있는 특이한 활동이나 알려지지 않은 동작을 강조

하는 지원 정보를 제공합니다. 조사 결과 범위 시간 내에서 새로 관찰된 지리적 위치 또는 API 직접 호출이 그 예가 될 수 있습니다. 현재 이러한 결과는 Detective에서만 볼 수 있으며 Security Hub CSPM으로 전송되지 않습니다.

결과 개요

조사 결과에 대한 요약 정보를 제공하는 단일 페이지입니다.

조사 결과 개요에는 조사 결과와 관련된 엔터티 목록이 포함되어 있습니다. 목록에서 엔터티의 프로필로 피벗할 수 있습니다.

조사 결과 개요에는 조사 결과 속성이 포함된 세부 정보 패널도 포함되어 있습니다.

대용량 엔터티

일정 기간 동안 많은 수의 다른 엔터티와 연결되거나 다른 엔터티에서 연결되어 있는 엔터티입니다. 예를 들어, EC2 인스턴스에는 수백만 개의 IP 주소에서의 연결이 있을 수 있습니다. 연결 수가 Detective에서 수용할 수 있는 임계값을 초과합니다.

현재 범위 시간에 대용량 시간 간격이 포함되어 있는 경우 Detective는 사용자에게 알립니다.

자세한 내용은 Amazon Detective 사용 설명서의 대용량 엔터티에 대한 세부 정보 보기를 참조하세요.

조사

의심스럽거나 흥미로운 활동을 분류하고, 범위를 결정하며, 근본 출처 또는 원인을 파악한 다음 진행 방법을 결정하는 프로세스입니다.

멤버 계정

관리자 계정이 동작 그래프에 데이터를 기여하도록 초대AWS 계정한 입니다. 조직 동작 그래프에서 멤버 계정은 Detective 관리자 계정이 멤버 계정으로 활성화한 조직 계정일 수 있습니다.

초대를 받은 멤버 계정은 동작 그래프 초대에 응답하고 동작 그래프에서 해당 계정을 제거할 수 있습니다. 자세한 내용은 the section called “멤버 계정의 경우: 초대 및 멤버십 관리” 단원을 참조하십시오.

조직 계정은 조직 동작 그래프에서 멤버십을 변경할 수 없습니다.

또한 모든 멤버 계정은 자신이 데이터를 제공하는 동작 그래프에서 해당 계정의 사용 정보를 볼 수 있습니다.

동작 그래프에 다른 접근 권한은 없습니다.

조직 동작 그래프

Detective 관리자 계정이 소유하는 동작 그래프입니다. 조직 관리 계정은 Detective 관리자 계정을 지정합니다. 자세한 내용은 the section called “Detective 관리자 계정 지정” 단원을 참조하십시오.

조직 동작 그래프에서 Detective 관리자 계정은 조직 계정이 멤버 계정인지 여부를 제어합니다. 조직 계정은 조직 동작 그래프에서 자체적으로 제거할 수 없습니다.

Detective 관리자 계정은 조직 동작 그래프에 다른 계정을 초대할 수도 있습니다.

프로필

엔터티의 활동과 관련된 데이터 시각화 컬렉션을 제공하는 단일 페이지입니다.

조사 결과의 경우, 프로필을 통해 분석가는 해당 결과가 진정한 우려인지 아니면 거짓 긍정인지 판단할 수 있습니다.

프로필은 조사 결과에 대한 조사를 지원하거나 의심스러운 활동에 대한 일반적인 추적을 지원하는 정보를 제공합니다.

프로필 패널

프로필에 대한 단일 시각화입니다. 각 프로필 패널은 분석가의 조사에 도움이 되도록 특정 질문이나 질문에 답변하는 데 도움을 주기 위한 것입니다.

프로필 패널에는 키-값 페어, 테이블, 타임라인, 막대형 차트 또는 지리적 위치 차트가 포함될 수 있습니다.

관계

개별 엔터티 간에 발생하는 활동입니다. 관계는 수신되는 소스 데이터에서도 추출됩니다.

엔터티와 마찬가지로 관계에도 유형이 있으며, 이를 통해 관련된 엔터티의 유형과 연결 방향을 식별할 수 있습니다. 관계 유형의 예로는 Amazon EC2 인스턴스에 연결하는 IP 주소가 있습니다.

범위 시간

프로필에 표시되는 데이터의 범위를 지정하는 데 사용되는 기간입니다.

조사 결과의 기본 범위 시간은 의심스러운 활동이 처음 관찰된 시간과 마지막 시간을 반영합니다.

엔터티 프로필의 경우 기본 범위 시간은 이전 24시간입니다.

Amazon Detective 시작하기

이 자습서에서는 Amazon Detective를 소개합니다. AWS 계정에서 Detective를 활성화하는 방법을 알아봅니다. 또한 Detective가 AWS 계정에서 동작 그래프로 데이터를 수집하고 추출하기 시작했는지 확인하는 방법도 알아봅니다.

Amazon Detective를 활성화하면 Detective는 사용자 계정을 관리자 계정으로 사용하는 리전별 동작 그래프를 생성합니다. 처음에는 이 계정이 동작 그래프에 있는 유일한 계정입니다. 그런 다음 관리자 계정은 다른 AWS 계정을 초대하여 데이터를 동작 그래프에 제공할 수 있습니다. 계정 관리을(를) 참조하세요.

리전에서 Detective를 처음 활성화하면 동작 그래프에 대한 30일 무료 평가판도 시작됩니다. 계정에서 Detective를 비활성화했다가 다시 활성화하면 무료 평가판을 사용할 수 없습니다. the section called “동작 그래프 무료 평가판에 대한 정보”을(를) 참조하세요.

무료 평가판 사용 후에는 동작 그래프에 있는 각 계정에 기여한 데이터에 대한 요금이 청구됩니다. 관리자 계정은 사용량을 추적하고 전체 동작 그래프에 대한 일반적인 30일 기간의 총 예상 비용을 확인할 수 있습니다. 자세한 내용은 the section called “관리자 계정 사용량 및 비용” 단원을 참조하십시오. 멤버 계정은 자신이 속한 동작 그래프의 사용량과 예상 비용을 추적할 수 있습니다. 자세한 내용은 the section called “멤버 계정 사용량 추적” 단원을 참조하십시오.

주제

- AWS 계정 설정
- Detective를 활성화하기 위한 사전 조건
- Detective를 활성화하기 위한 권장 사항
- Detective 활성화

AWS 계정 설정

Amazon Detective를 활성화하려면 AWS 계정가 있어야 합니다. AWS 계정이 없는 경우 다음 단계를 완료하여 계정을 생성합니다.

에 가입 AWS 계정

를 시작하려면이 AWS필요합니다 AWS 계정. 생성에 대한 자세한 AWS 계정내용은 AWS Account Management 참조 안내서의 시작하기 AWS 계정를 참조하세요.

Detective를 활성화하기 위한 사전 조건

Detective를 활성화하기 전에 다음 요구 사항을 충족하는지 확인합니다.

필요한 Detective 권한 부여

Detective를 활성화하려면 먼저 IAM 보안 주체에 필요한 Detective 권한이 있는지 확인해야 합니다. 보안 주체는 이미 사용 중인 기존 사용자 또는 역할일 수도 있고, Detective에 사용할 새 사용자 또는 역할을 만들 수도 있습니다.

Amazon Web Services(AWS)에 가입 시 해당 계정은 Amazon Detective를 포함한 모든 AWS 서비스에 자동으로 가입됩니다. 그러나 Detective를 활성화하고 사용하려면 Amazon Detective 콘솔에 대한 액세스와 API 작업에 대한 액세스를 허용하는 권한을 설정해야 합니다. 사용자 또는 관리자는 AWS Identity and Access Management (IAM)을 사용하여 모든 Detective 작업에 대한 액세스 권한을 부여하는 `AmazonDetectiveFullAccess` 관리형 정책을 IAM 보안 주체에 연결하여이 작업을 수행할 수 있습니다. 이러한 IAM 권한이 없으면 AWS 콘솔에서 Detective 시작하기 페이지를 볼 수 있습니다. 따라서 서비스가 활성화된 경우에도 이러한 권한이 추가될 때까지 콘솔에 활성 그래프가 표시되지 않습니다.

지원되는 AWS Command Line Interface 버전

AWS CLI 를 사용하여 Detective 작업을 수행하려면 최소 필수 버전은 1.16.303입니다.

Detective를 활성화하기 위한 권장 사항

Detective를 활성화하기 전에 다음 권장 사항을 따르는 것이 좋습니다.

GuardDuty 및 와의 권장 정렬 AWS Security Hub CSPM

GuardDuty에 등록되어 있고 해당 서비스의 관리자 계정이 되는 AWS Security Hub CSPM것이 좋습니다. 세 서비스 모두의 관리자 계정이 동일한 경우 다음 통합 지점이 원활하게 작동합니다.

- GuardDuty 또는 Security Hub CSPM에서 GuardDuty 결과에 대한 세부 정보를 볼 때 결과 세부 정보에서 Detective 결과 프로필로 피벗할 수 있습니다.
- Detective에서 GuardDuty 조사 결과를 조사할 때 해당 조사 결과를 보관하는 옵션을 선택할 수 있습니다.

GuardDuty 및 Security Hub CSPM의 관리자 계정이 다른 경우 자주 사용하는 서비스에 따라 관리자 계정을 정렬하는 것이 좋습니다.

- GuardDuty를 더 자주 사용하는 경우 GuardDuty 관리자 계정을 사용하여 Detective를 활성화합니다.

  AWS Organizations 를 사용하여 계정을 관리하는 경우 GuardDuty 관리자 계정을 조직의 Detective 관리자 계정으로 지정합니다.
- Security Hub CSPM을 더 자주 사용하는 경우 Security Hub CSPM 관리자 계정을 사용하여 Detective를 활성화합니다.

  Organizations를 사용하여 계정을 관리하는 경우 Security Hub CSPM 관리자 계정을 조직의 Detective 관리자 계정으로 지정합니다.

모든 서비스에서 동일한 관리자 계정을 사용할 수 없는 경우 Detective를 활성화한 후 선택적으로 크로스 계정 역할을 만들 수 있습니다. 이 역할은 관리자 계정에 다른 계정에 대한 액세스 권한을 부여합니다.

IAM이 이러한 유형의 역할을 지원하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 소유한 다른 AWS 계정의 IAM 사용자에게 액세스 권한 제공을 참조하세요.

GuardDuty CloudWatch 알림 빈도에 대한 권장 업데이트

GuardDuty의 탐지기는 Amazon CloudWatch 알림 빈도로 구성되어 후속 조사 결과 발생을 보고할 수 있습니다. 여기에는 Detective에 알림을 보내는 것도 포함됩니다.

기본 빈도는 6시간입니다. 즉, 조사 결과가 여러 번 반복되더라도 최대 6시간이 지나야 새로운 발생이 Detective에 반영됩니다.

Detective에서 이러한 업데이트를 수신하는 데 걸리는 시간을 줄이려면 GuardDuty 관리자 계정에서 감지기의 설정을 15분으로 변경하는 것이 좋습니다. 단, 구성을 변경해도 GuardDuty 사용 비용에는 영향을 미치지 않습니다.

알림 빈도 설정에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 Amazon CloudWatch Events를 사용한 GuardDuty 조사 결과 모니터링을 참조하세요.

Detective 활성화

Detective 콘솔, Detective API 또는 AWS Command Line Interface에서 Detective를 활성화할 수 있습니다.

Detective는 각 리전에서 한 번만 활성화할 수 있습니다. 이미 해당 리전의 동작 그래프의 관리자 계정인 경우 해당 리전에서 Detective를 다시 활성화할 수 없습니다.

Console

Detective 활성화(콘솔)

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. Get started를 선택합니다.
3. Amazon Detective 활성화 페이지에서 관리자 계정 정렬(권장)에는 Detective, Amazon GuardDuty, AWS Security Hub CSPM간에 관리자 계정을 정렬하기 위한 권장 사항이 설명되어 있습니다. the section called “GuardDuty 및 와의 권장 정렬 AWS Security Hub CSPM”을(를) 참조하세요.
4. IAM 정책 연결 버튼을 클릭하면 IAM 콘솔로 바로 이동하고 권장 정책이 열립니다. Detective에 사용하는 보안 주체에 권장 정책을 연결할 수 있습니다. IAM 콘솔에서 작업할 권한이 없는 경우 필수 권한 내에서 Amazon 리소스 이름(ARN) 정책을 복사하여 IAM 관리자에게 제공할 수 있습니다. 사용자를 대신하여 정책을 첨부할 수 있습니다.

   필수 IAM 정책이 적용되었는지 확인합니다.
5. 태그 추가 섹션에서는 동작 그래프에 태그를 추가할 수 있습니다.

   태그를 추가하려면 다음을 수행합니다.

   a. 새로운 태그 추가를 선택합니다.
   b. 키에는 태그의 이름을 입력합니다.
   c. 값에는 태그 값을 입력합니다.

   태그를 제거하려면 태그의 제거 옵션을 선택합니다.
6. Amazon Detective 활성화를 선택합니다.
7. Detective를 활성화한 후 멤버 계정을 동작 그래프에 초대할 수 있습니다.

   계정 관리 페이지로 이동하려면 지금 멤버 추가를 선택합니다. 멤버 계정 초대에 대한 자세한 내용은 the section called “초대된 멤버 계정 관리” 섹션을 참조하세요.

Detective API, AWS CLI

Detective API 또는 AWS Command Line Interface에서 Amazon Detective를 활성화할 수 있습니다.

Detective(Detective API AWS CLI)를 활성화하려면

- Detective API: `CreateGraph` 작업을 사용합니다.
- AWS CLI: 명령줄에서 `create-graph` 명령을 실행합니다.

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

다음 명령은 Detective를 활성화하고 `Department` 태그의 값을 `Security`로 설정합니다.

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

Python script on GitHub

GitHub.Detective는 GitHub에서 다음을 수행하는 오픈 소스 스크립트를 제공합니다.

- 지정된 리전 목록의 관리자 계정에 대해 Detective 활성화
- 제공된 멤버 계정 목록을 결과 동작 그래프에 추가
- 멤버 계정에 초대 이메일 전송
- 멤버 계정에 대한 초대 자동 수락

GitHub 스크립트를 구성하고 사용하는 방법에 대한 자세한 내용은 the section called “Amazon Detective Python 스크립트” 섹션을 참조하세요.

Detective가 AWS 계정에서 데이터를 수집하고 있는지 확인

Detective를 활성화하면 AWS 계정에서 동작 그래프로 데이터를 수집하고 추출하기 시작합니다.

초기 추출의 경우 일반적으로 2시간 이내에 동작 그래프에서 데이터를 사용할 수 있게 됩니다.

Detective가 데이터를 추출하고 있는지 확인하는 한 가지 방법은 Detective 검색 페이지에서 예제 값을 찾는 것입니다.

검색 페이지에서 예제 값 확인

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. 탐색 창에서 검색을 선택합니다.
3. 유형 선택 메뉴에서 항목 유형을 선택합니다.

데이터의 예제에는 동작 그래프 데이터에 있는 선택한 유형의 식별자 샘플 세트가 포함되어 있습니다.

예제 값을 보면 데이터가 수집되고 동작 그래프로 추출되고 있다는 것을 알 수 있습니다.

Detective 동작 그래프의 데이터

Amazon Detective에서는 Detective 동작 그래프의 데이터를 사용하여 조사를 수행합니다. 이 섹션에서는 Detective 동작 그래프에 사용되는 핵심 데이터 소스와 Detective가 소스 데이터를 사용하여 채우는 방법에 대해 알아볼 수 있습니다.

동작 그래프는 Detective 소스 데이터에서 생성된 연결된 데이터 세트로, 하나 이상의 Amazon Web Services(AWS) 계정에서 수집됩니다.

동작 그래프는 소스 데이터를 사용하여 다음을 수행합니다.

- 시간 경과에 따른 시스템, 사용자 및 이들 간의 상호 작용에 대한 전반적인 그림 생성
- 특정 활동을 더 자세히 분석하여 조사를 수행하면서 발생하는 질문에 답변
- 동일한 이벤트 또는 보안 문제와 관련이 있을 수 있는 조사 결과, 엔터티 및 증거 컬렉션 상호 연관

동작 그래프 데이터의 모든 추출, 모델링 및 분석은 각 개별 동작 그래프의 컨텍스트 내에서 이루어진다는 점에 유의하세요.

각 동작 그래프에는 하나 이상의 계정 데이터가 포함됩니다. 계정이 Detective를 활성화하면 해당 계정이 동작 그래프의 관리자 계정이 되고 동작 그래프에 사용할 멤버 계정을 선택합니다. 동작 그래프에는 최대 1,200개의 멤버 계정을 포함할 수 있습니다. 관리자 계정이 동작 그래프에서 멤버 계정을 관리하는 방법에 대한 자세한 내용은 Detective에서 계정 관리를 참조하세요.

내용

Detective가 동작 그래프를 채우는 방법

조사를 위한 원시 데이터를 제공하기 위해 Detective는 다음을 포함하여 AWS 환경 전반과 그 밖의 다양한 데이터를 수집합니다.

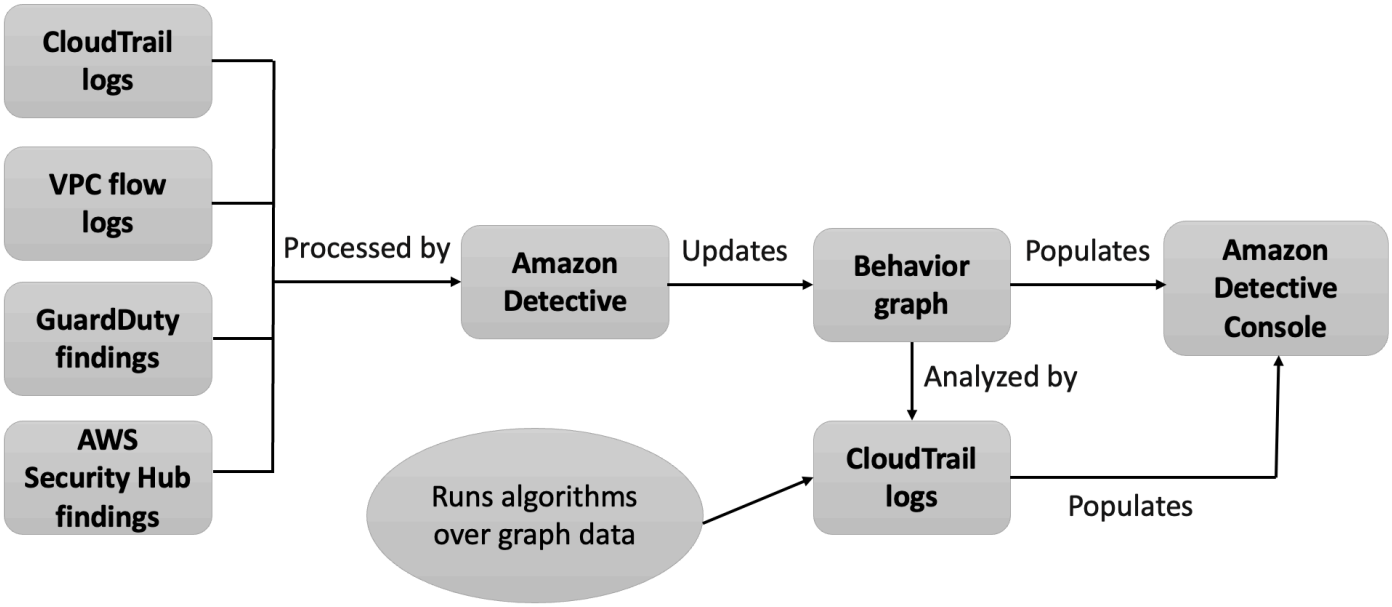
- Amazon Virtual Private Cloud(Amazon VPC) 및를 포함한 로그 데이터 AWS CloudTrail

- Amazon GuardDuty의 조사 결과
- 의 결과 AWS Security Hub CSPM

동작 그래프에 사용되는 소스 데이터에 대한 자세한 내용은 동작 그래프에 사용되는 소스 데이터를 참조하세요.

Detective에서 소스 데이터를 처리하는 방법

Detective는 새 데이터가 수신되면 추출과 분석을 조합하여 동작 그래프를 채웁니다.



Detective 추출

추출은 구성된 매핑 규칙을 기반으로 합니다. 매핑 규칙에는 기본적으로 “이 데이터를 볼 때마다 특정 방식으로 사용하여 동작 그래프 데이터를 업데이트하세요.”라고 되어 있습니다.

예를 들어, 수신되는 Detective 소스 데이터 레코드에는 IP 주소가 포함될 수 있습니다. 그럴 경우 Detective는 해당 레코드의 정보를 사용하여 새 IP 주소 엔터티를 만들거나 기존 IP 주소 엔터티를 업데이트합니다.

Detective 분석

분석은 데이터를 분석하여 엔터티와 관련된 활동에 대한 인사이트를 제공하는 보다 복잡한 알고리즘입니다.

예를 들어, 한 가지 유형의 Detective 분석은 알고리즘을 실행하여 활동이 발생하는 빈도를 분석합니다. API를 호출하는 엔터티의 경우 알고리즘은 엔터티가 일반적으로 사용하지 않는 API 직접 호출을 찾습니다. 또한 이 알고리즘은 API 직접 호출 수가 크게 증가하는 경우를 찾아냅니다.

분석 인사이트는 분석가의 주요 질문에 대한 답변을 제공하여 조사를 지원하며, 조사 결과 및 엔터티 프로필 패널을 채우는 데 자주 사용됩니다.

새 Detective 동작 그래프의 훈련 기간

조사 결과 조사의 한 가지 방법은 조사 결과 범위 시간 동안의 활동을 조사 결과가 탐지되기 전에 발생한 활동과 비교하는 것입니다. 이전에는 없었던 활동이 의심스러울 가능성이 더 높을 수 있습니다.

일부 Amazon Detective 프로필 패널은 조사 결과 전 기간 동안 관찰되지 않은 활동을 강조 표시합니다. 일부 프로필 패널에는 범위 시간 이전 45일 동안의 평균 활동을 보여주는 기준값도 표시됩니다. 범위 시간은 시간 경과에 따른 개체의 활동을 요약한 것입니다.

동작 그래프에서 더 많은 데이터를 추출할수록 Detective는 조직의 정상적인 활동과 비정상적 활동을 보다 정확하게 파악합니다.

그러나 이러한 그림을 만들려면 Detective가 최소 2주 분량의 데이터에 액세스해야 합니다. 동작 그래프의 계정 수에 따라 Detective 분석의 성숙도도 증가합니다.

Detective를 활성화한 후 처음 2주는 훈련 기간으로 간주됩니다. 이 기간 동안 범위 시간 활동을 이전 활동과 비교하는 프로필 패널에는 Detective가 훈련 중이라는 메시지가 표시됩니다.

평가판 기간 동안 Detective는 동작 그래프에 가능한 한 많은 멤버 계정을 추가할 것을 권장합니다. 이를 통해 Detective에 더 큰 데이터 풀이 제공되므로 조직의 정상적인 활동을 보다 정확하게 파악할 수 있습니다.

동작 그래프 데이터 구조 개요

동작 그래프 데이터 구조는 추출 및 분석된 데이터의 구조를 정의합니다. 또한 소스 데이터를 동작 그래프에 매핑하는 방법도 정의합니다.

동작 그래프 데이터 구조의 요소 유형

동작 그래프 데이터 구조는 다음 정보 요소로 이루어집니다.

엔터티

엔터티는 Detective 소스 데이터에서 추출한 항목을 나타냅니다.

각 엔터티에는 엔터티가 나타내는 객체 유형을 식별하는 유형이 있습니다. 개체 유형의 예로는 IP 주소, Amazon EC2 인스턴스 및 AWS 사용자가 있습니다.

각 엔터티의 소스 데이터는 엔터티 속성을 채우는 데에도 사용됩니다. 속성 값은 소스 레코드에서 직접 추출하거나 여러 레코드에서 집계할 수 있습니다.

일부 속성은 단일 스칼라 또는 집계된 값으로 구성됩니다. 예를 들어, EC2 인스턴스의 경우 Detective는 인스턴스 유형 및 처리된 총 바이트 수를 추적합니다.

시계열 속성은 시간 경과에 따른 활동을 추적합니다. 예를 들어, EC2 인스턴스의 경우 Detective는 시간 경과에 따라 해당 인스턴스가 사용한 고유 포트를 추적합니다.

관계

관계는 개별 엔터티 간에 발생하는 활동을 나타냅니다. Detective 소스 데이터에서도 관계가 추출됩니다.

엔터티와 마찬가지로 관계에도 유형이 있으며, 이를 통해 관련된 엔터티의 유형과 연결 방향을 식별할 수 있습니다. 관계 유형의 예로는 EC2 인스턴스에 연결하는 IP 주소가 있습니다.

Detective는 특정 인스턴스에 연결하는 특정 IP 주소와 같은 각 개별 관계에 대해 시간 경과에 따른 발생 상황을 추적합니다.

동작 그래프 데이터 구조의 엔터티 유형

동작 그래프 데이터 구조는 다음을 수행하는 엔터티 및 관계 유형으로 구성됩니다.

- 사용 중인 서버, IP 주소, 사용자 에이전트 추적
- 사용 중인 AWS 사용자, 역할 및 계정 추적
- AWS 환경에서 발생하는 네트워크 연결 및 권한 부여 추적

동작 그래프 데이터 구조에는 다음과 같은 엔터티 유형이 포함됩니다.

AWS 계정

AWS Detective 소스 데이터에 있는 계정.

Detective는 각 계정에 대해 다음과 같은 몇 가지 질문에 답변합니다.

- 해당 계정에서 사용한 API 직접 호출은 무엇입니까?
- 해당 계정에서 사용한 사용자 에이전트는 무엇입니까?

- 해당 계정에서 사용한 자율 시스템 조직(ASO)은 무엇입니까?
- 해당 계정이 활성화된 지리적 위치는 어디입니까?

AWS 역할

AWS Detective 소스 데이터에 있는 역할입니다.

Detective는 각 역할에 대해 다음과 같은 몇 가지 질문에 답변합니다.

- 해당 역할에서 사용한 API 직접 호출은 무엇입니까?
- 해당 역할에서 사용한 사용자 에이전트는 무엇입니까?
- 해당 역할에서 사용한 ASO는 무엇입니까?
- 해당 역할이 활성화된 지리적 위치는 어디입니까?
- 이 역할을 맡은 리소스는 무엇입니까?
- 이 역할을 맡은 역할은 무엇입니까?
- 이 역할과 관련된 역할 세션은 무엇입니까?

AWS 사용자

AWS Detective 소스 데이터에 있는 사용자.

Detective는 각 사용자에 대해 다음과 같은 몇 가지 질문에 답변합니다.

- 해당 사용자가 사용한 API 직접 호출은 무엇입니까?
- 해당 사용자가 사용한 사용자 에이전트는 무엇입니까?
- 해당 사용자가 활성화된 지리적 위치는 어디입니까?
- 이 사용자를 맡은 역할은 무엇입니까?
- 이 사용자와 관련된 역할 세션은 무엇입니까?

페더레이션 사용자

페더레이션 사용자의 인스턴스. 페더레이션 사용자의 예는 다음과 같습니다.

- Security Assertion Markup Language(SAML)를 사용하여 로그인하는 자격 증명
- 웹 ID 페더레이션을 사용하여 로그인하는 자격 증명

Detective는 각 페더레이션 사용자에 대해 다음과 같은 몇 가지 질문에 답변합니다.

- 페더레이션 사용자가 인증한 자격 증명 공급자는 무엇입니까?
- 페더레이션 사용자의 대상은 무엇입니까? 대상은 페더레이션 사용자의 웹 자격 증명 토큰을 요청한 애플리케이션을 식별합니다.
- 페더레이션 사용자가 활성화된 지리적 위치는 어디입니까?

- 페더레이션 사용자가 사용한 사용자 에이전트는 무엇입니까?
- 페더레이션 사용자가 사용한 ASO는 무엇입니까?
- 이 페더레이션 사용자를 맡은 역할은 무엇입니까?
- 이 페더레이션 사용자와 관련된 역할 세션은 무엇입니까?

EC2 인스턴스

Detective 소스 데이터에 있는 EC2 인스턴스.

Detective는 EC2 인스턴스에 대해 다음과 같은 몇 가지 질문에 답변합니다.

- 인스턴스와 통신한 IP 주소는 무엇입니까?
- 인스턴스와 통신하는 데 사용된 포트는 무엇입니까?
- 인스턴스와 주고받은 데이터의 양은 얼마입니까?
- 인스턴스가 포함된 VPC는 무엇입니까?
- EC2 인스턴스에서 사용한 API 직접 호출은 무엇입니까?
- EC2 인스턴스에서 사용한 사용자 에이전트는 무엇입니까?
- EC2 인스턴스에서 사용한 ASO는 무엇입니까?
- EC2 인스턴스가 활성화된 지리적 위치는 어디입니까?
- EC2 인스턴스를 맡은 역할은 무엇입니까?

역할 세션

역할을 수임하고 있는 리소스의 인스턴스. 각 역할 세션은 역할 식별자와 세션 이름으로 식별됩니다.

Detective는 각 역할에 대해 다음과 같은 몇 가지 질문에 답변합니다.

- 이 역할 세션에 참여한 리소스는 무엇입니까? 즉, 어떤 역할을 맡았고, 어떤 리소스가 해당 역할을 맡았습니까?

  단, 크로스 계정 역할 수임에서는 Detective에서 역할을 맡은 리소스를 식별할 수 없습니다.
- 해당 역할 섹션에서 사용한 API 직접 호출은 무엇입니까?
- 해당 역할 세션에서 사용한 사용자 에이전트는 무엇입니까?
- 해당 역할 세션에서 사용한 ASO는 무엇입니까?
- 해당 역할 세션이 활성화된 지리적 위치는 어디입니까?
- 이 역할 세션을 시작한 사용자 또는 역할은 무엇입니까?
- 이 역할 세션을 시작한 역할 세션은 무엇입니까?

조사 결과

Amazon GuardDuty에서 발견한 조사 결과를 Detective 소스 데이터에 입력했습니다.

각 조사 결과에 대해 Detective는 조사 결과 유형, 출처 및 조사 결과 활동의 기간을 추적합니다.

또한 탐지된 활동과 관련된 역할 또는 IP 주소와 같은 조사 결과와 관련된 정보도 저장합니다.

IP 주소

Detective 소스 데이터에 있는 IP 주소.

Detective는 각 IP 주소에 대해 다음과 같은 몇 가지 질문에 답변합니다.

- IP 주소가 사용한 API 직접 호출은 무엇입니까?
- IP 주소가 사용한 포트는 무엇입니까?
- IP 주소가 사용한 사용자 및 사용자 에이전트는 무엇입니까?
- 해당 IP 주소가 활성화된 지리적 위치는 어디입니까?
- 이 IP 주소가 할당되고 통신한 EC2 인스턴스는 무엇입니까?

S3 버킷

Detective 소스 데이터에 있는 S3 버킷

Detective는 각 S3 버킷에 대해 다음과 같은 몇 가지 질문에 답변합니다.

- S3 버킷과 상호 작용한 보안 주체는 무엇입니까?
- S3 버킷에 이루어진 API 직접 호출은 무엇입니까?
- 보안 주체가 S3 버킷으로 API 직접 호출을 수행한 지리적 위치는 어디입니까?
- S3 버킷과 상호 작용하는 데 사용된 사용자 에이전트는 무엇입니까?
- S3 버킷과 상호 작용하는 데 사용된 ASO는 무엇입니까?

S3 버킷을 삭제한 다음 같은 이름으로 새 버킷을 만들 수 있습니다. Detective는 S3 버킷 이름을 사용하여 S3 버킷을 식별하므로 이를 단일 S3 버킷 엔터티로 취급합니다. 엔터티 프로필에서 생성 시간은 첫 번째 생성 시간입니다. 삭제 시간은 가장 최근의 삭제 시간입니다.

모든 생성 및 삭제 이벤트를 보려면 생성 시간부터 시작하고 삭제 시간까지 종료되도록 범위 시간을 설정합니다. 전체 API 직접 호출량 프로필 패널에서 범위 시간에 대한 활동 세부 정보를 표시합니다. API 메서드를 필터링하여 `Create` 및 `Delete` 메서드를 표시합니다. the section called “전체 API 직접 호출량”을(를) 참조하세요.

사용자 에이전트

Detective 소스 데이터에 있는 사용자 에이전트.

Detective는 각 사용자 에이전트에 대해 다음과 같은 질문에 답변합니다.

- 사용자 에이전트가 사용한 API 직접 호출은 무엇입니까?
- 사용자 에이전트가 사용한 사용자 및 역할은 무엇입니까?
- 사용자 에이전트가 사용한 IP 주소는 무엇입니까?

EKS 클러스터

Detective 소스 데이터에 있는 EKS 클러스터.

> **Note**
>
> 이 엔터티 유형에 대한 전체 세부 정보를 보려면 선택적 EKS 감사 로그 데이터 소스를 활성화해야 합니다. 자세한 내용은 선택적 데이터 소스를 참조하세요.

Detective는 각 EKS 클러스터에 대해 다음과 같은 질문에 답변합니다.

- 이 클러스터에서 실행한 Kubernetes API 직접 호출은 무엇입니까?
- 이 클러스터에서 활성화된 Kubernetes 사용자 및 서비스 계정(보안 주체)은 무엇입니까?
- 이 클러스터에서 시작된 컨테이너는 무엇입니까?
- 이 클러스터에서 컨테이너를 시작하는 데 사용되는 이미지는 무엇입니까?

Kubernetes 포드

Detective 소스 데이터에 있는 Kubernetes 포드.

> **Note**
>
> 이 엔터티 유형에 대한 전체 세부 정보를 보려면 선택적 EKS 감사 로그 데이터 소스를 활성화해야 합니다. 자세한 내용은 선택적 데이터 소스를 참조하세요.

Detective는 각 포드에 대해 다음과 같은 질문에 답변합니다.

- 내 계정에서 흔히 볼 수 있는 이 포드의 컨테이너 이미지는 무엇입니까?
- 이 포드에는 지시되는 활동은 무엇입니까?
- 이 포드에서 실행되는 컨테이너는 무엇입니까?
- 이 포드에 있는 컨테이너의 레지스트리를 내 계정에서 흔히 볼 수 있습니까?
- 워크로드의 다른 포드에서 실행 중인 다른 컨테이너는 무엇입니까?
- 이 포드에는 워크로드의 다른 포드에는 없는 변칙 컨테이너가 있습니까?

컨테이너 이미지

Detective 소스 데이터에 있는 컨테이너 이미지.

> **Note**
>
> 이 엔터티 유형에 대한 전체 세부 정보를 보려면 선택적 EKS 감사 로그 데이터 소스를 활성화해야 합니다. 자세한 내용은 선택적 데이터 소스를 참조하세요.

Detective는 각 컨테이너 이미지에 대해 다음과 같은 질문에 답변합니다.

- 내 환경에서 이 이미지와 동일한 리포지토리 또는 레지스트리를 공유하는 다른 이미지는 무엇입니까?
- 내 환경에서 실행 중인 이 이미지의 복사본은 몇 개입니까?

Kubernetes 객체

Detective 소스 데이터에 있는 Kubernetes 객체. Kubernetes 객체는 사용자 또는 서비스 계정입니다.

> **Note**
>
> 이 엔터티 유형에 대한 전체 세부 정보를 보려면 선택적 EKS 감사 로그 데이터 소스를 활성화해야 합니다. 자세한 내용은 선택적 데이터 소스를 참조하세요.

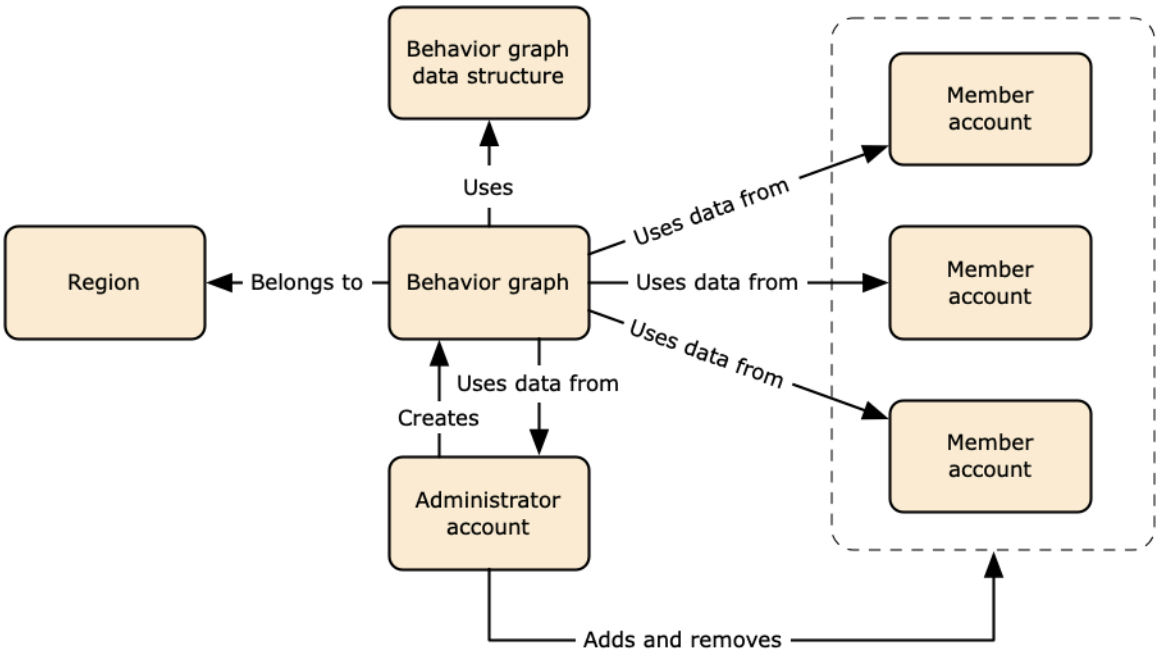
Detective는 각 객체에 대해 다음과 같은 질문에 답변합니다.

- 이 객체로 인증한 IAM 보안 주체는 무엇입니까?
- 이 객체와 관련된 조사 결과는 무엇입니까?
- 해당 객체가 사용하는 IP 주소는 무엇입니까?

Detective 동작 그래프에 사용되는 소스 데이터

Amazon Detective는 동작 그래프를 채우기 위해 동작 그래프 관리자 계정 및 멤버 계정의 소스 데이터를 사용합니다.

Detective를 사용하면 최대 1년 분량의 과거 이벤트 데이터에 액세스할 수 있습니다. 이 데이터는 선택한 기간 동안의 활동 유형 및 양의 변화를 보여주는 일련의 시각화를 통해 제공됩니다. Detective는 이러한 변경 사항을 GuardDuty 조사 결과와 연결합니다.



동작 그래프 데이터 구조에 대한 자세한 내용은 Detective 사용 설명서의 동작 그래프 데이터 구조 개요를 참조하세요.

Detective의 핵심 데이터 소스 유형

Detective는 다음과 같은 유형의 AWS 로그에서 데이터를 수집합니다.

- AWS CloudTrail 로그
- Amazon Virtual Private Cloud(VPC) 흐름 로그
  - IPv4 및 IPv6 레코드를 모두 수집하지만 Elastic Fabric Adapter에서 생성한 MAC 레코드는 수집하지 않습니다.
  - `log-status` 필드 값이 OK 상태일 때 로그 레코드를 수집합니다. 자세한 내용은 Amazon VPC 사용 설명서의 흐름 로그 레코드를 참조하세요.
  - 해당 VPCs에서만 실행되는 Amazon Elastic Compute Cloud 인스턴스에서 생성된 흐름 로그를 수집합니다. NAT 게이트웨이, RDS 인스턴스 또는 Fargate 클러스터와 같은 다른 리소스는 사용되지 않습니다.
  - 수락된 트래픽과 거부된 트래픽을 모두 수집합니다.
- GuardDuty에 등록된 계정의 경우 Detective는 GuardDuty 조사 결과도 수집합니다.

Detective는 CloudTrail 및 VPC 흐름 로그의 독립적이고 중복된 스트림을 통해 CloudTrail 및 VPC 흐름 로그 이벤트를 사용합니다. 이러한 프로세스는 기존 CloudTrail 및 VPC 흐름 로그 구성에 영향을 주거

나 이를 사용하지 않습니다. 또한 이러한 서비스의 성능에 영향을 미치거나 비용을 증가시키지 않습니다.

Detective의 선택적 데이터 소스 유형

Detective는 Detective 코어 패키지에 제공되는 세 가지 데이터 소스 외에도 선택적 소스 패키지를 제공합니다(코어 패키지에는 AWS CloudTrail 로그, VPC 흐름 로그 및 GuardDuty 조사 결과가 포함됨). 동작 그래프의 선택적 데이터 소스 패키지는 언제든지 시작하거나 중지할 수 있습니다.

Detective는 리전별 모든 핵심 및 선택적 소스 패키지에 대해 30일 무료 평가판을 제공합니다.

> **Note**
>
> Detective는 각 데이터 소스 패키지에서 받은 모든 데이터를 최대 1년 동안 보관합니다.

현재 사용 가능한 선택적 소스 패키지는 다음과 같습니다.

- EKS 감사 로그

  이 선택적 데이터 소스 패키지를 사용하면 Detective가 사용자 환경의 EKS 클러스터에 대한 세부 정보를 수집하고 해당 데이터를 동작 그래프에 추가할 수 있습니다. Detective는 이러한 로그를 수동으로 활성화하거나 저장할 필요 없이 사용자 활동과 AWS CloudTrail 관리 이벤트 및 네트워크 활동을 Amazon VPC 흐름 로그와 상호 연관시킵니다. 세부 정보는 Amazon EKS 감사 로그 섹션을 참조하세요.
- AWS 보안 조사 결과

  이 선택적 데이터 소스 패키지를 사용하면 Detective가 Security Hub CSPM에서 데이터를 수집하고 해당 데이터를 동작 그래프에 추가할 수 있습니다. 세부 정보는 AWS 보안 조사 결과 섹션을 참조하세요.

선택적 데이터 소스 시작 또는 중지:

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 선택적 소스 패키지에서 업데이트를 선택합니다. 그런 다음 활성화하려는 데이터 소스를 선택하거나 이미 활성화된 데이터 소소의 확인란을 선택 취소하고 업데이트를 선택하여 활성화된 데이터 소스 패키지를 변경합니다.

> **Note**
>
> 선택적 데이터 소스를 중지했다가 다시 시작하면 일부 엔터티 프로필에 표시된 데이터에 차이가 있는 것을 확인할 수 있습니다. 이 차이는 콘솔 디스플레이에 표시되며 데이터 소스가 중지된 기간을 나타냅니다. 데이터 소스가 재시작되면 Detective는 데이터를 소급하여 수집하지 않습니다.

Amazon EKS 감사 로그

Amazon EKS 감사 로그는 Detective 행동 그래프에 추가할 수 있는 선택적 데이터 소스 패키지입니다. 콘솔의 설정 페이지 또는 Detective API를 통해 계정에서 사용 가능한 선택적 소스 패키지와 해당 상태를 볼 수 있습니다.

이 데이터 소스에 대해 30일 무료 평가판이 제공됩니다. 자세한 내용은 선택적 데이터 소스에 대한 무료 평가판 섹션을 참조하세요.

Amazon EKS 감사 로그를 활성화하면 Detective에서 Amazon EKS로 생성한 리소스에 대한 심층적인 정보를 동작 그래프에 추가할 수 있습니다. 이 데이터 소스는 EKS 클러스터, Kubernetes 포드, 컨테이너 이미지 및 Kubernetes 객체와 같은 엔터티 유형에 대해 제공된 정보를 개선합니다.

또한 Amazon GuardDuty에서 EKS 감사 로그를 데이터 소스로 활성화한 경우 GuardDuty에서 Kubernetes 조사 결과에 대한 세부 정보를 볼 수 있습니다. GuardDuty에서 이 데이터 소스를 활성화하는 방법에 대한 자세한 내용은 Amazon GuardDuty의 Kubernetes 보호를 참조하세요.

> **Note**
>
> 이 데이터 소스는 2022년 7월 26일 이후에 생성된 새 동작 그래프에 대해 기본적으로 활성화됩니다. 2022년 7월 26일 이전에 만든 동작 그래프의 경우 수동으로 활성화해야 합니다.

Amazon EKS 감사 로그를 선택적 데이터 소스로 추가 또는 제거:

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 소스 패키지에서 EKS 감사 로그를 선택하여 이 데이터 소스를 활성화합니다. 이미 활성화되어 있는 경우 다시 선택하면 EKS 감사 로그가 동작 그래프에 수집되는 것을 중지할 수 있습니다.

AWS 보안 조사 결과

AWS 보안 조사 결과는 Detective 동작 그래프에 추가할 수 있는 선택적 데이터 소스 패키지입니다.

콘솔의 설정 페이지 또는 Detective API를 통해 계정에서 사용 가능한 선택적 소스 패키지와 해당 상태를 볼 수 있습니다.

이 데이터 소스에 대해 30일 무료 평가판이 제공됩니다. 자세한 내용은 선택적 데이터 소스에 대한 무료 평가판 섹션을 참조하세요.

AWS 보안 조사 결과를 활성화하면 Detective는 AWS Security Format(ASFF)이라는 표준 조사 결과 형식으로 Security Hub에서 집계한 Security Hub CSPM의 조사 결과를 업스트림 서비스에서 사용할 수 있으므로 시간이 많이 걸리는 데이터 변환 작업이 필요하지 않습니다. 그러면 가장 중요한 제품에 우선 순위를 부여하기 위해 제품 전반에 걸쳐 수집된 조사 결과를 상호 연관시킵니다.

AWS 보안 조사 결과를 선택적 데이터 소스로 추가 또는 제거:

> **Note**
>
> AWS 보안 조사 결과 데이터 소스는 2023년 5월 16일 이후에 생성된 새 동작 그래프에 대해 기본적으로 활성화됩니다. 2023년 5월 16일 이전에 만든 동작 그래프의 경우 수동으로 활성화해야 합니다.

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 소스 패키지에서 AWS 보안 조사 결과를 선택하여이 데이터 소스를 활성화합니다. 이미 활성화되어 있는 경우 다시 선택하면 AWS Security Finding Format(AWS ASFF) 조사 결과를 동작 그래프에 수집하는 것을 중지할 수 있습니다.

현재 지원되는 조사 결과

Detective는 Amazon 또는가 소유한 서비스에서 Security Hub CSPM의 모든 ASFF 결과를 수집합니다 AWS.

- 지원되는 서비스 통합 목록을 보려면 AWS Security Hub 사용 설명서의 사용 가능한 AWS 서비스 통합을 참조하세요.
- 지원되는 리소스 목록은 AWS Security Hub 사용 설명서의 리소스를 참조하세요.

- AWS 규정 준수 상태가 로 설정되지 않은 서비스 조사 결과 FAILED 및 교차 리전 집계 조사 결과는 수집되지 않습니다.

Detective가 소스 데이터를 수집하고 저장하는 방법

Detective가 활성화되면 Detective는 동작 그래프 관리자 계정에서 소스 데이터를 수집하기 시작합니다. 멤버 계정이 동작 그래프에 추가되면 Detective는 해당 멤버 계정의 데이터도 사용하기 시작합니다.

Detective 소스 데이터는 원본 피드의 구조화된 버전과 처리된 버전으로 구성됩니다. Detective 분석을 지원하기 위해 Detective는 Detective 소스 데이터의 사본을 저장합니다.

Detective 수집 프로세스는 Detective 소스 데이터 스토어의 Amazon Simple Storage Service(S3) 버킷에 데이터를 제공합니다. 새 소스 데이터가 도착하면 다른 Detective 구성 요소가 데이터를 수집하여 추출 및 분석 프로세스를 시작합니다. 자세한 내용은 Detective 사용 설명서의 Detective가 소스 데이터를 사용하여 동작 그래프를 채우는 방법 참조하세요.

Detective가 동작 그래프의 데이터 볼륨 할당량을 적용하는 방법

Detective는 각 동작 그래프에서 허용하는 데이터의 볼륨에 대해 엄격한 할당량을 적용합니다. 데이터 볼륨은 Detective 동작 그래프에 유입되는 일일 데이터 양입니다.

Detective는 관리자 계정이 Detective를 활성화하고 멤버 계정이 동작 그래프에 제공하도록 초대를 수락할 때 이러한 할당량을 적용합니다.

- 관리자 계정의 데이터 볼륨이 하루 10TB를 초과하는 경우 관리자 계정에서 Detective를 활성화할 수 없습니다.
- 멤버 계정에서 추가된 데이터 볼륨으로 인해 동작 그래프가 하루 10TB를 초과하는 경우 멤버 계정을 활성화할 수 없습니다.

동작 그래프의 데이터 볼륨은 시간 경과에 따라 자연스럽게 증가할 수도 있습니다. Detective는 매일 동작 그래프 데이터 볼륨을 확인하여 할당량을 초과하지 않는지 확인합니다.

동작 그래프 데이터 볼륨이 할당량에 가까워지면 Detective는 콘솔에 경고 메시지를 표시합니다. 할당량을 초과하지 않도록 멤버 계정을 제거할 수 있습니다.

동작 그래프 데이터 용량이 하루 10TB를 초과하는 경우 동작 그래프에 새 멤버 계정을 추가할 수 없습니다.

동작 그래프 데이터 용량이 하루 15TB를 초과하는 경우 Detective는 동작 그래프에 대한 데이터 수집을 중단합니다. 일일 15TB 할당량은 일반적인 데이터 볼륨과 데이터 볼륨 급증을 모두 반영합니다. 이 할당량에 도달하면 동작 그래프에 새 데이터가 수집되지 않지만 기존 데이터는 제거되지 않습니다. 해당 과거 데이터를 조사에 계속 사용할 수 있습니다. 콘솔에 동작 그래프에 대한 데이터 수집이 일시 중단되었음을 알리는 메시지가 표시됩니다.

데이터 수집이 일시 중지된 경우를 사용하여 다시 활성화 지원 해야 합니다. 가능하면에 문의하기 전에 멤버 계정을 제거하여 할당량 미만의 데이터 볼륨을 가져오 지원십시오. 그러면 동작 그래프에 대한 데이터 수집을 다시 활성화하기가 더 쉬워집니다.

Detective 요약 대시보드 사용

Amazon Detective의 요약 대시보드를 사용하여 지난 24시간 동안 활동의 출처를 조사할 엔터티를 식별합니다. Amazon Detective 요약 대시보드를 사용하면 특정 유형의 비정상적인 활동과 관련된 엔터티를 식별할 수 있습니다. 이는 조사를 시작할 수 있는 여러 가지 시작점 중 하나입니다.

요약 대시보드를 표시하려면 Detective 탐색 창에서 요약을 선택합니다. Detective 콘솔을 처음 열 때 요약 대시보드도 기본적으로 표시됩니다.

요약 대시보드에서 다음 기준을 충족하는 엔터티를 식별할 수 있습니다.

- Detective에서 식별한 잠재적 보안 이벤트를 보여주는 조사
- 새로 관찰된 지리적 위치에서 발생한 활동과 관련된 엔터티
- API 직접 호출 횟수가 가장 많은 엔터티
- 트래픽이 가장 많았던 EC2 인스턴스
- 컨테이너 수가 가장 많은 컨테이너 클러스터

각 요약 대시보드 패널에서 선택한 개체의 프로필로 피벗할 수 있습니다.

요약 대시보드를 검토할 때 범위 시간을 조정하여 지난 365일 동안 24시간 동안의 활동을 볼 수 있습니다. 시작 날짜 및 시간을 변경하면 종료 날짜 및 시간이 선택한 시작 시간으로부터 24시간 후로 자동 업데이트됩니다.

Detective를 사용하면 최대 1년 분량의 과거 이벤트 데이터에 액세스할 수 있습니다. 이 데이터는 선택한 기간 동안의 활동 유형 및 양의 변화를 보여주는 일련의 시각화를 통해 제공됩니다. Detective는 이러한 변경 사항을 GuardDuty 조사 결과와 연결합니다.

Detective의 소스 데이터에 대한 자세한 내용은 동작 그래프에 사용된 소스 데이터를 참조하세요.

조사

조사를 통해 Detective에서 식별한 잠재적 보안 이벤트를 확인할 수 있습니다. 조사 패널에서는 심각한 조사 결과와 일정 기간 동안 보안 이벤트의 영향을 받은 해당 AWS 역할 및 사용자를 볼 수 있습니다. 조사는 손상 지표를 그룹화하여 AWS 리소스가 악의적인 행동과 그 영향을 나타낼 수 있는 비정상적인 활동에 관여하고 있는지 확인하는 데 도움이 됩니다.

모든 조사 보기를 선택하여 조사 결과를 검토하고, 조사 결과 그룹 및 리소스 세부 정보를 분류하여 보안 조사를 가속화합니다. 선택한 범위 시간에 따라 조사가 표시됩니다. 범위 시간을 조정하여 지난 365

일간의 조사를 24시간 단위로 볼 수 있습니다. 심각한 조사 결과로 바로 전환하여 자세한 조사 보고서를 볼 수 있습니다.

의심스러운 활동이 있는 것으로 보이는 AWS 역할 또는 사용자를 식별하는 경우 조사 패널에서 역할 또는 사용자로 직접 피벗하여 조사를 계속할 수 있습니다. 역할 또는 사용자로 전환하고 조사 실행을 클릭하여 조사 보고서를 생성합니다. 역할 또는 사용자에 대해 조사를 실행하면 역할 또는 사용자가 조사됨 탭으로 이동합니다.

새로 관찰된 지리적 위치

새로 관찰된 지리적 위치는 이전 24시간 동안 활동의 출처였지만 그 이전의 기준선 기간에는 볼 수 없었던 지리적 위치를 강조 표시합니다.

패널에는 최대 100개의 지리적 위치가 포함됩니다. 위치는 지도에 표시되며 지도 아래 표에 나열되어 있습니다.

각 지리적 위치에 대해 테이블에는 지난 24시간 동안 해당 지리적 위치에서 이루어진 API 직접 호출 실패 및 성공 수가 표시됩니다.

각 지리적 위치를 확장하여 해당 지리적 위치에서 API를 직접 호출한 사용자 및 역할 목록을 표시할 수 있습니다. 테이블에는 각 보안 주체에 대한 유형과 관련 AWS 계정가 나열되어 있습니다.

의심스러운 사용자 또는 역할을 식별한 경우 패널에서 직접 사용자 또는 역할 프로필로 피벗하여 조사를 계속할 수 있습니다. 프로필로 피벗하려면 사용자 또는 역할 식별자를 선택합니다.

Detective는 MaxMind GeoIP 데이터베이스를 사용하여 요청 위치를 결정합니다. MaxMind는 국가 수준에서 매우 높은 데이터 정확도를 보고하지만, 정확도는 국가 및 IP 유형과 같은 요인에 따라 다릅니다. MaxMind에 대한 자세한 내용은 MaxMind IP 지리적 위치를 참조하세요. GeoIP 데이터가 잘못되었다고 생각되면 Maxmind(MaxMind Correct GeoIP2 Data)에 정정 요청을 제출할 수 있습니다.

지난 7일간의 활동 조사 결과 그룹

지난 7일 동안의 활성 조사 결과 그룹은 지정된 기간 동안 발생한 환경 내 Detective 조사 결과, 엔터티 및 증거를 상호 연관시켜 그룹화합니다. 이러한 그룹화는 악의적인 동작을 나타낼 수 있는 비정상적인 활동과 연관되어 있습니다. 요약 대시보드에는 지난 주에 활성 상태였던 가장 중요한 조사 결과가 포함된 그룹별로 정렬된 그룹이 최대 5개까지 표시됩니다.

전술, 계정, 리소스 및 조사 결과 콘텐츠에서 값을 선택하여 자세한 내용을 볼 수 있습니다.

조사 결과 그룹은 매일 생성됩니다. 관심 있는 조사 결과 그룹을 식별한 경우 제목을 선택하여 그룹 프로필의 세부 보기로 이동해 조사를 계속할 수 있습니다.

API 직접 호출량이 가장 많은 역할 및 사용자

API 직접 호출량이 가장 많은 역할 및 사용자는 지난 24시간 동안 API 직접 호출을 가장 많이 한 사용자와 역할을 식별합니다.

패널에는 최대 100명의 사용자 및 역할이 포함될 수 있습니다. 각 사용자 또는 역할에 대해 유형(사용자 또는 역할) 및 관련 계정을 볼 수 있습니다. 또한 지난 24시간 동안 해당 사용자 또는 역할이 실행한 API 직접 호출 수를 확인할 수 있습니다.

기본적으로 서비스 연결 역할이 표시됩니다. 서비스 연결 역할은 대량의 AWS CloudTrail 활동을 생성하여 추가로 조사하려는 보안 주체를 대체할 수 있습니다. 서비스 연결 역할 표시를 끄고 요약 대시보드 보기에서 서비스 연결 역할을 필터링하도록 선택할 수 있습니다.

이 패널의 데이터가 포함된 쉼표로 구분된 값(.csv) 파일을 내보낼 수 있습니다.

또한 이전 7일간의 API 직접 호출량 타임라인도 있습니다. 타임라인을 통해 해당 보안 주체의 API 직접 호출 양이 비정상적인지 여부를 확인할 수 있습니다.

API 직접 호출량이 의심스러운 사용자 또는 역할을 식별한 경우 패널에서 직접 사용자 또는 역할 프로필로 피벗하여 조사를 계속할 수 있습니다. 사용자 또는 역할과 관련된 계정의 프로필도 볼 수 있습니다. 프로필을 보려면 사용자, 역할 또는 계정 식별자를 선택합니다.

트래픽 볼륨이 가장 많은 EC2 인스턴스

트래픽 볼륨이 가장 많은 EC2 인스턴스는 지난 24시간 동안 총 트래픽량이 가장 많았던 EC2 인스턴스를 식별합니다.

패널에는 최대 100개의 EC2 인스턴스가 포함될 수 있습니다. 각 EC2 인스턴스에 대해 관련 계정과 지난 24시간 동안의 인바운드 바이트 수, 아웃바운드 바이트 수, 총 바이트 수를 볼 수 있습니다.

이 패널의 데이터가 들어 있는 쉼표로 구분된 값(.csv) 파일을 내보낼 수 있습니다.

또한 지난 7일 동안의 인바운드 및 아웃바운드 트래픽을 보여주는 타임라인도 볼 수 있습니다. 타임라인은 해당 EC2 인스턴스의 트래픽 양이 비정상적인지 여부를 판단하는 데 도움이 될 수 있습니다.

트래픽 볼륨이 의심스러운 EC2 인스턴스를 식별한 경우 패널에서 직접 EC2 인스턴스 프로파일로 이동하여 조사를 계속할 수 있습니다. EC2 인스턴스를 소유한 계정의 프로필을 볼 수도 있습니다. 프로필을 보려면 EC2 인스턴스 또는 계정 식별자를 선택합니다.

Kubernetes 포드가 가장 많은 컨테이너 클러스터

가장 많은 Kubernetes 포드가 생성된 컨테이너 클러스터는 지난 24시간 동안 가장 많은 컨테이너를 실행한 클러스터를 식별합니다.

이 패널에는 관련 조사 결과가 가장 많은 클러스터를 기준으로 구성된 최대 100개의 클러스터가 포함됩니다. 각 클러스터에 대해 관련 계정, 해당 클러스터의 현재 컨테이너 수, 지난 24시간 동안 해당 클러스터와 관련된 조사 결과 수를 볼 수 있습니다. 이 패널의 데이터가 들어 있는 쉼표로 구분된 값(.csv) 파일을 내보낼 수 있습니다.

최근 조사 결과가 있는 클러스터를 식별한 경우 패널에서 클러스터 프로파일로 직접 이동하여 조사를 계속할 수 있습니다. 클러스터를 소유한 계정의 프로필로 피벗할 수도 있습니다. 프로필로 피벗하려면 클러스터 이름 또는 계정 식별자를 선택합니다.

대략적인 값 알림

API 직접 호출량이 가장 많은 역할 및 사용자와 트래픽 볼륨이 가장 많은 EC2 인스턴스에서 값 뒤에 별표(*)가 있으면 값이 근사치임을 의미합니다. 실제 값은 표시된 값과 같거나 더 큽니다.

이는 Detective가 각 시간 간격의 볼륨을 계산하는 데 사용하는 방법 때문에 발생합니다. 요약 페이지에서 시간 간격은 1시간입니다.

Detective는 매 시간마다 볼륨이 가장 큰 1,000개의 사용자, 역할 또는 EC2 인스턴스의 총 볼륨을 계산합니다. 나머지 사용자, 역할 또는 EC2 인스턴스에 대한 데이터는 제외됩니다.

리소스가 상위 1,000위 안에 드는 경우도 있고 그렇지 않은 경우 해당 리소스에 대해 계산된 볼륨에 모든 데이터가 포함되지 않을 수 있습니다. 상위 1,000위 내에 포함되지 않은 시간 간격의 데이터는 제외됩니다.

이는 요약 페이지에만 적용된다는 점에 유의하세요. 사용자, 역할 또는 EC2 인스턴스의 프로필은 정확한 세부 정보를 제공합니다.

Detective가 조사에 사용되는 방법

Amazon Detective를 사용하면 보안 조사 결과 또는 의심스러운 활동의 근본 원인을 분석 및 조사하고 신속하게 식별할 수 있습니다. Detective는 전체 조사 프로세스를 지원하는 도구를 제공합니다. Detective에서의 조사는 조사 결과, 조사 결과 그룹 또는 엔터티로부터 시작할 수 있습니다.

Detective의 조사 단계

모든 Detective 조사 프로세스에는 다음 단계가 포함됩니다.

심사

조사 프로세스는 악의적이거나 고위험 활동으로 의심되는 사례가 있다는 통지를 받으면 시작됩니다. 예를 들어, 사용자는 Amazon GuardDuty 및 Amazon Inspector와 같은 서비스에서 발견한 조사 결과 또는 경고를 조사하도록 배정됩니다.

심사 단계에서는 해당 활동이 참 긍정(진정한 악의적 활동)인지 아니면 거짓 긍정(악의적이거나 고위험 활동이 아님)인지 판단합니다. Detective 프로필은 관련 엔터티의 활동에 대한 통찰력을 제공하여 분류 프로세스를 지원합니다.

참 긍정 인스턴스의 경우 다음 단계로 넘어갑니다.

범위 지정

범위 지정 단계에서 분석가는 악의적 또는 고위험 활동의 범위와 근본 원인을 파악합니다.

범위 지정은 다음과 같은 유형의 질문에 대한 답을 제공합니다.

- 어떤 시스템과 사용자가 피해를 입었습니까?
- 공격이 어디에서 시작되었습니까?
- 공격이 일어난 지 얼마나 되었습니까?
- 밝혀내야 할 다른 관련 활동이 있습니까? 예를 들어 공격자가 시스템에서 데이터를 추출하는 경우 어떻게 데이터를 얻었을까요?

Detective 시각화는 관련되었거나 영향을 받은 다른 엔터티를 식별하는 데 도움이 될 수 있습니다.

응답

마지막 단계는 공격에 대응하여 공격을 막고 피해를 최소화하며 유사한 공격이 다시 발생하지 않도록 하는 것입니다.

탐지 조사의 시작점

Detective의 모든 조사에는 필수적인 시작점이 있습니다. 예를 들어 조사할 Amazon GuardDuty 또는 AWS Security Hub CSPM 조사 결과가 할당될 수 있습니다. 또는 특정 IP 주소의 비정상적인 활동이 우려될 수도 있습니다.

일반적인 조사 시작점에는 GuardDuty에서 탐지한 조사 결과 및 Detective 소스 데이터에서 추출한 엔터티가 포함됩니다.

GuardDuty에서 발견한 조사 결과

GuardDuty는 로그 데이터를 사용하여 악의적이거나 고위험 활동이 의심되는 사례를 찾아냅니다. Detective는 이러한 조사 결과를 조사하는 데 도움이 되는 리소스를 제공합니다.

각 조사 결과에 대해 Detective는 관련 조사 결과 세부 정보를 제공합니다. Detective는 결과에 연결된 IP 주소 및 AWS 계정과 같은 엔터티도 표시합니다.

그런 다음 관련 엔터티의 활동을 탐색하여 조사 결과에서 탐지된 활동이 진정한 우려 원인인지 확인할 수 있습니다.

자세한 내용은 the section called “조사 결과 개요” 단원을 참조하십시오.

AWS Security Hub CSPM에서 집계한 보안 조사 결과

AWS Security Hub CSPM 는 다양한 조사 결과 공급자의 보안 조사 결과를 한 곳에서 집계하고의 보안 상태에 대한 포괄적인 보기를 제공합니다 AWS. Security Hub CSPM은 여러 공급자의 대량 조사 결과를 해결하는 복잡성을 제거합니다. 이를 통해 모든 AWS 계정, 리소스 및 워크로드의 보안을 관리하고 개선하는 데 필요한 노력을 줄일 수 있습니다. Detective는 이러한 조사 결과를 조사하는 데 도움이 되는 리소스를 제공합니다.

각 조사 결과에 대해 Detective는 관련 조사 결과 세부 정보를 제공합니다. Detective는 결과에 연결된 IP 주소 및 AWS 계정과 같은 엔터티도 표시합니다.

자세한 내용은 the section called “조사 결과 개요” 단원을 참조하십시오.

Detective 소스 데이터에서 추출한 엔터티

수집된 Detective 소스 데이터에서 Detective는 IP 주소 및 AWS 사용자와 같은 엔터티를 추출합니다. 이중 하나를 조사 시작점으로 사용할 수 있습니다.

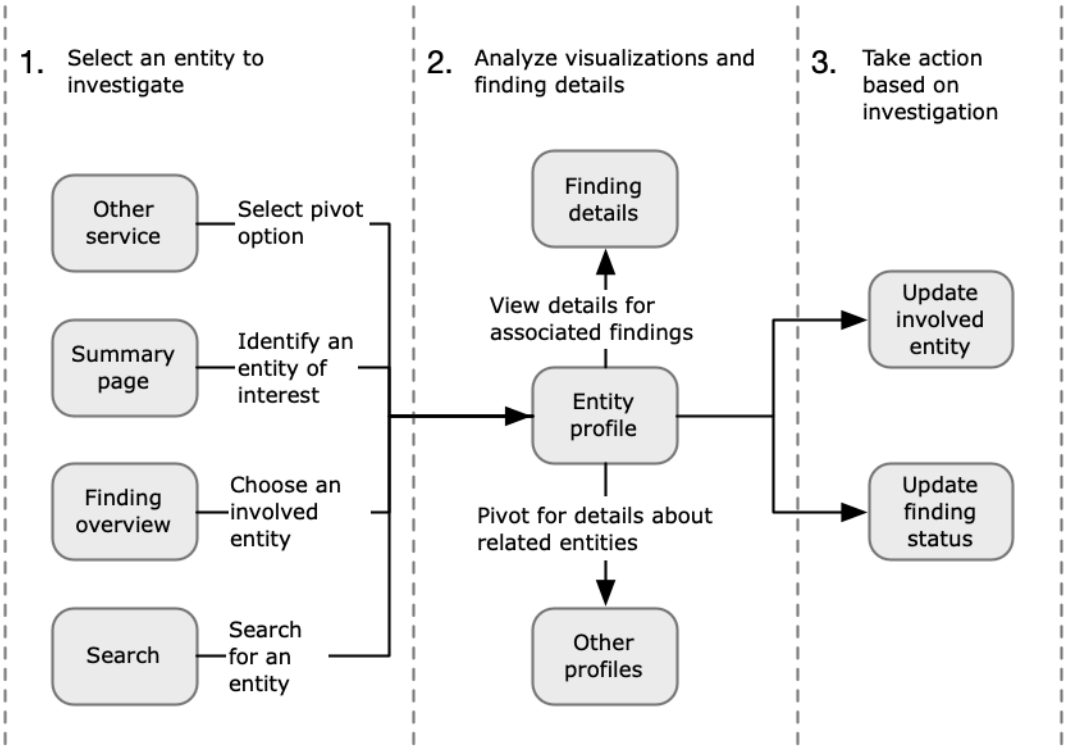
Detective는 IP 주소 또는 사용자 이름과 같은 엔터티에 대한 일반적인 세부 정보를 제공합니다. 또한 활동 기록에 대한 세부 정보도 제공합니다. 예를 들어 Detective는 엔터티가 연결되었거나 사용된 다른 IP 주소를 보고할 수 있습니다.

자세한 내용은 개체 분석 단원을 참조하십시오.

탐지 조사 흐름

Amazon Detective를 사용하여 EC2 인스턴스 또는 AWS 사용자와 같은 개체를 조사할 수 있습니다. 보안 조사 결과를 조사할 수도 있습니다.

다음 이미지는 Detective 조사 프로세스를 개괄적으로 보여줍니다.



1단계: 조사할 엔터티 선택

GuardDuty에서 조사 결과를 확인할 때 분석가는 Detective에서 관련 엔터티를 조사할 수 있습니다. the section called “다른 콘솔에서 피벗”을(를) 참조하세요.

엔터티를 선택하면 Detective의 엔터티 프로필로 이동합니다.

2단계: 프로필의 시각화 분석

각 엔터티 프로필에는 동작 그래프에서 생성된 시각화 세트가 포함되어 있습니다. 동작 그래프는 Detective에 입력되는 로그 파일 및 기타 데이터에서 생성됩니다.

시각화는 엔터티와 관련된 활동을 보여줍니다. 이러한 시각화를 사용하여 질문에 답하고 엔터티 활동이 비정상적인지 여부를 확인할 수 있습니다. 개체 분석을(를) 참조하세요.

각 시각화에 제공된 Detective 지침을 사용하면 조사를 안내하는 데 도움이 됩니다. 이 지침은 표시된 정보를 간략하게 설명하고, 질문할 질문을 제안하고, 답변을 기반으로 다음 단계를 제안합니다. the section called “프로필 패널 지침 사용”을(를) 참조하세요.

각 프로필에는 관련 결과 조사 결과가 포함되어 있습니다. 조사 결과에 대한 세부 정보 및 조사 결과 개요를 볼 수 있습니다. the section called “엔터티에 대한 조사 결과 보기”을(를) 참조하세요.

엔터티 프로필에서 다른 엔터티 및 조사 결과 프로필로 피벗하여 관련 자산의 활동을 더 자세히 조사할 수 있습니다.

3단계: 작업 수행

조사 결과에 따라 적절한 조치를 취합니다.

조사 결과가 거짓 긍정인 경우 조사 결과를 보관할 수 있습니다. Detective에서 GuardDuty 조사 결과를 보관할 수 있습니다. 자세한 내용은 Amazon GuardDuty 결과 보관을 참조하세요.

그렇지 않으면 적절한 조치를 취해 취약성을 해결하고 피해를 줄일 수 있습니다. 예를 들어 리소스 구성을 업데이트해야 할 수 있습니다.

탐지 조사

Amazon Detective 조사를 사용하여 침해 지표를 사용하여 IAM 사용자 및 IAM 역할을 조사할 수 있으며, 이를 통해 리소스가 보안 인시던트에 관여했는지 확인할 수 있습니다. 손상 지표(IOC)는 네트워크, 시스템 또는 환경에서 관찰된 아티팩트로, 높은 수준의 신뢰도로 악의적인 활동이나 보안 인시던트를 식별할 수 있습니다. Detective 조사를 사용하면 효율성을 극대화하고, 보안 위협에 집중하고, 발생률 대응 기능을 강화할 수 있습니다.

Detective 조사는 기계 학습 모델과 위협 인텔리전스를 사용하여 AWS 환경의 리소스를 자동으로 분석하여 잠재적 보안 인시던트를 식별합니다. 이를 통해 Detective의 동작 그래프를 기반으로 구축된 자동화를 사전 예방적이고 효과적이며 효율적으로 사용하여 보안 운영을 개선할 수 있습니다. Detective 조사를 사용하면 공격 전술, 불가능한 이동, 플래그가 지정된 IP 주소 및 조사 결과 그룹을 조사할 수 있습니다. 초기 보안 조사 단계를 수행하고 Detective에서 식별한 위험을 강조하는 보고서를 생성하여 보안 이벤트를 이해하고 잠재적 인시던트에 대응하는 데 도움을 줍니다.

주제

- Detective 조사 실행

- Detective 조사 보고서 검토
- Detective 조사 보고서 이해
- Detective 조사 보고서 요약
- Detective 조사 보고서 다운로드
- Detective 조사 보고서 보관

Detective 조사 실행

조사 실행을 사용하여 IAM 사용자 및 IAM 역할과 같은 리소스를 분석하고 조사 보고서를 생성할 수 있습니다. 생성된 보고서는 잠재적 손상을 나타내는 이상 동작을 자세히 설명합니다.

Console

Amazon Detective 콘솔을 사용하여 조사 페이지에서 Detective 조사를 실행하려면 다음 단계를 따르세요.

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 조사를 선택합니다.
3. 조사 페이지의 오른쪽 상단 모서리에서 조사 실행을 선택합니다.
4. 리소스 선택 섹션에는 조사를 실행하는 세 가지 방법이 있습니다. Detective에서 권장하는 리소스에 대한 조사를 실행하도록 선택할 수 있습니다. 특정 리소스에 대한 조사를 실행할 수 있습니다. Detective 검색 페이지에서 리소스를 조사할 수도 있습니다.

    1. `Choose a recommended resource` - Detective는 조사 결과 및 조사 결과 그룹의 활동을 기반으로 리소스를 권장합니다. Detective에서 권장하는 리소스에 대한 조사를 실행하려면 권장 리소스 테이블에서 조사할 리소스를 선택합니다.

        추천 리소스 테이블에서는 다음 세부 정보를 제공합니다.

        - 리소스 ARN - 리소스의 Amazon AWS 리소스 이름(ARN)입니다.
        - 조사 이유 - 리소스를 조사해야 하는 주요 이유를 표시합니다. Detective가 리소스 조사를 추천하는 이유는 다음과 같습니다.
            - 리소스가 지난 24시간 동안 심각도가 높은 검색 결과에 연루된 경우.
            - 리소스가 지난 7일 동안 관찰 대상 조사 결과 그룹에 포함된 경우. Detective 조사 결과 그룹을 사용하면 잠재적 보안 이벤트와 관련된 여러 활동을 검사할 수 있습니다. 자세한 내용은 the section called “결과 그룹” 섹션을 참조하세요.

- 리소스가 지난 7일 동안 조사 결과에 포함된 경우
- 최신 조사 결과 - 최신 조사 결과가 목록 맨 위에 우선적으로 표시됩니다.
- 리소스 유형 - 리소스 유형을 식별합니다. 사용자 또는 AWS 역할을 예로 AWS 들 수 있습니다.

2. `Specify an AWS role or user with an ARN` - AWS 역할 또는 AWS 사용자를 선택하고 특정 리소스에 대한 조사를 실행할 수 있습니다.

   다음 단계에 따라 특정 리소스 유형을 조사합니다.

   a. 리소스 유형 선택 드롭다운 목록에서 AWS 역할 또는 AWS 사용자를 선택합니다.

   b. IAM 리소스의 리소스 ARN을 입력합니다. 리소스 ARNs에 대한 자세한 내용은 IAM 사용 설명서의 Amazon 리소스 이름(ARNs)을 참조하세요.

3. `Find a resource to investigate from the Search page` - Detective 검색 페이지에서 모든 IAM 리소스를 검색할 수 있습니다.

   다음 단계에 따라 검색 페이지에서 리소스를 조사합니다.

   a. 탐색 창에서 검색을 선택합니다.

   b. 검색 페이지에서 IAM 리소스를 검색합니다.

   c. 리소스의 프로필 페이지로 이동하여 여기에서 조사를 실행합니다.

5. 조사 범위 시간 섹션에서 선택한 리소스의 활동을 평가할 조사의 범위 시간을 선택합니다. 시작 날짜와 시작 시간을 선택하고 종료 날짜와 종료 시간을 UTC 형식으로 선택할 수 있습니다. 선택한 범위 기간은 최소 3시간에서 최대 30일 사이일 수 있습니다.
6. 조사 실행을 선택합니다.

API

프로그래밍 방식으로 조사를 실행하려면 Detective API의 StartInvestigation 작업을 사용합니다. AWS Command Line Interface (AWS CLI)를 사용하여 조사를 실행하려면 start-investigation 명령을 실행합니다.

요청 시 다음 파라미터를 사용하여 Detective에서 조사를 실행합니다.

- `GraphArn` - 동작 그래프의 Amazon 리소스 이름(ARN)을 지정합니다.
- `EntityArn` - IAM 사용자 및 IAM 역할의 고유한 Amazon 리소스 이름(ARN)을 지정합니다.
- `ScopeStartTime` - 선택적으로 조사를 시작해야 하는 날짜 및 시간을 지정합니다. 값은 UTC ISO8601 형식의 문자열입니다. 예: `2021-08-18T16:35:56.284Z`

- `ScopeEndTime` - 선택적으로 조사를 종료해야 하는 날짜 및 시간을 지정합니다. 값은 UTC ISO8601 형식의 문자열입니다. 예: `2021-08-18T16:35:56.284Z`

이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
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
```

Detective의 다음 페이지에서도 조사를 실행할 수 있습니다.

- Detective의 IAM 사용자 또는 IAM 역할 프로필 페이지.
- 조사 결과 그룹의 그래프 시각화 창.
- 관련 리소스의 작업 열.
- 조사 결과 페이지의 IAM 사용자 또는 IAM 역할.

Detective가 리소스에 대한 조사를 실행한 후 조사 보고서가 생성됩니다. 보고서에 액세스하려면 탐색 창에서 조사로 이동합니다.

Detective 조사 보고서 검토

조사 보고서를 사용하면 이전에 Detective에서 실행한 조사에 대해 생성된 보고서를 검토할 수 있습니다.

조사 보고서를 검토하려면

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 조사를 선택합니다.

조사 보고서의 다음 속성을 기록합니다.

- ID - 조사 보고서의 생성된 식별자입니다. 이 ID를 선택하여 조사 세부 정보가 포함된 조사 보고서의 요약을 읽을 수 있습니다.
- 상태 - 각 조사는 조사 완료 상태에 따른 상태와 연결됩니다. 상태 값은 진행 중, 성공 또는 실패일 수 있습니다.
- 심각도 - 각 조사에는 심각도가 할당됩니다. Detective는 조사 결과에 심각도를 자동으로 할당합니다.

  심각도는 주어진 범위 시간 내에서 단일 리소스를 조사하여 분석한 결과를 나타냅니다. 조사를 통해 보고된 심각도는 영향을 받는 리소스가 조직에 미칠 수 있는 심각성이나 중요성을 암시하거나 나타내지 않습니다.

  조사 심각도 값은 가장 높은 심각도부터 가장 낮은 심각도 순으로 심각, 높음, 중간, 낮음 또는 정보용입니다.

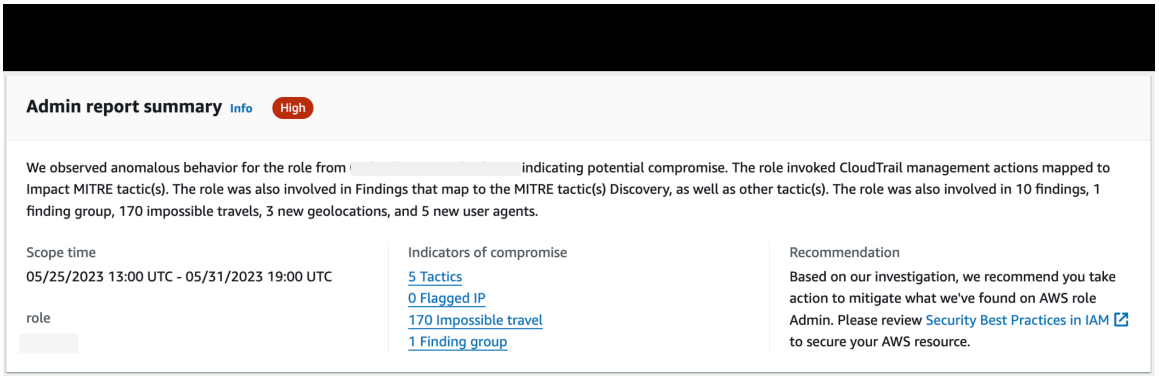
  심각 또는 높음 심각도 값이 할당된 조사는 Detective에서 식별한 영향력이 큰 보안 문제를 나타낼 가능성이 높으므로 우선적으로 추가 검사해야 합니다.
- 엔터티 - 엔터티 열에는 조사에서 탐지된 특정 엔터티에 대한 세부 정보가 포함됩니다. 일부 엔터티는 사용자 및 역할과 같은 AWS 계정입니다.
- 상태 - 생성 날짜 열에는 조사 보고서가 처음 생성된 날짜 및 시간에 대한 세부 정보가 포함됩니다.

Detective 조사 보고서 이해

Detective 조사 보고서에는 손상을 나타내는 흔하지 않은 동작 또는 악의적인 활동에 대한 요약이 나열됩니다. 또한 Detective가 보안 위험을 완화하기 위해 제안하는 권장 사항도 나열되어 있습니다.

특정 조사 ID에 대한 조사 보고서를 보려면

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 조사를 선택합니다.
3. 보고서 테이블에서 조사 ID를 선택합니다.



Detective는 선택한 범위 시간 및 사용자에 대한 보고서를 생성합니다. 보고서에는 아래 나열된 하나 이상의 손상 지표에 대한 세부 정보가 포함된 손상 지표 섹션이 포함되어 있습니다. 각 손상 지표를 검토할 때 필요한 경우 드릴다운할 항목을 선택하여 세부 정보를 검토할 수 있습니다.

- 전술, 기법 및 절차 - 잠재적 보안 이벤트에 사용되는 전술, 기법 및 절차(TTP)를 식별합니다. MITRE ATT&CK 프레임워크는 TTP를 이해하는 데 사용됩니다. 전술은 MITRE ATT&CK Matrix for Enterprise를 기반으로 합니다.
- 위협 인텔리전스 플래그가 지정된 IP 주소 - 의심스러운 IP 주소는 Detective 위협 인텔리전스를 기반으로 치명적이거나 심각한 위협으로 플래그가 지정되고 식별됩니다.
- 불가능한 이동 - 계정에서 비정상적이거나 불가능한 사용자 활동을 탐지하고 식별합니다. 예를 들어, 이 지표는 짧은 기간 동안 사용자의 출발지와 목적지 위치 간의 급격한 변화를 보여줍니다.
- 관련 조사 결과 그룹 - 잠재적 보안 이벤트와 관련된 여러 활동을 보여줍니다. Detective는 조사 결과와 엔터티 간의 관계를 추론하고 이들을 조사 결과 그룹으로 묶는 그래프 분석 기법을 사용합니다.
- 관련 조사 결과 - 잠재적 보안 이벤트와 관련된 관련 활동입니다. 리소스 또는 조사 결과 그룹과 관련된 증거의 모든 카테고리를 나열합니다.
- 새 지리적 위치 - 리소스 또는 계정 수준에서 사용되는 새 지리적 위치를 식별합니다. 예를 들어, 이 지표는 이전 사용자 활동을 기반으로 자주 사용되지 않거나 사용되지 않는 위치인 관찰된 지리적 위치를 나열합니다.
- 새 사용자 에이전트 - 리소스 또는 계정 수준에서 사용되는 새 사용자 에이전트를 식별합니다.
- 새 ASO - 리소스 또는 계정 수준에서 사용되는 새로운 자율 시스템 조직(ASO)을 식별합니다. 예를 들어, 이 지표는 ASO로 할당된 새 조직을 나열합니다.

Detective 조사 보고서 요약

조사 요약에는 선택한 범위 시간 동안 주의가 필요한 이상 지표가 강조 표시됩니다. 요약을 사용하면 잠재적 보안 문제의 근본 원인을 더 빠르게 식별하고 패턴을 식별하며 보안 이벤트의 영향을 받는 리소스를 이해할 수 있습니다.

세부 조사 보고서 요약에서 다음과 같은 세부 정보를 볼 수 있습니다.

조사 개요

개요 패널에서는 높음 심각도 활동이 있는 IP를 시각화하여 공격자의 경로에 대한 자세한 컨텍스트를 제공할 수 있습니다.

Detective는 조사에서의 비정상적인 활동을 강조합니다. 예를 들어 IAM 사용자가 출발지에서 멀리 떨어진 목적지로 이동하는 것이 불가능한 경우가 있습니다.

Detective는 조사를 잠재적 보안 이벤트에 사용되는 전술, 기법 및 절차(TTP)에 매핑합니다. MITRE ATT&CK 프레임워크는 TTP를 이해하는 데 사용됩니다. 전술은 MITRE ATT&CK Matrix for Enterprise를 기반으로 합니다.

조사 지표

지표 창의 정보를 사용하여 AWS 리소스가 악의적인 동작과 그 영향을 나타낼 수 있는 비정상적인 활동에 연루되어 있는지 확인할 수 있습니다. 손상 지표(IOC)는 네트워크, 시스템 또는 환경에서 관찰된 아티팩트로, 높은 수준의 신뢰도로 악의적인 활동이나 보안 인시던트를 식별할 수 있습니다.

Detective 조사 보고서 다운로드

Detective 조사 보고서를 JSON 형식으로 다운로드하여 추가로 분석하거나 Amazon S3 버킷과 같은 선호하는 스토리지 솔루션에 저장할 수 있습니다.

보고서 테이블에서 조사 보고서를 다운로드하려면

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 조사를 선택합니다.
3. 보고서 테이블에서 조사를 선택하고 다운로드를 선택합니다.

요약 페이지에서 조사 보고서를 다운로드하려면

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 조사를 선택합니다.
3. 보고서 테이블에서 조사를 선택합니다.
4. 조사 요약 페이지에서 다운로드를 선택합니다.

Detective 조사 보고서 보관

Amazon Detective에서 조사를 완료하면 조사 보고서를 보관할 수 있습니다. 보관된 조사는 조사 검토를 완료했음을 나타냅니다.

Detective 관리자인 경우에만 조사를 보관하거나 보관 취소할 수 있습니다. Detective는 보관된 조사를 90일 동안 저장합니다.

보고서 테이블에서 조사 보고서를 보관하려면

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 조사를 선택합니다.
3. 보고서 테이블에서 조사를 선택하고 보관을 선택합니다.

요약 페이지에서 조사 보고서를 보관하려면

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 조사를 선택합니다.
3. 보고서 테이블에서 조사를 선택합니다.
4. 조사 요약 페이지에서 보관을 선택합니다.

Amazon Detective에서 조사 결과 분석

조사 결과는 잠재적으로 악의적인 활동이나 탐지된 기타 위험의 인스턴스입니다. Amazon GuardDuty 및AWS보안 조사 결과는 Amazon Detective에 로드되므로 Detective를 사용하여 관련 엔터티와 관련된 활동을 조사할 수 있습니다. GuardDuty 조사 결과는 Detective 코어 패키지의 일부이며 기본적으로 수집됩니다. Security Hub CSPM에서 집계한 다른 모든AWS보안 조사 결과는 선택적 데이터 소스로 수집됩니다. 자세한 내용은 동작 그래프에 사용된 소스 데이터를 참조하세요.

Detective 조사 결과 개요는 조사 결과에 대한 자세한 정보를 제공합니다. 또한 관련 엔터티 프로필로 연결되는 링크와 함께 관련 엔터티에 대한 요약도 표시됩니다.

Detective는 조사 결과가 대규모 활동과 상관관계가 있는 경우 조사 결과 그룹으로 이동하라는 알림을 표시합니다. 조사 결과 그룹을 사용하면 잠재적 보안 이벤트와 관련된 여러 활동을 조사할 수 있으므로 조사 결과 그룹을 사용하여 조사를 계속하는 것이 좋습니다. the section called “결과 그룹”을(를) 참조하세요.

Amazon Detective는 조사 결과 그룹에 대한 대화형 시각화를 제공합니다. 이 시각화는 적은 노력으로 문제를 더 빠르고 철저하게 조사할 수 있도록 설계되었습니다. 조사 결과 그룹 시각화 패널에는 조사 결과 그룹과 관련된 조사 결과 및 엔터티가 표시됩니다. 이 대화형 시각화를 사용하여 조사 결과 그룹의 영향을 분석, 이해 및 분류할 수 있습니다. 이 패널은 관련 엔터티 및 관련 조사 결과 테이블에 표시된 정보를 시각화하는 데 도움이 됩니다. 시각적 프레젠테이션에서 추가 분석을 위한 조사 결과 또는 엔터티를 선택할 수 있습니다. 조사 결과 그룹 시각화를 참조하세요.

내용

Detective에서 결과 개요 분석

Detective 조사 결과 개요는 조사 결과에 대한 자세한 정보를 제공합니다. 또한 관련 엔터티 프로필로 연결되는 링크와 함께 관련 엔터티에 대한 요약도 표시됩니다.

조사 결과 개요에 사용된 범위 시간

조사 결과 개요의 범위 시간은 조사 결과 기간으로 설정됩니다. 조사 결과 기간에는 조사 결과 활동이 처음으로 관찰된 시간과 마지막 시간이 반영됩니다.

조사 결과 세부 정보

오른쪽 패널에는 조사 결과에 대한 세부 정보가 포함되어 있습니다. 이는 조사 결과 제공자가 제공한 세부 정보입니다.

조사 결과 세부 정보에서 조사 결과를 보관할 수도 있습니다. 자세한 내용은 Amazon GuardDuty 결과 보관을 참조하세요.

관련 엔터티

조사 결과 개요에는 조사 결과와 관련된 엔터티 목록이 포함되어 있습니다. 각 엔터티의 경우 목록은 엔터티에 대한 개요 정보를 제공합니다. 이 정보는 해당 엔터티 프로필의 엔터티 세부 정보 프로필 패널에 있는 정보를 반영합니다.

목록은 엔터티 유형을 기준으로 필터링할 수 있습니다. 엔터티 식별자에 있는 텍스트를 기준으로 목록을 필터링할 수도 있습니다.

엔터티의 프로필로 피벗하려면 프로필 보기를 선택합니다. 엔터티 프로필에 피벗하면 다음과 같이 진행됩니다.

- 범위 시간은 조사 결과 기간으로 설정됩니다.
- 엔터티의 관련 조사 결과 패널에서 조사 결과가 선택됩니다. 조사 결과 세부 정보는 엔터티 프로필 오른쪽에 계속 표시됩니다.

'페이지를 찾을 수 없음' 문제 해결

Detective에서 엔터티 또는 조사 결과로 이동할 때 페이지를 찾을 수 없음 오류 메시지가 표시될 수 있습니다.

이 문제를 해결하려면 다음 중 한 가지 방법을 사용합니다.

- 엔터티 또는 조사 결과가 멤버 계정 중 하나에 속하는지 확인합니다. 멤버 계정을 검토하는 방법에 대한 자세한 내용은 계정 목록 보기를 참조하세요.

- 관리자 계정이 GuardDuty 및/또는 Security Hub CSPM과 정렬되어 이러한 서비스에서 Detective로 피벗되는지 확인합니다. 권장 사항은 GuardDuty 및 Security Hub CSPM과의 권장 정렬을 참조하세요.
- 멤버 계정이 초대를 수락한 이후에 조사 결과가 나왔는지 확인합니다.
- Detective 동작 그래프가 선택적 데이터 소스 패키지의 데이터를 수집하고 있는지 확인합니다. Detective 동작 그래프에 사용되는 소스 데이터에 대한 자세한 내용은 동작 그래프에 사용되는 소스 데이터를 참조하세요.
- Detective가 Security Hub CSPM에서 데이터를 수집하고 동작 그래프에 해당 데이터를 추가할 수 있도록 하려면AWS보안 조사 결과에 대해 Detective를 데이터 소스 패키지로 활성화해야 합니다. 자세한 내용은 AWS보안 조사 결과를 참조하세요.
- Detective에서 엔터티 프로필이나 조사 결과 개요로 이동하려는 경우 URL 형식이 올바른지 확인합니다. 프로필 URL 형성에 대한 자세한 내용은 URL을 사용하여 엔터티 프로필 또는 조사 결과 개요로 이동을 참조하세요.

조사 결과 그룹 분석

Amazon Detective 조사 결과 그룹을 사용하면 잠재적 보안 이벤트와 관련된 여러 활동을 검사할 수 있습니다. Amazon Detective의 조사 결과 그룹은 Detective가 동일한 잠재적 보안 인시던트와 관련이 있음을 암시하는 여러 조사 결과 간의 패턴 또는 관계를 탐지할 때 생성됩니다. 이 그룹화는 관련 조사 결과를 보다 효율적으로 관리하고 조사하는 데 도움이 됩니다.

조사 결과 그룹을 사용하여 심각도가 높은 GuardDuty 조사 결과의 근본 원인을 분석할 수 있습니다. 위협 행위자가AWS환경을 손상하려고 하면 일반적으로 여러 보안 조사 결과와 비정상적인 동작으로 이어지는 일련의 작업을 수행합니다. 이러한 동작은 시간 및 엔터티 전반에 걸쳐 발생하는 경우가 많습니다. 보안 조사 결과를 개별적으로 조사하면 해당 중요성이 잘못 해석되어 근본 원인을 찾는 데 어려움이 있을 수 있습니다. Amazon Detective는 조사 결과와 엔터티 간의 관계를 추론하고 이들을 그룹화하는 그래프 분석 기법을 적용하여 이 문제를 해결합니다. 관련 엔터티 및 조사 결과를 조사하기 위한 출발점으로 조사 결과 그룹을 처리하는 것이 좋습니다.

Detective는 조사 결과의 데이터를 분석하고 공유 리소스를 기반으로 관련될 가능성이 있는 다른 조사 결과와 그룹화합니다. 예를 들어, 동일한 IAM 역할 세션에서 취하거나 동일한 IP 주소에서 발생한 조치와 관련된 조사 결과는 동일한 기본 활동의 일부일 가능성이 큽니다. Detective가 식별한 연관성이 관련 없더라도 그룹으로 조사 결과와 증거를 조사하는 것이 중요합니다.

결과 그룹은 다음 기준에 따라 생성됩니다.

- 임시 근접성 - 가까운 기간 내에 발생하는 결과는 동일한 인시던트와 관련이 있을 수 있으므로 종종 함께 그룹화됩니다.
- 일반 엔터티 - IP 주소, 사용자 또는 리소스와 같은 동일한 엔터티와 관련된 결과가 함께 그룹화됩니다. 이렇게 하면 환경의 여러 부분에서 인시던트의 범위를 이해하는 데 도움이 됩니다.
- 패턴 및 행동 - Detective는 유사한 유형의 공격 또는 의심스러운 활동과 같은 조사 결과의 패턴과 행동을 분석하여 관계를 결정하고 그에 따라 그룹화합니다.
- 전술, 기법 및 절차(TTPs) - MITRE ATT&CK와 같은 프레임워크에 설명된 대로 유사한 TTPs를 공유하는 결과가 함께 그룹화되어 잠재적으로 조정된 공격을 강조합니다.

이러한 기준은 조사 프로세스를 간소화하는 데 도움이 되므로 동일한 보안 인시던트를 나타낼 수 있는 상관관계가 있는 결과에 집중할 수 있습니다.

조사 결과 외에도 각 그룹에는 조사 결과와 관련된 엔터티가 포함됩니다. 엔터티에는 IP 주소 또는 사용자 에이전트AWS와 같은 외부 리소스가 포함될 수 있습니다.

> **Note**
>
> 초기 GuardDuty 조사 결과가 발생한 후 다른 조사 결과와 관련이 있는 것으로 확인되면 48시간 내에 모든 관련 조사 결과 및 모든 관련 엔터티가 포함된 조사 결과 그룹이 생성됩니다.

조사 결과 그룹 페이지 이해

결과 그룹 페이지에는 동작 그래프에서 Amazon Detective가 수집한 모든 결과 그룹이 나열됩니다. 결과 그룹의 다음 속성을 기록해 둡니다.

그룹의 심각도

각 결과 그룹에는 관련 결과의AWS Security Finding Format(ASFF) 심각도에 따라 심각도가 할당됩니다. ASFF 조사 결과 심각도 값은 가장 높은 심각도부터 가장 낮은 심각도 순으로 심각, 높음, 중간, 낮음 또는 정보용입니다. 그룹화의 심각도는 해당 그룹의 조사 결과 중에서 가장 높은 심각도 조사 결과와 같습니다.

다수의 엔터티에 영향을 미치는 심각 또는 높은 심각도 조사 결과로 구성된 그룹은 영향력이 큰 보안 문제를 나타낼 가능성이 높으므로 조사 우선 순위를 지정해야 합니다.

그룹 제목

제목 열에서 각 그룹에는 고유한 ID와 고유하지 않은 제목이 있습니다. 이는 그룹의 ASFF 유형 네임스페이스와 클러스터의 해당 네임스페이스 내 조사 결과 수를 기반으로 합니다. 예를 들어 그룹화 제목이 TTP(2), 효과(1), 비정상 동작(2)인 그룹인 경우 TTP 네임스페이스의 조사 결과 2개, 효과 네임스페이스의 조사 결과 1개, 비정상 동작 네임스페이스의 조사 결과 2개로 구성된 총 5개의 조사 결과가 포함됩니다. 네임스페이스의 전체 목록은 ASFF의 유형 분류를 참조하세요.

그룹 내 전술

그룹의 전술 열에는 해당 활동이 속하는 전술 범주가 자세히 나와 있습니다. 다음 목록의 전술, 기법 및 절차 범주는 MITRE ATT&CK matrix와 일치합니다.

체인에서 전술을 선택하여 전술에 대한 설명을 볼 수 있습니다. 체인 다음에는 그룹 내에서 탐지된 전술 목록이 있습니다. 이러한 범주와 이들이 일반적으로 나타내는 활동은 다음과 같습니다.

- 초기 액세스 - 공격자가 다른 사람의 네트워크에 침입하려고 합니다.
- 실행 - 공격자가 다른 사람의 네트워크에 침입하려고 합니다.
- 지속성 - 공격자가 거점을 유지하려고 합니다.
- 권한 에스컬레이션 - 공격자가 더 높은 수준의 권한을 얻으려고 합니다.
- 방어 회피 - 공격자가 탐지를 피하려고 합니다.
- 보안 인증 정보 액세스 - 공격자가 계정 이름과 암호를 도용하려고 합니다.
- 검색 - 공격자가 환경을 이해하고 알아내려고 합니다.
- 측면 이동 - 공격자가 환경을 통해 이동하려고 합니다.
- 수집 - 공격자가 목표를 달성하기 위해 관심 있는 데이터를 수집하려고 합니다.
- 명령 및 제어 - 공격자가 다른 사람의 네트워크에 침입하려고 합니다.
- 유출 - 공격자가 데이터를 훔치려고 합니다.
- 영향 - 공격자가 시스템과 데이터를 조작, 방해 또는 파괴하려고 합니다.
- 기타 - 매트릭스에 나열된 전술과 일치하지 않는 조사 결과로 인한 활동을 나타냅니다.

그룹 내 엔터티

엔터티 열에는 이 그룹 내에서 탐지된 특정 엔터티에 대한 세부 정보가 들어 있습니다. ID, 네트워크, 스토리지, 컴퓨팅 등의 범주를 기준으로 엔터티를 분류하려면 이 값을 선택합니다. 각 범주에 속하는 엔터티의 예는 다음과 같습니다.

- 자격 증명 - 사용자 및 역할과AWS 계정같은 IAM 보안 주체 및
- 네트워크 - IP 주소 또는 기타 네트워킹 및 VPC 엔터티

- 스토리지 - Amazon S3 버킷 또는 DDB
- 컴퓨팅 - Amazon EC2 인스턴스 또는 Kubernetes 컨테이너

그룹 내 계정

계정 열에는 그룹의 조사 결과와 관련된 엔터티를 소유한AWS계정이 표시됩니다.AWS계정은 이름 및AWS ID별로 나열되므로 중요한 계정과 관련된 활동에 대한 조사의 우선순위를 지정할 수 있습니다.

그룹 내 조사 결과

조사 결과 열에는 심각도별로 그룹 내 엔터티가 나열되어 있습니다. 조사 결과에는 Amazon GuardDuty 조사 결과, Amazon Inspector 조사 결과,AWS보안 조사 결과 및 Detective의 증거가 포함됩니다. 그래프를 선택하여 심각도별로 정확한 조사 결과 수를 확인할 수 있습니다.

GuardDuty 조사 결과는 Detective 코어 패키지의 일부이며 기본적으로 수집됩니다. Security Hub CSPM에서 집계한 다른 모든AWS보안 조사 결과는 선택적 데이터 소스로 수집됩니다. 자세한 내용은 동작 그래프에 사용된 소스 데이터를 참조하세요.

조사 결과 그룹에 대한 정보용 조사 결과

Amazon Detective는 지난 45일 이내에 수집된 동작 그래프의 데이터를 기반으로 조사 결과 그룹과 관련된 추가 정보를 식별합니다. Detective는 이 정보를 정보용 심각도가 포함된 조사 결과로 제시합니다. 증거는 조사 결과 그룹 내에서 볼 때 잠재적으로 의심스러울 수 있는 특이한 활동이나 알려지지 않은 동작을 강조하는 지원 정보를 제공합니다. 여기에는 새로 관찰된 지리적 위치 또는 조사 결과 범위 내에서 관찰된 API 직접 호출이 포함될 수 있습니다. 증거 결과는 Detective에서만 볼 수 있으며 로 전송되지 않습니다AWS Security Hub CSPM.

Detective는 MaxMind GeoIP 데이터베이스를 사용하여 요청 위치를 결정합니다. MaxMind는 국가 수준에서 매우 높은 데이터 정확도를 보고하지만, 정확도는 국가 및 IP 유형과 같은 요인에 따라 다릅니다. MaxMind에 대한 자세한 내용은 MaxMind IP 지리적 위치를 참조하세요. GeoIP 데이터가 잘못되었다고 생각되면 Maxmind(MaxMind Correct GeoIP2 Data)에 정정 요청을 제출할 수 있습니다.

다양한 보안 주체 유형(예: IAM 사용자 또는 IAM 역할)에 대한 증거를 관찰할 수 있습니다. 일부 증거 유형의 경우 모든 계정의 증거를 관찰할 수 있습니다. 즉, 증거가 전체 동작 그래프에 영향을 미칩니다. 모든 계정에서 증거 조사 결과가 관찰되면 개별 IAM 역할에 대해 동일한 유형의 추가 정보용 증거 조사 결과도 하나 이상 확인할 수 있습니다. 예를 들어 모든 계정에 대해 관찰된 새로운 지리적 위치 조사 결과가 관찰된 경우, 보안 주체에 대해 관찰된 새로운 지리적 위치에 대한 또 다른 지리적 위치가 표시됩니다.

조사 결과 그룹의 증거 유형

- 새로운 지리적 위치가 관찰됨
- 새로운 자율 시스템 조직(ASO)이 관찰됨
- 새로운 사용자 에이전트가 관찰됨
- 새로운 API 직접 호출이 실행됨
- 모든 계정에 대해 관찰된 새로운 지리적 위치
- 모든 계정에 대해 관찰된 새로운 IAM 보안 주체

조사 결과 그룹 프로필

그룹 제목을 선택하면 해당 그룹에 대한 추가 세부 정보가 포함된 조사 결과 그룹 프로필이 열립니다. 조사 결과 그룹 프로필 페이지의 세부 정보 패널에는 상위 및 하위 그룹을 찾기 위한 항목 및 조사 결과를 최대 1000개까지 표시할 수 있습니다.

그룹 프로필 페이지에는 그룹에 설정된 범위 시간이 표시됩니다. 이는 그룹에 포함된 가장 빠른 조사 결과 또는 증거부터 그룹에서 가장 최근에 업데이트된 조사 결과 또는 증거까지의 날짜 및 시간입니다. 또한 그룹 내 조사 결과 중 가장 높은 심각도 범주에 해당하는 조사 결과 그룹 심각도도 확인할 수 있습니다. 이 프로필 패널의 기타 세부 정보는 다음과 같습니다.

- 관련 전술 체인은 그룹 내 조사 결과에 따른 전술이 무엇인지 보여줍니다. 전술은 MITRE ATT&CK Matrix for Enterprise를 기반으로 합니다. 전술은 초기 단계부터 최신 단계까지의 일반적인 공격 진행 상황을 나타내는 컬러 도트 체인으로 표시됩니다. 즉, 사슬에서 가장 왼쪽에 있는 원은 공격자가 주변 환경에 대한 접근 권한을 얻거나 유지하려는 경우 일반적으로 덜 심각한 활동을 나타냅니다. 반대로 오른쪽으로의 활동은 가장 심각하며 데이터 변조 또는 파기를 포함할 수 있습니다.
- 이 그룹이 다른 그룹과 맺고 있는 관계. 때로는 이전에 연결되지 않은 하나 이상의 조사 결과 그룹이 새로 발견된 연결을 기반으로 새 그룹으로 병합될 수 있습니다(예: 기존 그룹의 엔터티가 포함된 조사 결과). 이 경우 Amazon Detective는 상위 그룹을 비활성화하고 하위 그룹을 생성합니다. 모든 그룹의 계보를 추적하여 상위 그룹까지 추적할 수 있습니다. 그룹은 다음과 같은 관계를 가질 수 있습니다.
  - 하위 결과 그룹 - 다른 두 개의 조사 결과 그룹에 포함된 조사 결과가 새 조사 결과에 포함될 때 생성되는 조사 결과 그룹입니다. 모든 하위 그룹에 대해 조사 결과의 상위 그룹이 나열됩니다.
  - 상위 조사 결과 그룹 - 하위 그룹이 생성된 경우 조사 결과 그룹은 상위 그룹입니다. 조사 결과 그룹이 상위인 경우 관련 하위 그룹도 함께 나열됩니다. 상위 그룹이 활성 하위 그룹에 병합되면 상위 그룹의 상태는 비활성 상태가 됩니다.

프로필 패널을 여는 두 개의 정보 탭이 있습니다. 관련 엔터티 및 관련 결과 탭을 사용하여 그룹에 대한 추가 세부 정보를 볼 수 있습니다.

조사 실행을 사용하여 조사 보고서를 생성합니다. 생성된 보고서는 손상을 나타내는 이상 동작을 자세히 설명합니다.

그룹 내 프로필

관련 엔터티

각 엔터티가 연결된 그룹 내의 조사 결과를 포함하여 조사 결과 그룹의 엔터티에 초점을 맞춥니다. 각 엔터티에 연결된 태그도 표시되므로 태그 지정을 기반으로 중요한 엔터티를 빠르게 식별할 수 있습니다. 엔터티를 선택하면 해당 엔터티 프로필을 볼 수 있습니다.

관련 조사 결과

조사 결과의 심각도, 관련된 각 엔터티, 해당 조사 결과가 처음 발견되고 마지막으로 확인된 시기 등 각 조사 결과에 대한 세부 정보가 있습니다. 목록에서 조사 결과 유형을 선택하면 해당 조사 결과에 대한 추가 정보가 포함된 조사 결과 세부 정보 패널이 열립니다. 관련 조사 결과 패널의 일부로 동작 그래프의 Detective 증거를 기반으로 한 정보용 조사 결과를 볼 수 있습니다.

조사 결과 그룹 시각화

Amazon Detective는 조사 결과 그룹에 대한 대화형 시각화를 제공합니다. 이 시각화는 적은 노력으로 문제를 더 빠르고 철저하게 조사할 수 있도록 설계되었습니다. 조사 결과 그룹 시각화 패널에는 조사 결과 그룹과 관련된 조사 결과 및 엔터티가 표시됩니다. 이 대화형 시각화를 사용하여 조사 결과 그룹의 영향을 분석, 이해 및 분류할 수 있습니다. 이 패널은 관련 엔터티 및 관련 조사 결과 테이블에 표시된 정보를 시각화하는 데 도움이 됩니다. 시각적 프레젠테이션에서 추가 분석을 위한 조사 결과 또는 엔터티를 선택할 수 있습니다.

조사 결과가 집계된 Detective조사 결과 그룹은 동일한 유형의 리소스에 연결된 조사 결과의 클러스터입니다. 조사 결과를 집계하면 조사 결과 그룹의 구성을 빠르게 평가하고 보안 문제를 더 빠르게 해석할 수 있습니다. 조사 결과 그룹 세부 정보 패널에는 유사한 조사 결과가 결합되어 있으며 조사 결과를 확장하여 비교적 유사한 조사 결과를 함께 볼 수 있습니다. 예를 들어, 동일한 유형의 정보용 조사 결과 및 중간 조사 결과가 있는 증거 노드가 집계됩니다. 현재 집계된 조사 결과를 통해 조사 결과 그룹의 제목, 소스, 유형 및 심각도를 볼 수 있습니다.

이 대화형 패널에서 다음을 수행할 수 있습니다.

- 조사 실행을 사용하여 조사 보고서를 생성합니다. 생성된 보고서에는 손상을 나타내는 이상 동작이 자세히 설명되어 있습니다. 자세한 내용은 탐지 조사를 참조하세요.
- 집계된 조사 결과가 포함된 조사 결과 그룹에 대한 자세한 내용을 확인하여 관련 증거, 엔터티 및 조사 결과를 분석할 수 있습니다.
- 엔터티 및 조사 결과의 레이블을 확인하여 잠재적 보안 문제가 있는 영향을 받는 엔터티를 식별할 수 있습니다. 레이블을 끌 수 있습니다.
- 엔터티 및 조사 결과를 재정렬하여 상호 연관성을 더 잘 이해합니다. 조사 결과 그룹에서 선택한 항목을 이동하여 항목과 조사 결과를 그룹에서 분리합니다.
- 증거, 엔터티 및 조사 결과를 선택하면 이에 대한 자세한 내용을 볼 수 있습니다. 여러 항목을 선택하려면 **command/control**을 선택하고 항목을 선택하거나 포인터를 사용하여 끌어다 놓습니다.
- 모든 엔터티 및 조사 결과가 조사 결과 그룹 창에 맞도록 레이아웃을 조정합니다. 조사 결과 그룹에 널리 사용되는 엔터티 유형을 확인합니다.

> **Note**
>
> 조사 결과 그룹 시각화 패널은 최대 100개의 엔터티 및 조사 결과가 포함된 조사 결과 그룹을 표시할 수 있습니다.

드롭다운을 사용하여 Radial, Circle, Force-directed 또는 Grid 레이아웃의 조사 결과 및 엔터티를 볼 수 있습니다. 방사형 레이아웃은 더 쉬운 데이터 해석을 위해 향상된 시각화를 제공합니다. 힘 방향 레이아웃에서는 항목 간에 링크 길이가 일정하고 링크가 균등하게 분산되도록 엔터티 및 조사 결과를 배치합니다. 이렇게 하면 중복을 줄이는 데 도움이 됩니다. 선택한 레이아웃에 따라 시각화 패널에서의 조사 결과 배치가 정의됩니다.

타임라인 레이아웃

타임라인 레이아웃은 시간 경과에 따라 결과 그룹이 어떻게 진화하는지 시각화하는 동적 방법을 제공합니다. 이를 통해 이벤트 진행 상황을 확인할 수 있으므로 Detective를 사용하여 보안 인시던트의 순서와 잠재적 인과관계를 더 잘 이해할 수 있습니다.

시각화 패널 하단의 타임라인 슬라이더를 사용하여 특정 시점을 선택합니다. 시각화는 해당 시점에 조사 결과 그룹의 상태를 표시하도록 업데이트됩니다. 타임라인을 자동으로 진행할 수 있는 재생 버튼입니다. 재생 버튼을 클릭하여 애니메이션을 시작합니다. 시각화는 실시간으로 업데이트되어 시간 경과에 따라 결과 그룹이 어떻게 변경되는지 보여줍니다. 일시 중지 버튼을 사용하여 언제든지 애니메이션을 중지합니다.

이제 필터 드롭다운을 사용하여 심각도 수준에 따라 결과를 필터링할 수 있습니다. 필터를 적용하면 선택한 심각도 수준과 일치하는 조사 결과만 표시되도록 시각화가 업데이트됩니다. 필터는 타임라인에 표시된 결과에만 영향을 미치며 전체 결과 그룹 시각화에는 영향을 미치지 않습니다. 이를 통해 우선순위가 높은 문제에 빠르게 집중하거나 특정 유형의 조사 결과를 조사할 수 있습니다.

필터링 기능을 타임라인 레이아웃과 함께 사용하여 다양한 심각도 수준의 결과가 시간이 지남에 따라 어떻게 나타나고 진화하는지 확인할 수 있습니다.

향상된 조사 워크플로

타임라인 레이아웃 및 필터링 기능이 추가되어 이제 보다 포괄적인 조사를 수행할 수 있습니다.

1. 먼저 정적 레이아웃(래디얼, 원, 강제 지시 또는 그리드) 중 하나를 사용하여 전체 결과 그룹을 봅니다.
2. 타임라인을 사용하여 시간이 지남에 따라 상황이 어떻게 진행되었는지 파악합니다.
3. 재생 버튼을 사용하면 타임라인을 자동으로 진행하여 주요 순간이나 패턴을 감시할 수 있습니다.
4. 중요한 지점에서 일시 중지하여 자세히 조사합니다.
5. 필터를 적용하여 특정 심각도 수준의 결과에 초점을 맞춥니다.
6. 키보드 바로 가기 및 선택 도구를 사용하여 관심 있는 엔터티와 조사 결과를 자세히 살펴봅니다.

이 향상된 워크플로를 사용하면 복잡한 보안 시나리오를 보다 미묘하고 철저하게 조사할 수 있습니다. 보다 효율적이고 효과적인 보안 조사를 수행하여 인시던트 해결을 가속화하고 전반적인 보안 태세를 개선할 수 있습니다.

키보드 바로 가기

다음 키보드 바로 가기를 사용하여 결과 그룹 시각화 패널과 상호 작용할 수 있습니다.

- 클릭 - 단일 노드를 선택하고, 다른 모든 노드를 선택 취소하고, 공백을 클릭하면 모든 노드를 선택 취소합니다.
- Ctrl + 클릭 - 단일 노드를 선택하고 다른 노드의 선택을 취소하지 않습니다.
- 끌어오기 - 보기를 이동합니다.
- Ctrl + 끌어오기 - Marquee는 다른 노드의 선택을 취소하지 않습니다.
- Shift + Drag - Marquee는 다른 모든 노드를 선택하고 선택 취소합니다.
- 화살표 키 - 노드 간의 초점을 변경합니다.
- Ctrl + Space - 현재 집중된 노드를 선택하거나 선택 취소합니다.

- Shift + Arrow 키 - 노드 간의 초점을 변경하고 선택합니다.

동적 범례는 현재 그래프의 엔터티 및 조사 결과에 따라 달라집니다. 이를 통해 각 시각적 요소가 무엇을 나타내는지 식별할 수 있습니다.

생성형 AI 기반 조사 결과 그룹 요약

기본적으로 Amazon Detective는 개별 조사 결과 그룹의 요약을 자동으로 제공합니다. 요약은 Amazon Bedrock에서 호스팅되는 생성형 인공 지능(생성형 AI) 모델을 기반으로 합니다. Detective가 활성화된 경우 추가 비용 없이 결과 그룹 요약을 사용할 수 있습니다.

> **Note**
>
> 2026년 2월 16일부터 Detective의 결과 그룹 요약 기능은 결과 그룹 데이터를 처리하고를 사용하여 요약을 생성할 최적의 AWS 리전(지리 내의 리전 엔드포인트 그룹화에서)을 자동으로 선택합니다the section called “교차 리전 추론”.
> 이 기능을 사용하지 않으려면 Detective의 콘솔에서 비활성화하거나 Detective의 콘솔에 액세스하는 데 사용되는 IAM 역할에 대한 거부 권한을 사용하면 됩니다. the section called “결과 그룹 요약 옵트아웃”을(를) 참조하세요.

조사 결과 그룹을 사용하면 잠재적 보안 이벤트와 관련된 여러 보안 조사 결과를 검토하고 잠재적 위협 행위자를 식별할 수 있습니다. 조사 결과 그룹을 위한 조사 그룹 요약은 이러한 기능을 기반으로 합니다. 조사 결과 그룹 요약은 조사 결과 그룹에 대한 데이터를 사용하고 조사 결과와 영향을 받는 리소스 간의 관계를 신속하게 분석한 다음 잠재적 위협을 자연어로 요약합니다. 이러한 요약을 활용하여 더 큰 보안 위협을 식별하고, 조사 효율성을 높이고, 대응 일정을 단축할 수 있습니다.

> **Note**
>
> 생성형 AI 기반의 조사 결과 그룹 요약에서 항상 정확한 정보를 얻을 수 있는 것은 아닙니다. 자세한 내용은 AWS 책임감 있는 AI를 참조하세요.

조사 결과 그룹 요약 검토

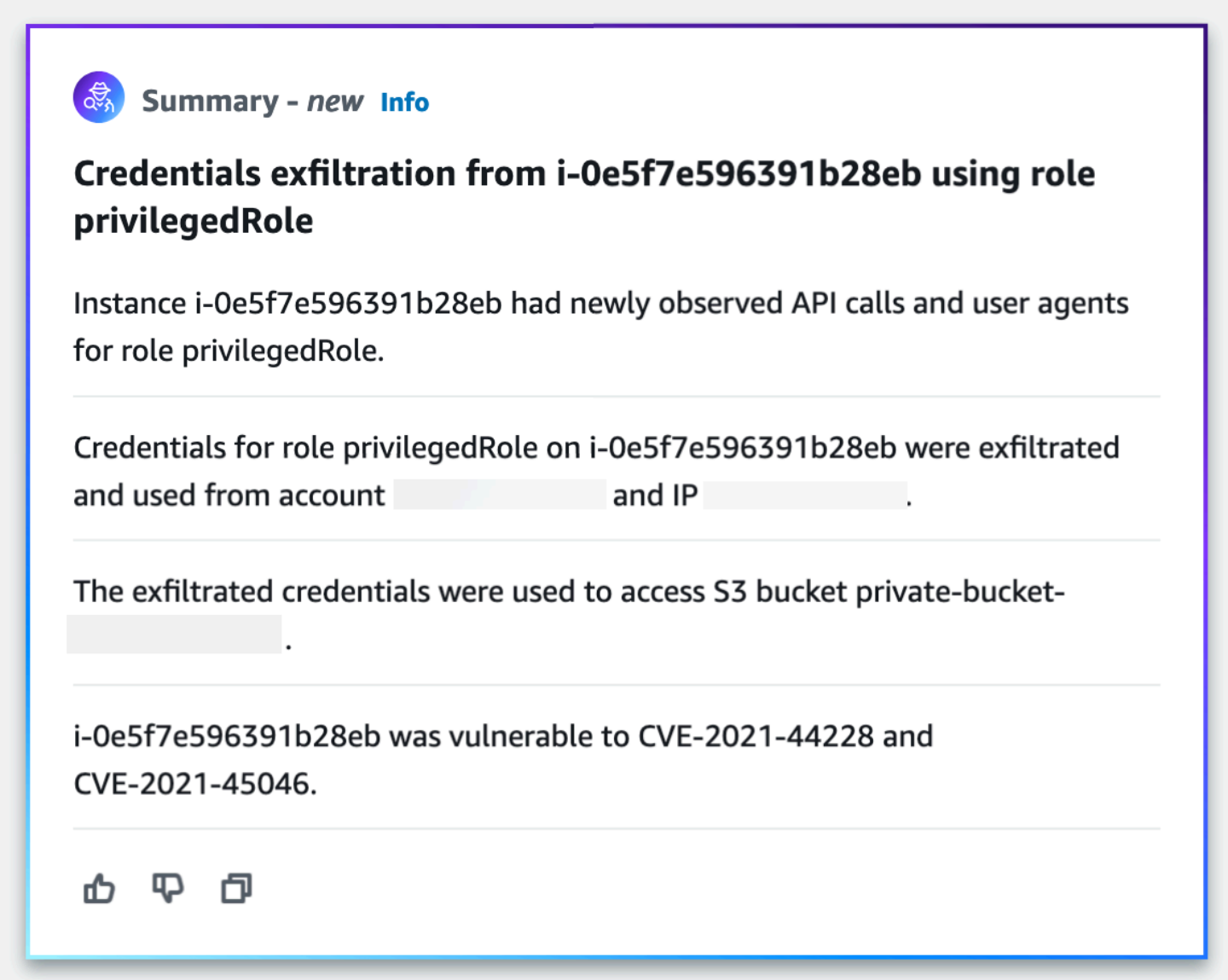
조사 결과 그룹의 조사 결과 그룹 요약은 보안 이벤트에 대한 명확하고 상세한 설명을 제공합니다. 자연어 설명에는 간결한 제목, 관련 리소스 요약, 해당 리소스에 대한 선별된 정보가 포함됩니다.

조사 결과 그룹 요약을 검토하려면

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 조사 결과 그룹을 선택합니다.
3. 조사 결과 그룹 테이블에서 요약을 표시할 조사 결과 그룹을 선택합니다. 세부 정보 페이지가 나타납니다.

세부 정보 페이지에서 요약 창을 사용하여 조사 결과 그룹의 상위 조사 결과에 대해 생성된 설명 요약을 검토할 수 있습니다. 또한 조사 결과 그룹의 주요 위협 이벤트에 대한 분석을 검토한 다음 더 자세히 조사할 수 있습니다. 생성된 요약을 메모나 티켓팅 시스템에 추가하려면 창에서 복사 아이콘을 선택합니다. 요약이 클립보드에 복사됩니다. 요약에서 조사 결과 그룹 요약 출력에 대한 피드백을 공유할 수도 있습니다. 그러면 향후 더 나은 경험을 제공할 수 있습니다. 피드백을 공유하려면 피드백의 성격에 따라 좋아요 또는 싫어요 아이콘을 선택합니다.

> **Note**
>
> 조사 결과 그룹 요약에 대한 피드백을 제공하는 경우 피드백은 모델 조정에 사용되지 않습니다. Detective의 프롬프트를 효과적으로 제작하기 위한 용도로만 사용됩니다.



결과 그룹 요약 옵트아웃

기본적으로 조사 결과 그룹에는 조사 결과 그룹 요약이 활성화되어 있습니다. 조사 결과 그룹 요약 기능을 사용하지 않으려는 고객은 사용자 수준에서 또는 AWS 관리 콘솔에 액세스하는 데 사용되는 IAM 역할을 통해 옵트아웃할 수 있습니다.

사용자 수준 옵트아웃

Detective에 액세스하는 각 사용자는 결과 그룹 요약 기능을 옵트아웃하도록 개별 기본 설정을 지정할 수 있습니다. 요약을 옵트아웃하면 조사 결과 그룹 데이터가 교차 리전 추론을 통해 처리되지 않습니다.

결과 그룹 요약을 옵트아웃하려면

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 Preferences(기본 설정)를 선택합니다.
3. 조사 결과 그룹 요약에서 편집을 선택합니다.
4. 활성화됨을 끕니다.
5. 저장을 선택합니다.

IAM 역할 기반 옵트아웃

Detective에 액세스하는 데 사용되는 IAM 역할을 수정하여 여러 사용자가 결과 그룹 요약 기능을 옵트아웃할 수 있습니다. 역할에 대한 `detective:InvokeAssistant` 권한에 대해 거부 문을 추가하면 해당 역할을 통해 Detective에 액세스하는 모든 사용자가 결과 그룹 요약 기능을 사용하지 못하게 되어 리전 간 추론을 통해 결과 그룹 데이터를 처리할 수 없습니다. 그런 다음 사용자는 사용자 수준 옵트아웃 단계를 개별적으로 수행하여 요약 창이 나타나지 않도록 할 수 있습니다.

IAM을 사용하여 조사 결과 그룹 요약을 옵트아웃하려면

1. Amazon Detective에 액세스하는 데 사용되는 IAM 역할을 식별합니다.
2. `detective:InvokeAssistant` 작업에 대한 `Deny` 효과가 포함된 IAM 정책 설명을 역할에 추가합니다.

조사 결과 그룹 요약 활성화

이전에 조사 결과 그룹에 대한 조사 결과 그룹 요약을 옵트아웃한 경우 언제든지 다시 활성화할 수 있습니다.

조사 결과 그룹 요약을 활성화하려면

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 Preferences(기본 설정)를 선택합니다.
3. 조사 결과 그룹 요약에서 편집을 선택합니다.
4. 활성화됨을 켭니다.
5. 저장을 선택합니다.

교차 리전 추론

Detective는 지리 내에서 최적의 AWS 리전을 자동으로 선택하여 결과 그룹 데이터를 처리하고 요약을 생성합니다. 이렇게 하면 사용 가능한 컴퓨팅 리소스와 모델 가용성이 극대화되고 최상의 고객 경험이 제공됩니다. 조사 결과 그룹 데이터는 요약 요청이 시작된 리전에만 저장되지만 조사 결과 그룹 데이터 및 요약 결과는 해당 리전 외부에서 처리될 수 있습니다. 모든 데이터는 Amazon의 보안 네트워크를 통해 암호화되어 전송됩니다.

Detective는 다음 표와 같이 요청이 시작된 지리적 영역 내의 사용 가능한 컴퓨팅 리소스로 추론 요청을 안전하게 라우팅합니다.

리전 간 추론 라우팅

지원되는 Detective 지리	Detective 리전	추론 리전
미국	us-east-1	us-east-1, us-east-2, us-west-1, us-west-2
	us-west-2	us-east-1, us-east-2, us-west-1, us-west-2
유럽	eu-central-1	eu-central-1, eu-central-2, eu-north-1, eu-south-1, eu-south-2, eu-west-1, eu-west-2, eu-west-3
일본	ap-northeast-1	ap-northeast-1, ap-northeast-3

지원되는 리전:

결과 그룹 요약은 다음 AWS 리전에서 사용할 수 있습니다.

- 미국 동부(버지니아 북부)
- 미국 서부(오레곤)
- 아시아 태평양(도쿄)
- 유럽(프랑크푸르트)

Amazon GuardDuty 조사 결과 보관

Amazon GuardDuty 조사 결과에 대한 조사를 완료하면 Amazon Detective의 조사 결과를 보관할 수 있습니다. 이를 통해 업데이트를 하기 위해 GuardDuty로 돌아가야 하는 수고를 덜 수 있습니다. 조사 결과를 보관하면 조사를 마쳤다는 뜻입니다.

조사 결과와 관련된 계정의 GuardDuty 관리자 계정이기도 한 경우에만 Detective 내에서 GuardDuty 조사 결과를 보관할 수 있습니다. GuardDuty 관리자 계정이 아닌 사용자가 조사 결과를 보관하려고 하면 GuardDuty에 오류가 표시됩니다.

GuardDuty 조사 결과 보관

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. Detective 콘솔의 조사 결과 세부 정보 패널에서 조사 결과 보관을 선택합니다.
3. 확인하라는 메시지가 나타나면 보관을 선택합니다.

보관된 GuardDuty 조사 결과는 GuardDuty 콘솔에서 볼 수 있습니다. 보관된 결과는 90일 동안 GuardDuty에 저장되며 해당 기간 동안 언제든지 볼 수 있습니다. 결과 테이블에서 아카이브됨을 선택하거나 serviceGuardDuty의 afindingCriteriacriterion이 true인 ListFindingsAPI를 사용하여 GuardDuty API를 통해 GuardDuty 콘솔에서 억제된 결과를 볼 수 있습니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 금지 규칙을 참조하세요.

Amazon Detective에서 개체 분석

엔터티는 소스 데이터에서 추출한 단일 객체입니다. 예로는 특정 IP 주소, Amazon EC2 인스턴스 또는 AWS 계정이 있습니다. 이벤트 유형 목록은 the section called “동작 그래프 데이터 구조의 엔터티 유형” 섹션을 참조하세요.

Amazon Detective 엔터티 프로필은 엔터티 및 해당 활동에 대한 세부 정보를 제공하는 단일 페이지입니다. 엔터티 프로필은 조사 결과에 대한 조사를 위한 지원 세부 정보를 얻거나 의심스러운 활동에 대한 일반적인 추적의 일환으로 사용할 수 있습니다.

내용

개체 프로파일 사용

엔터티 프로필은 다음 작업 중 하나를 수행할 때 나타납니다.

- Amazon GuardDuty 콘솔에서 선택한 조사 결과와 관련된 엔터티를 조사하는 옵션을 선택합니다.

  the section called “다른 콘솔에서 피벗”을(를) 참조하세요.
- 엔터티 프로필을 보려면 Detective URL로 이동합니다.

  the section called “URL을 사용하여 이동”을(를) 참조하세요.
- Detective 콘솔에서 Detective 조사을 사용하여 엔터티를 조회할 수 있습니다.
- 다른 엔터티 프로필 또는 조사 결과 개요에서 엔터티 프로필로 연결되는 링크를 선택합니다.

엔터티 프로파일의 범위 시간

범위 시간을 제공하지 않고 엔터티 프로필로 직접 이동하면 범위 시간이 이전 24시간으로 설정됩니다.

다른 엔터티 프로파일에서 엔터티 프로파일로 이동해도 현재 선택한 범위 시간이 그대로 유지됩니다.

조사 결과 개요에서 엔터티 프로필로 이동하면 범위 시간이 조사 결과 기간으로 설정됩니다.

엔터티 프로필에 표시되는 데이터를 제한하기 위해 범위 시간을 사용자 지정하는 방법에 대한 자세한 내용은 범위 시간 관리를 참조하세요.

엔터티 식별자 및 유형

프로필 상단에는 엔터티 식별자와 엔터티 유형이 있습니다. 각 엔터티 유형에는 해당 아이콘이 있어 프로필 유형의 시각적 지표기를 제공합니다.

관련 조사 결과

각 프로필에는 범위 시간 동안 해당 엔터티가 관여한 조사 결과 목록이 포함되어 있습니다.

각 조사 결과에 대한 세부 정보를 확인하고, 범위 시간을 조사 결과 기간으로 변경하며, 조사 결과 개요로 이동하여 다른 관련 리소스를 찾아볼 수 있습니다.

the section called “엔터티에 대한 조사 결과 보기”을(를) 참조하세요.

해당 엔터티와 관련된 조사 결과 그룹

각 프로필에는 엔터티가 포함된 조사 결과 그룹 목록이 포함되어 있습니다.

조사 결과 그룹은 발생 가능한 보안 문제에 대한 추가 컨텍스트를 제공하기 위해 Detective가 그룹으로 수집하는 조사 결과, 엔터티 및 증거로 구성됩니다.

조사 결과 그룹에 대한 자세한 내용은 the section called “결과 그룹” 섹션을 참조하셍쇼.

엔터티 세부 정보 및 분석 결과를 포함하는 프로필 패널

각 엔터티 프로필에는 하나 이상의 탭 세트가 포함되어 있습니다. 각 탭에는 하나 이상의 프로필 패널이 포함되어 있습니다. 각 프로필 프로필에는 동작 그래프 데이터에서 생성된 텍스트 및 시각화가 포함되어 있습니다. 특정 탭과 프로필 패널은 엔터티 유형에 맞게 조정됩니다.

대부분의 엔터티의 경우 첫 번째 탭 상단의 패널은 엔터티에 대한 높은 수준의 요약 정보를 제공합니다.

다른 프로필 패널은 다양한 유형의 활동을 강조 표시합니다. 조사 결과와 관련된 엔터티의 경우, 엔터티 프로필 패널에 있는 정보는 조사를 완료하는 데 도움이 되는 추가 증거 자료를 제공할 수 있습니다. 각 프로필 패널은 정보 사용 방법에 대한 지침을 제공합니다. 자세한 내용은 the section called “프로필 패널 지침 사용” 단원을 참조하십시오.

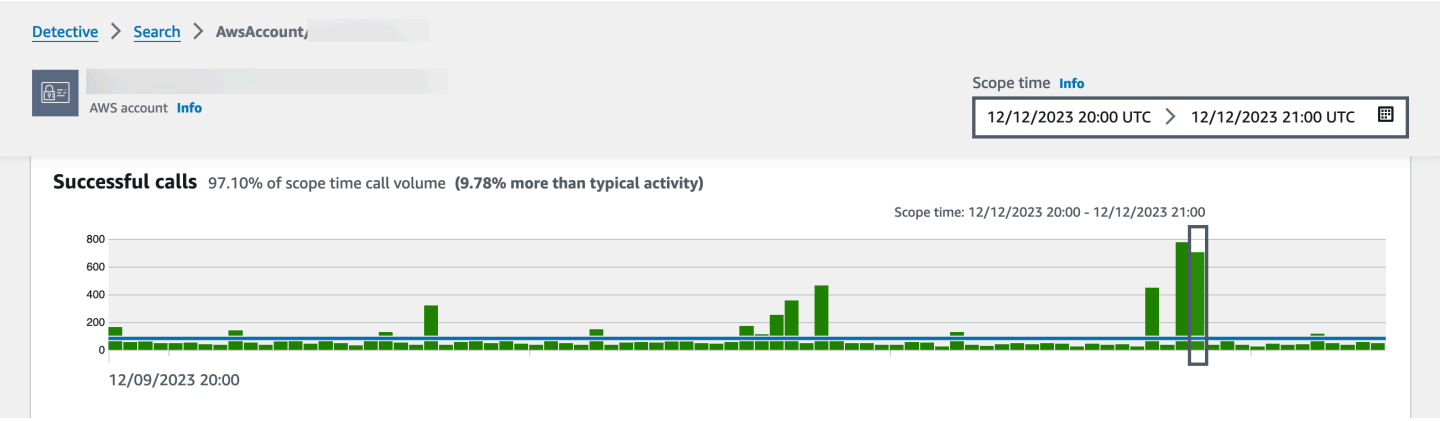
프로필 패널, 프로필 패널에 포함된 데이터 유형, 프로필 패널과 상호 작용하는 데 사용할 수 있는 옵션에 대한 자세한 정보는 the section called “프로필 패널” 섹션을 참조하세요.

개체 프로필 탐색

엔터티 프로필에는 하나 이상의 탭 세트가 포함되어 있습니다. 각 탭에는 하나 이상의 프로필 패널이 포함되어 있습니다. 각 프로필 프로필에는 동작 그래프 데이터에서 생성된 텍스트 및 시각화가 포함되어 있습니다.

프로필 탭을 아래로 스크롤해도 프로필 상단에 다음과 같은 정보가 계속 표시됩니다.

- 엔터티 유형
- 엔터티 식별자
- 범위 시간



Detective 프로필 패널 보기 및 상호 작용

Amazon Detective 콘솔의 각 엔터티 프로필은 프로필 패널 세트로 구성되어 있습니다. 프로필 패널은 일반적인 세부 정보를 제공하거나 엔터티와 관련된 특정 활동을 강조 표시하는 시각화입니다. 프로필

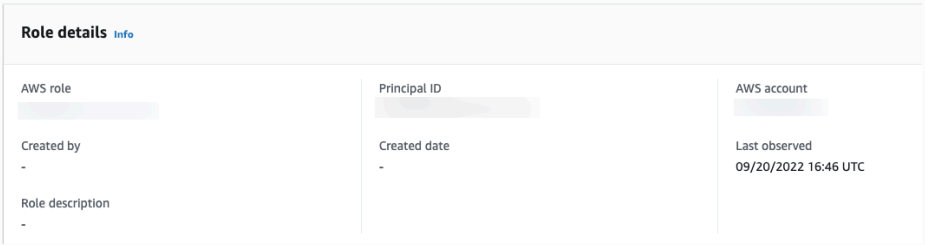
패널은 다양한 유형의 시각화를 사용하여 다양한 유형의 정보를 표시합니다. 추가 세부 정보 또는 다른 프로필로 연결되는 링크를 제공할 수도 있습니다.

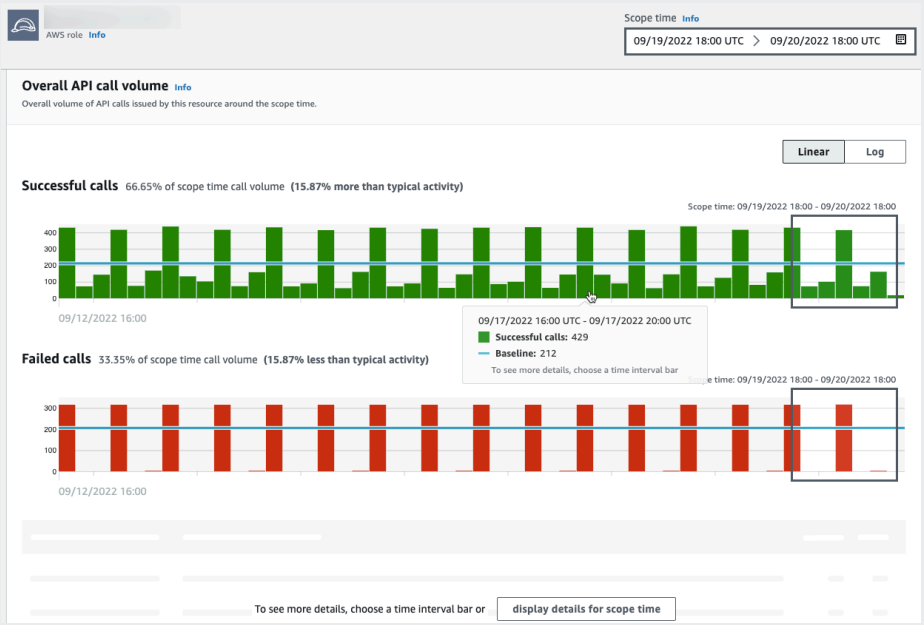
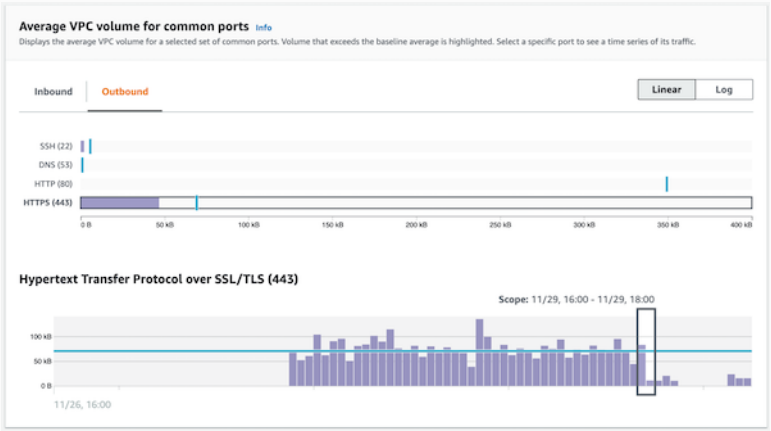
각 프로필 패널은 분석가가 엔터티 및 관련 활동에 대한 특정 질문에 대한 답을 찾는 데 도움을 주기 위한 것입니다. 이러한 질문에 대한 답은 해당 활동이 진정한 위협인지 여부에 대한 결론을 내리는 데 도움이 됩니다.

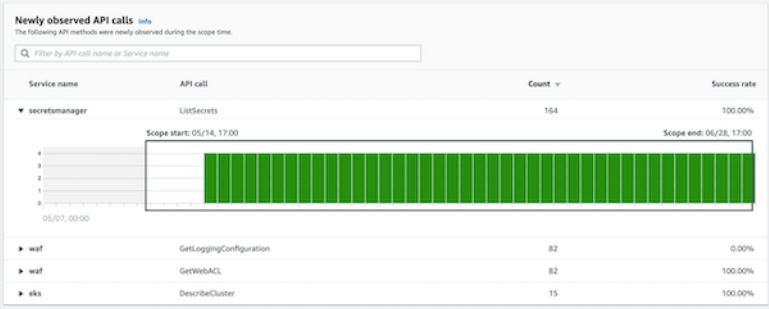
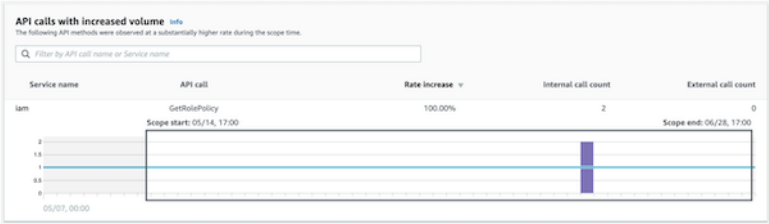
프로필 패널은 다양한 유형의 시각화를 사용하여 다양한 유형의 정보를 표시합니다.

프로필 패널의 정보 유형

프로필 패널은 일반적으로 다음과 같은 유형의 데이터를 제공합니다.

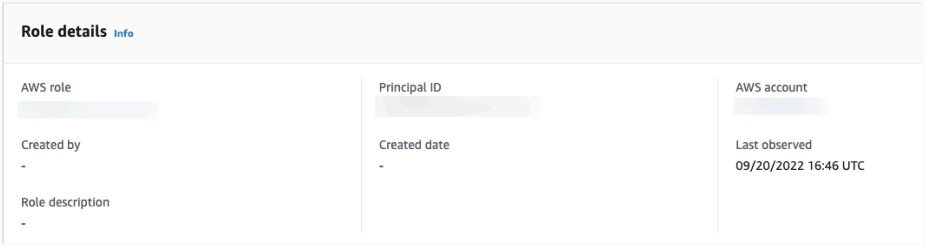
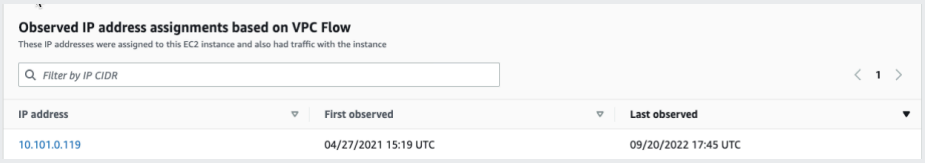
패널 데이터 유형	설명
조사 결과 또는 엔터티에 대한 상위 수준 정보	가장 간단한 패널 유형은 엔터티에 대한 몇 가지 기본 정보를 제공합니다. 정보 패널에 포함되는 정보의 예로는 식별자, 이름, 유형, 생성 날짜 등이 있습니다.  대부분의 엔터티 프로필에는 해당 엔터티에 대한 정보 패널이 포함되어 있습니다.
시간 경과에 따른 활동에 대한 일반적인 요약	시간 경과에 따른 엔터티의 활동 요약을 표시합니다. 이 유형의 패널은 범위 기간 동안 엔터티가 어떻게 동작하는지에 대한 전반적인 보기를 제공합니다.

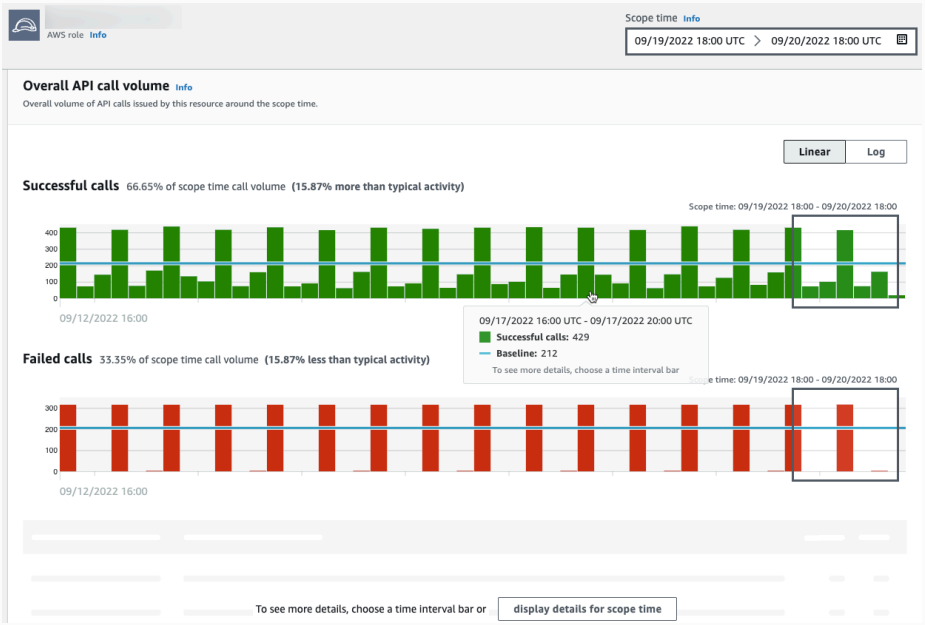
패널 데이터 유형	설명
	 다음은 Detective 프로필 패널에 제공된 요약 데이터 예입니다. • 실패한 통화 및 성공한 API 통화 • 인바운드 및 아웃바운드 VPC 볼륨
값별로 그룹화된 활동 요약	엔터티의 활동 요약을 특정 값별로 그룹화하여 표시합니다. EC2 인스턴스의 프로파일에서 이러한 유형의 프로파일 패널을 볼 수 있습니다. 프로파일 패널은 특정 유형의 서비스와 연결된 공통 포트의 EC2 인스턴스에서 주고받는 VPC 흐름 로그 데이터의 평균 볼륨을 보여줍니다. 

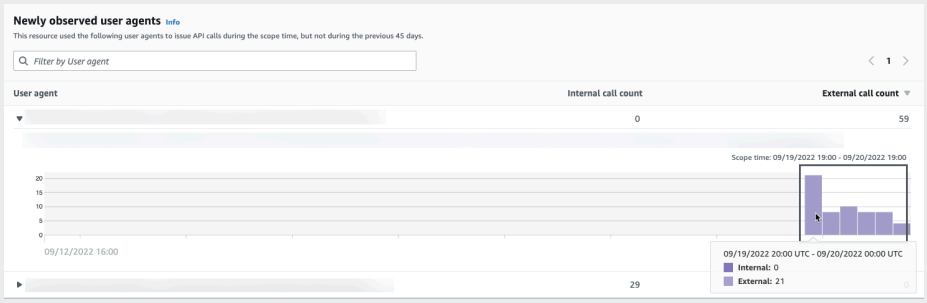
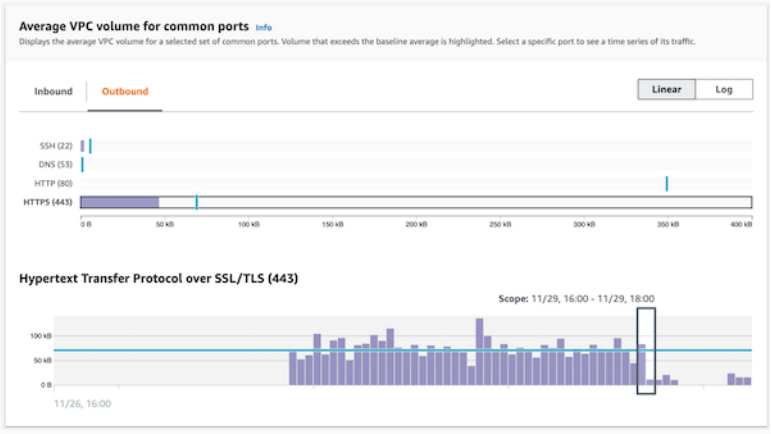
패널 데이터 유형	설명
범위 시간 동안에만 시작된 활동	조사 중에 특정 기간 동안에만 어떤 활동이 시작되었는지 확인하는 것이 중요합니다. 예를 들어 이전에는 볼 수 없었던 API 통화, 지리적 위치 또는 사용자 에이전트가 있나요?  동작 그래프가 아직 훈련 모드인 경우 프로필 패널에 알림 메시지가 표시됩니다. 동작 그래프에 최소 2주 분량의 데이터가 누적되면 메시지가 삭제됩니다. 훈련 모드에 관한 자세한 정보는 the section called “새로운 동작 그래프에 대한 훈련 기간” 섹션을 참조하세요.
범위 시간 동안 크게 변경된 활동	새 활동 패널과 마찬가지로 프로필 패널도 범위 시간 동안 크게 변경된 활동을 표시할 수 있습니다. 예를 들어, 사용자는 정기적으로 일주일에 몇 번 특정 API 호출을 실행할 수 있습니다. 동일한 사용자가 갑자기 하루에 같은 호출을 여러 번 하면 이는 악의적인 활동의 증거일 수 있습니다.  동작 그래프가 아직 훈련 모드인 경우 프로필 패널에 알림 메시지가 표시됩니다. 동작 그래프에 최소 2주 분량의 데이터가 누적되면 메시지가 삭제됩니다. 훈련 모드에 관한 자세한 정보는 the section called “새로운 동작 그래프에 대한 훈련 기간” 섹션을 참조하세요.

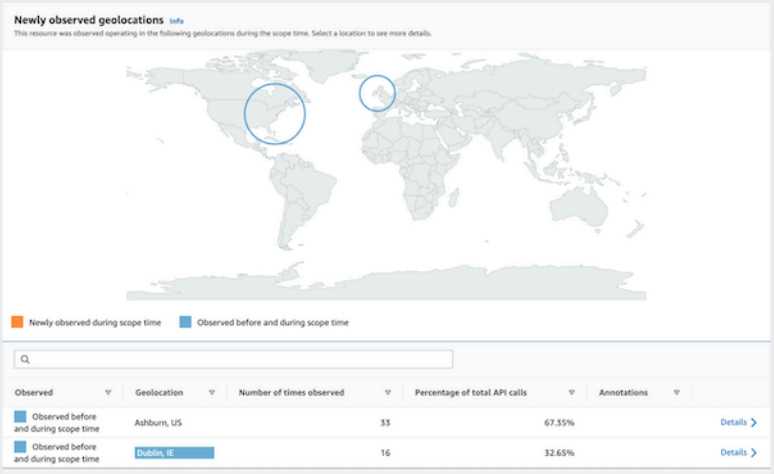
프로필 패널 시각화 유형

프로필 패널 내용은 다음 양식 중 하나를 사용할 수 있습니다.

시각화 유형	설명
키-값 페어	가장 간단한 시각화 유형은 키-값 페어의 집합입니다. 키-값 페어 패널의 가장 일반적인 예는 조사 결과 또는 엔터티 정보 패널입니다.  키-값 페어를 사용하여 다른 유형의 패널에 추가 정보를 추가할 수도 있습니다. 키-값 페어 패널에서 값이 엔터티의 식별자인 경우 해당 프로필로 피벗할 수 있습니다.
표	테이블은 여러 열로 구성된 간단한 항목 목록입니다.  표를 정렬하고, 필터링하고, 페이지를 넘길 수 있습니다. 각 페이지에 표시할 엔터티 수를 변경할 수 있습니다. the section called “프로필 패널 기본 설정”을 참조하세요. 테이블의 값이 엔터티의 식별자인 경우 해당 프로필로 피벗할 수 있습니다.
타임라인	타임라인 시각화는 시간 경과에 따른 정의된 간격의 집계된 값을 보여줍니다.

시각화 유형	설명
	 타임라인은 현재 범위 시간을 강조 표시하고 범위 시간 전후의 추가 주변 시간을 포함합니다. 주변 시간은 범위 시간의 활동에 대한 컨텍스트를 제공합니다. 시간 간격을 마우스로 가리키면 해당 시간 간격의 데이터 요약이 표시됩니다.

시각화 유형	설명
확장 가능한 테이블	확장 가능한 테이블은 테이블과 타임라인을 결합합니다.  시각화는 테이블로 시작됩니다. 표를 정렬하고, 필터링하고, 페이지를 넘길 수 있습니다. 각 페이지에 표시할 엔터티 수를 변경할 수 있습니다. the section called “프로필 패널 기본 설정”을 참조하세요. 그런 다음 각 행을 확장하여 해당 행과 관련된 타임라인 시각화를 표시할 수 있습니다.
막대 차트	막대형 차트는 그룹화를 기반으로 값을 표시합니다. 차트에 따라 막대를 선택하여 관련 활동의 타임라인을 표시할 수 있습니다. 

시각화 유형	설명
지리적 위치 차트	지리적 위치 차트는 지리적 위치를 기반으로 데이터를 강조 표시하도록 표시된 지도를 표시합니다. 그 다음에는 개별 지리적 위치에 대한 세부 정보가 포함된 테이블이 표시될 수 있습니다.  참고로 Detective는 수신되는 지리 데이터를 처리할 때 위도 및 경도 값을 소수점 한 자리까지 반올림합니다.

프로필 패널 콘텐츠에 대한 참고 사항

프로필 패널 내용을 볼 때 다음 사항에 유의하세요.

대략적인 개수 데이터 경고

이 경고는 적용 가능한 데이터의 양으로 인해 개수가 매우 적은 항목은 표시되지 않음을 나타냅니다.

완전히 정확하게 개수를 계산하려면 데이터 양을 줄입니다. 가장 간단한 방법은 범위 시간의 길이를 줄이는 것입니다. the section called “범위 시간 관리”을 참조하세요.

지리적 위치에 대한 반올림

Detective는 모든 위도 및 경도 값을 소수점 한 자리까지 반올림합니다.

Detective가 API 호출을 나타내는 방식에 대한 변경 사항

2021년 7월 14일부터 Detective는 각 API 호출을 수행한 서비스를 추적합니다. Detective가 API 메서드를 표시할 때마다 연결된 서비스도 표시됩니다. API 호출에 대한 정보를 표시하는 프로필 패널

에서 호출은 항상 서비스별로 그룹화됩니다. 해당 날짜 이전에 Detective에서 수집한 데이터의 경우 서비스 이름이 알 수 없는 서비스로 표시됩니다.

또한 2021년 7월 14일부터 계정 및 역할의 경우 전체 API 통화 볼륨 프로필 패널의 활동 세부 정보에는 더 이상 통화를 실행한 리소스AKID의 가 표시되지 않습니다. 계정의 경우 Detective는 호출을 실행한 보안 주체(사용자 또는 역할)의 식별자를 표시합니다. 역할의 경우 Detective는 역할 세션의 식별자를 표시합니다. Detective가 2021년 7월 14일 이전에 수집한 데이터의 경우 식별자는 알 수 없는 리소스로 표시됩니다.

API 호출 목록을 표시하는 프로파일 패널의 경우 관련 타임라인은 이 전환이 발생한 기간을 강조 표시합니다. 강조 표시는 2021년 7월 14일에 시작되며, 업데이트가 Detective에 완전히 전파되면 종료됩니다.

프로필 패널의 기본 설정 지정

프로파일 패널의 경우 프로파일 패널의 각 페이지에 표시되는 행 수를 로 사용자 지정하고 타임스탬프 형식 기본 설정을 구성할 수 있습니다.

테이블 길이 설정

테이블 또는 확장 가능한 테이블을 포함하는 프로필 패널의 경우 각 페이지에 표시할 행 수를 구성할 수 있습니다.

각 페이지의 엔터티 수에 대한 기본 설정을 지정합니다.

1. 에서 Amazon Detective 콘솔을 엽니다https://console.aws.amazon.com/detective/.
2. Detective 탐색 창의 설정에서 기본 설정을 선택합니다.
3. 기본 설정 페이지의 표 길이에서 편집을 클릭합니다.
4. 각 페이지에 표시할 테이블 행 수를 선택합니다.
5. 저장(Save)을 선택합니다.

타임스탬프 형식 설정

프로필 패널의 경우 Detective의 각 IAM 사용자 또는 IAM 역할에 대한 모든 타임스탬프에 적용될 타임스탬프 형식 기본 설정을 구성할 수 있습니다.

> **Note**
>
> 타임스탬프 형식 기본 설정은 전체 AWS 계정에 적용되지 않습니다.

타임스탬프의 기본 설정 지정

1. 에서 Amazon Detective 콘솔을 엽니다https://console.aws.amazon.com/detective/.
2. Detective 탐색 창의 설정에서 기본 설정을 선택합니다.
3. 기본 설정 페이지의 타임스탬프 기본 설정에서 모든 타임스탬프에 대해 선호하는 표시를 확인하고 변경할 수 있습니다.
4. 기본적으로 타임스탬프 형식은 로 설정됩니다UTC. 편집을 클릭하여 현지 시간대를 선택합니다.

   예시

   Example

   UTC - 09/20/22 16:39 UTC

   로컬 - 09/20/2022 9:39(UTC-07:00)
5. 저장(Save)을 선택합니다.

엔터티 프로필 또는 조사 결과 개요로 직접 이동

Amazon Detective에서 엔터티 프로필 또는 조사 결과 개요로 직접 이동하기 위해 다음 옵션 중 하나를 사용할 수 있습니다.

- Amazon GuardDuty 또는에서 GuardDuty 결과에서 해당 Detective 결과 프로필로 피벗할 AWS Security Hub CSPM수 있습니다.
- 조사 결과 또는 엔터티를 식별하고 사용할 범위 시간을 설정하는 Detective URL을 조합할 수 있습니다.

Amazon GuardDuty 또는에서 개체 프로필 또는 결과 개요로 피벗 AWS Security Hub CSPM

Amazon GuardDuty 콘솔에서 조사 결과와 관련된 엔터티의 엔터티 프로필로 이동할 수 있습니다.

GuardDuty 및 AWS Security Hub CSPM 콘솔에서 결과 개요로 이동할 수도 있습니다. 여기에는 관련 엔터티의 엔터티 프로파일에 대한 링크도 제공됩니다.

이러한 링크는 조사 프로세스를 간소화하는 데 도움이 될 수 있습니다. Detective를 사용하여 관련 엔터티 활동을 빠르게 확인하고 다음 단계를 결정할 수 있습니다. 그런 다음 조사 결과가 거짓 긍정인지 여부를 보관하거나 더 자세히 탐색하여 문제의 범위를 파악할 수 있습니다.

Amazon Detective 콘솔로 피벗하는 방법

조사 링크는 모든 GuardDuty 조사 결과에 사용할 수 있습니다. 또한 GuardDuty를 사용하면 엔터티 프로필로 이동할지 또는 조사 결과 개요로 이동할지 선택할 수 있습니다.

GuardDuty 콘솔에서 Detective로 피벗

1. https://console.aws.amazon.com/guardduty/에서 GuardDuty 콘솔을 엽니다.
2. 필요한 경우 왼쪽 탐색 창에서 조사 결과를 선택합니다.
3. GuardDuty 조사 결과 페이지에서 조사 결과를 선택합니다.

   조사 결과 세부 정보 창은 조사 결과 목록 오른쪽에 표시됩니다.
4. 조사 결과 세부 정보 창에서 Detective에서 조사를 선택합니다.

   GuardDuty는 Detective에서 조사할 수 있는 항목 목록을 표시합니다.

   목록에는 IP 주소 또는 EC2 인스턴스와 같은 관련 엔터티와 조사 결과가 모두 포함되어 있습니다.
5. 엔터티 또는 조사 결과를 선택합니다.

   Detective 콘솔이 새 탭에서 열립니다. 콘솔이 열리고 엔터티 또는 조사 결과 프로필이 표시됩니다.

   Detective를 활성화하지 않은 경우 콘솔에서 Detective에 대한 개요를 제공하는 랜딩 페이지가 열립니다. 여기에서 Detective를 활성화하도록 선택할 수 있습니다.

Security Hub CSPM 콘솔에서 Detective로 피벗하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 필요한 경우 왼쪽 탐색 창에서 조사 결과를 선택합니다.
3. Security Hub CSPM 조사 결과 페이지에서 GuardDuty 조사 결과를 선택합니다.
4. 세부 정보 창에서 Detective에서 조사를 선택한 다음 조사 결과 조사를 선택합니다.

조사 결과 조사를 선택하면 Detective 콘솔이 새 탭에서 열립니다. 콘솔이 열리고 조사 결과 개요가 표시됩니다.

집계 영역에서 피벗하더라도 Detective 콘솔은 조사 결과가 발생한 리전으로 항상 열립니다. 집계 조사에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 리전별 조사 결과 집계를 참조하세요.

Detective를 활성화하지 않은 경우 콘솔에서 Detective 랜딩 페이지가 열립니다. 여기에서 Detective를 활성화할 수 있습니다.

피벗 문제 해결

피벗을 사용하려면 다음이 true여야 합니다.

- 계정은 Detective 및 피벗 대상 서비스 모두의 관리자 계정이어야 합니다.
- 관리자 계정에 동작 그래프에 대한 액세스 권한을 부여하는 크로스 계정 역할을 맡았습니다.

관리자 계정 정렬 권장 사항에 대한 자세한 내용은 Amazon GuardDuty 및 와의 권장 정렬을 AWS Security Hub CSPM 참조하세요.

피벗이 작동하지 않는 경우 다음을 확인합니다.

- 조사 결과가 동작 그래프에서 활성화된 멤버 계정에 속합니까? 관련 계정이 멤버 계정으로 동작 그래프에 초대되지 않은 경우 동작 그래프에는 해당 계정에 대한 데이터가 포함되지 않습니다.

  초대된 멤버 계정이 초대를 수락하지 않은 경우 동작 그래프에는 해당 계정에 대한 데이터가 포함되지 않습니다.
- 조사 결과가 보관되었습니까? Detective는 GuardDuty로부터 보관된 조사 결과를 받지 않습니다.
- Detective가 동작 그래프에 데이터를 수집하기 시작하기 전에 조사 결과가 있었습니까? Detective가 수집하는 데이터에 해당 조사 결과가 없으면 동작 그래프에 해당 데이터가 포함되지 않습니다.
- 조사 결과가 정확한 리전에서 나온 결과입니까? 각 동작 그래프는 리전별로 다릅니다. 동작 그래프에는 다른 리전의 데이터가 포함되지 않습니다.

URL을 사용하여 엔터티 프로파일 또는 조사 결과 개요로 이동

Amazon Detective에서 엔터티 프로필 또는 조사 결과 개요로 이동하기 위해 직접 연결되는 링크를 제공하는 URL을 사용할 수 있습니다. URL은 조사 결과 또는 엔터티를 식별합니다. 또한 프로필에서 사용할 범위 시간을 지정할 수 있습니다. Detective는 최대 1년의 과거 이벤트 데이터를 유지 관리합니다.

프로필 URL 형식

> **Note**
>
> 이전 URL 형식을 사용하는 경우 Detective는 자동으로 새 URL로 리디렉션합니다. 이전 URL 형식은 다음과 같습니다.
> https://console.aws.amazon.com/detective/home?region=*Region*#*type*/*namespace*/*instanceID*?*parameters*

프로필 URL의 새 형식은 다음과 같습니다.

- 엔터티의 경우 - https://console.aws.amazon.com/detective/home?region=*Region*#*entities*/*namespace*/*instanceID*?*parameters*
- 조사 결과의 경우 - https://console.aws.amazon.com/detective/home?region=*Region*#*findings*/*instanceID*?*parameters*

URL에는 다음 값이 필요합니다.

##

사용하려는 리전.

type

이동하려는 프로필의 항목 유형.

- `entities` - 엔터티 프로파일로 이동 중임을 나타냄
- `findings` – 조사 결과 개요로 이동 중임을 나타냄

######

엔터티의 경우 네임스페이스는 엔터티 유형의 이름입니다.

- `AwsAccount`
- `AwsRole`

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

instanceID

조사 결과 또는 엔터티의 인스턴스 식별자입니다.

- GuardDuty 조사 결과의 경우 GuardDuty 조사 결과 식별자입니다.
- AWS 계정의 경우 계정 ID입니다.
- AWS 역할 및 사용자의 경우 역할 또는 사용자의 보안 주체 ID입니다.
- 페더레이션 사용자의 경우 페더레이션 사용자의 보안 주체 ID입니다. 보안 주체 ID는 *<identityProvider>*:*<username>* 또는 *<identityProvider>*:*<audience>*:*<username>*입니다.
- IP 주소의 경우 IP 주소입니다.
- 사용자 에이전트의 경우 사용자 에이전트 이름입니다.
- EC2 인스턴스의 경우, 인스턴스 ID입니다.
- 역할 세션의 경우 세션 식별자입니다. 세션 식별자는 *<rolePrincipalID>*:*<sessionName>* 형식을 사용합니다.
- S3 버킷의 경우 버킷 이름입니다.
- FindingGroups의 경우 UUID(예: ca6104bc-a315-4b15-bf88-1c1e60998f83)입니다.
- EKS 리소스의 경우 다음 형식을 사용합니다.
  - EKS클러스터: *<clusterName>~<accountId>~EKS*
  - Kubernetes 포드: *<podUid>~<clusterName>~<accountId>~EKS*
  - Kubernetes 객체: *<subjectName>~<clusterName>~<accountId>*

- 컨테이너 이미지: *<registry>/<repository>:<tag>@<digest>*

조사 결과 또는 엔터티는 동작 그래프에서 활성화된 계정과 연결되어야 합니다.

URL에는 범위 시간을 설정하는 데 사용되는 다음과 같은 선택적 파라미터도 포함될 수 있습니다. 범위 시간 및 프로필에서의 범위 시간 사용 방법에 대한 자세한 내용은 the section called “범위 시간 관리” 섹션을 참조하세요.

`scopeStart`

프로필에서 사용할 범위 시간의 시작 시간. 시작 시간은 지난 365일 이내여야 합니다.

값은 에포크 타임스탬프입니다.

시작 시간은 제공하지만 종료 시간은 제공하지 않는 경우 범위 시간은 현재 시간에 종료됩니다.

`scopeEnd`

프로필에서 사용할 범위 시간의 종료 시간.

값은 에포크 타임스탬프입니다.

종료 시간은 제공하지만 시작 시간은 제공하지 않는 경우 범위 시간에는 종료 시간 이전의 모든 시간이 포함됩니다.

범위 시간을 지정하지 않으면 기본 범위 시간이 사용됩니다.

- 조사 결과의 경우 기본 범위 시간은 조사 결과 활동이 관찰된 첫 번째 시간과 마지막 시간을 사용합니다.
- 엔터티의 경우 기본 범위 시간은 이전 24시간입니다.

다음은 Detective URL의 예입니다.

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

이 예제 URL은 다음 지침을 따릅니다.

- IP 주소 192.168.1의 엔터티 프로필을 표시합니다.
- 범위 시간은 2019년 3월 18일 월요일 오전 12:00:00 GMT로 시작하여 2019년 3월 18일 월요일 오후 12:00:00 GMT로 종료되는 시간을 사용합니다.

URL 문제 해결

URL에 예상 프로필이 표시되지 않는 경우 먼저 URL이 올바른 형식을 사용하고 올바른 값을 입력했는지 확인합니다.

- 올바른 URL(`findings`또는`entities`)로 시작했습니까?
- 올바른 네임스페이스를 지정했습니까?
- 올바른 식별자를 입력했습니까?

값이 정확하면 다음 사항도 확인할 수 있습니다.

- 조사 결과 또는 엔터티가 동작 그래프에서 활성화된 멤버 계정에 속합니까? 관련 계정이 멤버 계정으로 동작 그래프에 초대되지 않은 경우 동작 그래프에는 해당 계정에 대한 데이터가 포함되지 않습니다.

  초대된 멤버 계정이 초대를 수락하지 않은 경우 동작 그래프에는 해당 계정에 대한 데이터가 포함되지 않습니다.
- 조사 결과의 경우, 조사 결과가 보관되었습니까? Detective는Amazon GuardDuty로부터 보관된 조사 결과를 받지 않습니다.
- Detective가 동작 그래프에 데이터를 수집하기 시작하기 전에 조사 결과 또는 엔터티가 있었습니까? Detective가 수집하는 데이터에 해당 조사 결과 또는 엔터티가 없으면 동작 그래프에 해당 데이터가 포함되지 않습니다.
- 조사 결과 또는 엔터티가 정확한 리전에서 나온 것입니까? 각 동작 그래프는 리전별로 다릅니다. 동작 그래프에는 다른 리전의 데이터가 포함되지 않습니다.

Splunk에 조사 결과용 Detective URL 추가

Splunk Trumpet 프로젝트를 사용하면 AWS 서비스에서 Splunk로 데이터를 전송할 수 있습니다.

Amazon GuardDuty 조사 결과용 Detective URL을 생성하도록 Trumpet 프로젝트를 구성할 수 있습니다. 그런 다음 이러한 URL을 사용하여 Splunk에서 해당 Detective 조사 결과 프로필로 직접 피벗할 수 있습니다.

Trumpet 프로젝트는 GitHub의 https://github.com/splunk/splunk-aws-project-trumpet에서 이용할 수 있습니다.

Trumpet 프로젝트의 구성 페이지에 있는 AWS CloudWatch Events에서 Detective GuardDuty URL을 선택합니다.

프로필 패널에서 다른 콘솔로 피벗

EC2 인스턴스, IAM 사용자, IAM 역할의 경우 세부 정보 프로필 패널에서 해당 콘솔로 직접 이동할 수 있습니다. 콘솔에서 사용할 수 있는 정보는 보안 조사를 위한 추가 입력을 제공할 수 있습니다.

EC2 인스턴스 세부 정보 프로필 패널에서 EC2 인스턴스 식별자는 Amazon EC2 콘솔에 연결되어 있습니다.

사용자 세부 정보 프로필 패널에서 사용자 이름은 IAM 콘솔에 연결되어 있습니다.

역할 세부 정보 프로필 패널에서 역할 이름은 IAM 콘솔에 연결되어 있습니다.

프로필 패널에서 다른 엔터티 프로필로 피벗

프로필 패널에 다른 엔터티의 식별자가 포함된 경우 이는 일반적으로 해당 엔터티 프로필로 연결되는 링크입니다. EC2 인스턴스의 Amazon EC2 및 IAM 콘솔, IAM 사용자, IAM 역할 프로필에 대한 링크는 예외입니다. the section called “다른 콘솔로 피벗”을(를) 참조하세요.

예를 들어 IP 주소 목록에서 특정 IP 주소의 프로필을 표시할 수 있습니다. 이를 통해 조사를 완료하는 데 도움이 되는 다른 정보가 있는지 확인할 수 있습니다.

프로필 패널에서 활동 세부 정보 탐색

조사 중에 엔터티의 활동 패턴을 더 자세히 조사해 보는 것이 좋습니다.

다음 프로필 패널에는 활동 세부 정보의 요약을 표시할 수 있습니다.

- 전체 API 직접 호출량(사용자 에이전트 프로필의 프로필 패널 제외)
- 새로 관찰된 지리적 위치
- 전체 VPC 흐름 볼륨
- 단일 IP 주소와 관련된 조사 결과의 경우, 조사 결과 IP 주소로 들어오고 나가는 VPC 흐름 볼륨
- 컨테이너 세부 정보:
- 클러스터의 VPC 흐름 볼륨
- 전체 Kubernetes API 활동

활동 세부 정보는 다음과 같은 유형의 질문에 답할 수 있습니다.

- 어떤 IP 주소가 사용되었습니까?
- 해당 IP 주소는 어디에 있었습니까?
- 각 IP 주소는 어떤 API 직접 호출을 했고, 어떤 서비스에서 해당 호출을 했습니까?
- 호출할 때 사용된 보안 주체 또는 액세스 키 식별자(AKID)는 무엇입니까?
- 호출하는 데 사용된 리소스는 무엇입니까?
- 몇 번 호출했습니까? 성공 횟수와 실패 횟수는 얼마입니까?
- 각 IP 주소로 또는 각 IP 주소에서 전송된 VPC 흐름 로그 데이터의 양은 얼마입니까?
- 특정 클러스터, 이미지 또는 포드에서 어떤 컨테이너가 활성 상태였습니까?

주제

전체 API 직접 호출량에 대한 활동 세부 정보

전체 API 직접 호출량의 활동 세부 정보에는 선택한 시간 범위 동안 실행된 API 직접 호출이 표시됩니다.

단일 시간 간격의 활동 세부 정보를 표시하려면 차트에서 시간 간격을 선택합니다.

현재 범위 시간에 대한 활동 세부 정보를 표시하려면 범위 시간 세부 정보 표시를 선택합니다.

참고로 Detective는 2021년 7월 14일부터 API 직접 호출에 대한 서비스 이름을 저장하고 표시하기 시작했습니다. 해당 날짜는 프로필 패널 타임라인에 강조 표시되어 있습니다. 해당 날짜 이전에 발생한 활동의 경우 서비스 이름은 알 수 없는 서비스로 표시됩니다.

활동 세부 정보의 내용(사용자, 역할, 계정, 역할 세션, EC2 인스턴스, S3 버킷)

IAM 사용자, IAM 역할, 계정, 역할 세션, EC2 인스턴스 및 S3 버킷의 경우 활동 세부 정보에는 다음 정보가 포함됩니다.

- 각 탭은 선택한 시간 범위 동안 실행된 API 직접 호출 세트에 대한 정보를 제공합니다.

  S3 버킷의 경우 정보는 S3 버킷에 대한 API 직접 호출을 반영합니다.

API 직접 호출은 호출한 서비스별로 그룹화됩니다. S3 버킷의 경우 서비스는 항상 Amazon S3입니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.

- 각 항목에 대한 활동 세부 정보에는 성공한 호출 및 실패한 호출 수가 표시됩니다. 관찰된 IP 주소 탭에는 각 IP 주소의 위치도 표시됩니다.
- 각 항목에는 호출한 대상에 대한 정보가 표시됩니다. 계정의 경우 활동 세부 정보는 사용자 또는 역할을 식별합니다. 역할의 경우, 활동 세부 정보는 역할 세션을 식별합니다. 사용자 및 역할 세션의 경우 활동 세부 정보는 액세스 키 식별자(AKID)를 식별합니다.

  2021년 7월 14일부터 계정 프로필의 경우 활동 세부 정보에는 AKID 대신 사용자 또는 역할이 표시됩니다. 역할 프로필의 경우 활동 세부 정보에는 AKID 대신 역할 세션이 표시됩니다. 2021년 7월 14일 이전에 발생한 활동의 경우 호출자는 알 수 없는 리소스로 표시됩니다.

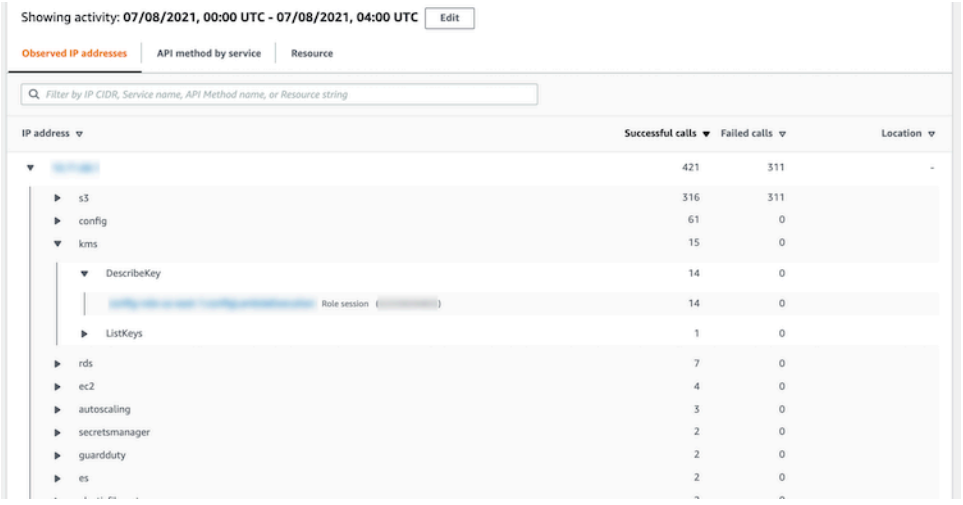
활동 세부 정보에는 다음과 같은 탭이 있습니다.

관찰된 IP 주소

처음에는 API 직접 호출을 실행하는 데 사용된 IP 주소 목록을 표시합니다.

각 IP 주소를 확장하여 해당 IP 주소에서 실행된 API 직접 호출 목록을 표시할 수 있습니다. API 직접 호출은 호출한 서비스별로 그룹화됩니다. S3 버킷의 경우 서비스는 항상 Amazon S3입니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.

그런 다음 각 API 직접 호출을 확장하여 해당 IP 주소의 호출자 목록을 표시할 수 있습니다. 프로필에 따라 호출자는 사용자, 역할, 역할 세션 또는 AKID일 수 있습니다.

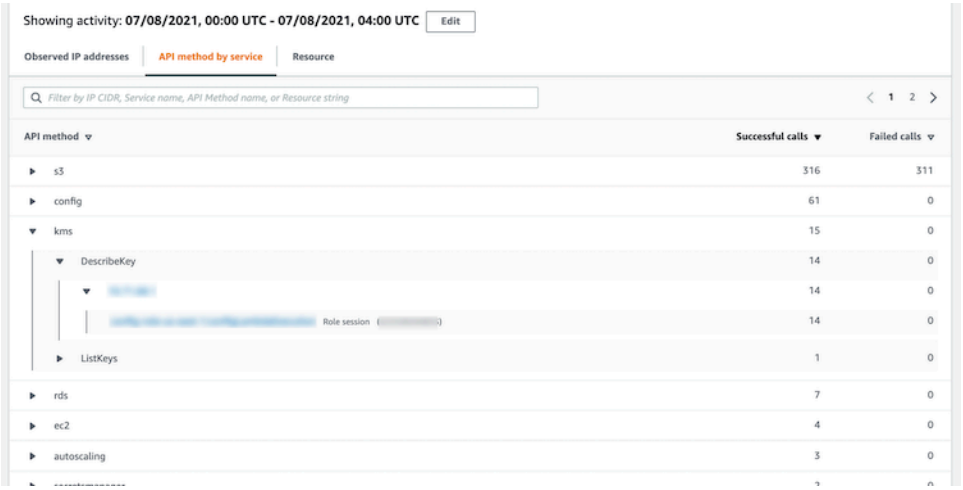


서비스별 API 메서드

처음에는 실행된 API 직접 호출 목록을 표시합니다. API 직접 호출은 호출을 실행한 서비스별로 그룹화됩니다. S3 버킷의 경우 서비스는 항상 Amazon S3입니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.

각 API 메서드를 확장하여 호출이 실행된 IP 주소 목록을 표시할 수 있습니다.

그런 다음 각 IP 주소를 확장하여 해당 IP 주소에서 API 직접 호출을 실행한 AKID 목록을 표시할 수 있습니다.

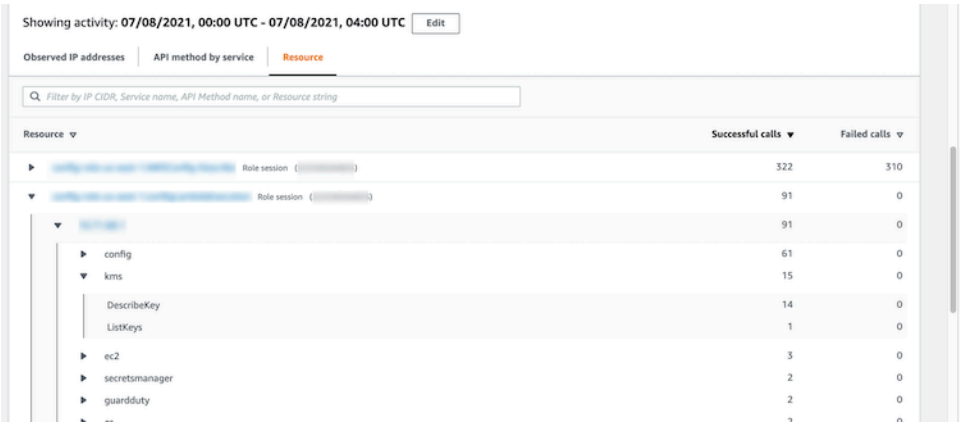


리소스 또는 액세스 키 ID

처음에는 API 직접 호출을 실행하는 데 사용된 사용자, 역할, 역할 세션 또는 AKID 목록을 표시합니다.

각 호출자를 확장하여 API 직접 호출을 실행한 호출자의 IP 주소 목록을 표시할 수 있습니다.

각 IP 주소를 확장하여 해당 IP 주소에서 실행된 API 직접 호출 목록을 표시할 수 있습니다. API 직접 호출은 호출을 실행한 서비스별로 그룹화됩니다. S3 버킷의 경우 서비스는 항상 Amazon S3입니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.



활동 세부 정보 내용(IP 주소)

IP 주소의 경우 활동 세부 정보에는 다음 정보가 포함됩니다.

- 각 탭은 선택한 시간 범위 동안 실행된 API 직접 호출 세트에 대한 정보를 제공합니다. API 직접 호출은 호출을 실행한 서비스별로 그룹화됩니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.
- 각 항목에 대한 활동 세부 정보에는 성공한 호출 및 실패한 호출 수가 표시됩니다.

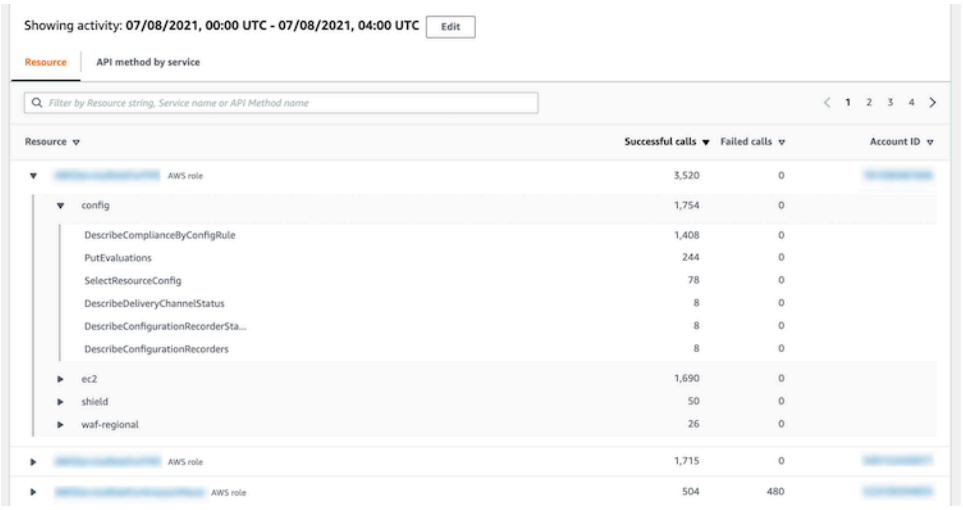
활동 세부 정보에는 다음과 같은 탭이 있습니다.

Resource

처음에는 IP 주소에서 API 직접 호출을 실행한 리소스 목록을 표시합니다.

각 리소스의 목록에는 리소스 이름, 유형 및 AWS 계정이 포함됩니다.

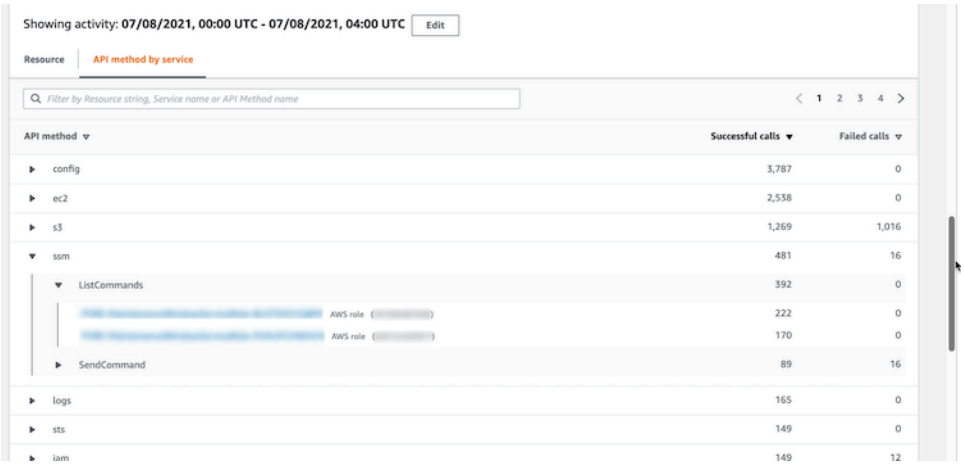
각 리소스를 확장하여 해당 리소스가 IP 주소에서 실행한 API 직접 호출 목록을 표시할 수 있습니다. API 직접 호출은 호출을 실행한 서비스별로 그룹화됩니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.



서비스별 API 메서드

처음에는 실행된 API 직접 호출 목록을 표시합니다. API 직접 호출은 호출을 실행한 서비스별로 그룹화됩니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.

각 API 직접 호출을 확장하여 선택한 기간 동안 IP 주소에서 API 직접 호출을 실행한 리소스 목록을 표시할 수 있습니다.



활동 세부 정보 정렬

목록 열을 기준으로 활동 세부 정보를 정렬할 수 있습니다.

첫 번째 열을 사용하여 정렬하면 최상위 목록만 정렬됩니다. 하위 수준 목록은 항상 성공한 API 직접 호출 수를 기준으로 정렬됩니다.

활동 세부 정보 필터링

필터링 옵션을 사용하여 활동 세부 정보에 표시된 활동의 특정 서브넷 또는 측면에 초점을 맞출 수 있습니다.

모든 탭에서 첫 번째 열의 값을 기준으로 목록을 필터링할 수 있습니다.

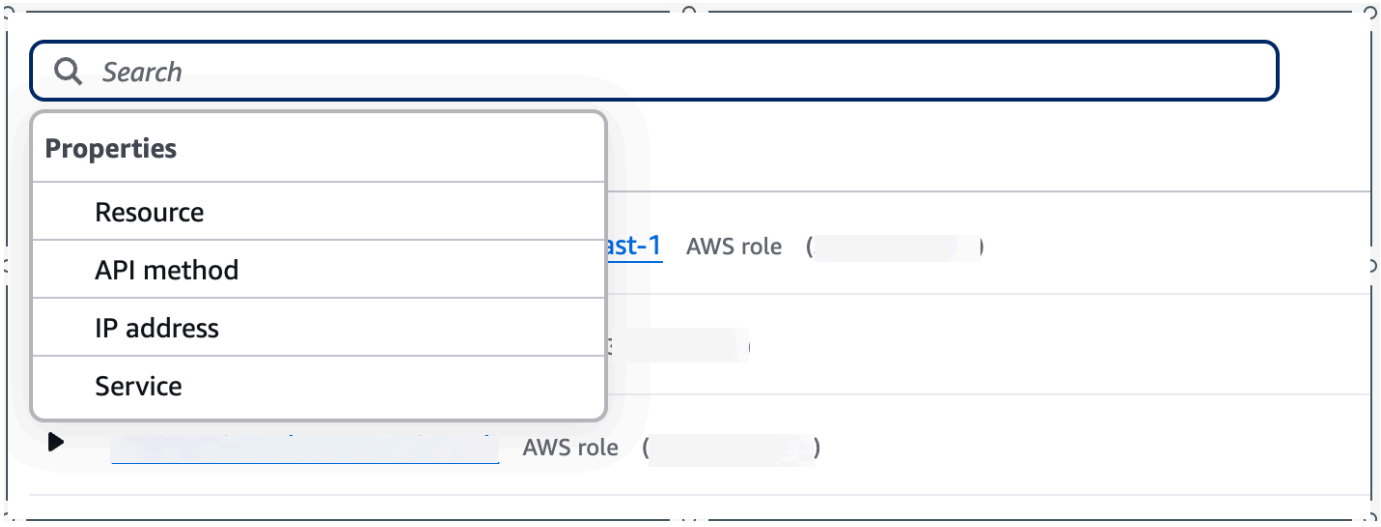
필터 추가

1. 필터 상자를 선택합니다.
2. 속성에서 필터링에 사용할 속성을 선택합니다.
3. 필터링에 사용할 값을 입력합니다. 필터는 부분 값을 지원합니다. 예를 들어 API 메서드별로 필터링할 때 **`Instance`** 기준으로 필터링하면 이름에 `Instance`가 있는 모든 API 작업이 결과에 포함됩니다. 따라서 `ListInstanceAssociations` 및 `UpdateInstanceInformation` 모두 일치합니다.

   서비스 이름, API 메서드, IP 주소의 경우 값을 지정하거나 내장된 필터를 선택할 수 있습니다.

   일반 API 하위 문자열의 경우 작업 유형을 나타내는 하위 문자열(예: `List`, `Create`, `Delete`)을 선택합니다. 각 API 메서드 이름은 작업 유형으로 시작합니다.

   CIDR 패턴의 경우 퍼블릭 IP 주소, 프라이빗 IP 주소 또는 특정 CIDR 패턴과 일치하는 IP 주소만 포함하도록 선택할 수 있습니다.
4. 부울 옵션 *`###`* 또는 *`###`*: 포함 또는 !: 포함하지 않음, *`API #`*서드 또는 *`IP ##`* = 같음 또는 !: 필터 설정과 같지 않음을 선택합니다.



필터를 제거하려면 태그의 오른쪽 상단에 있는 x 아이콘을 선택합니다.

모든 필터를 지우려면 필터 지우기를 선택합니다.

활동 세부 정보의 시간 범위 선택

활동 세부 정보를 처음 표시할 때 시간 범위는 범위 시간 또는 선택한 시간 간격입니다. 활동 세부 정보의 시간 범위를 변경할 수 있습니다.

활동 세부 정보의 시간 범위 변경

1. 편집을 선택합니다.
2. 시간 편집 창에서 사용할 시작 및 종료 시간을 선택합니다.

   기간을 프로필의 기본 범위 시간으로 설정하려면 기본 범위 시간으로 설정을 선택합니다.
3. 기간 업데이트를 선택합니다.

활동 세부 정보의 시간 범위는 프로필 패널 차트에 강조 표시됩니다.

원시 로그 쿼리

Amazon Detective는 Security Lake와 통합되어 Security Lake에 저장된 원시 로그 데이터를 쿼리하고 검색할 수 있습니다. 이 통합에 대한 자세한 내용은 Security Lake와 Detective 통합 단원을 참조하세요.

이 통합을 사용하면 Security Lake에서 기본적으로 지원하는 다음 소스에서 로그와 이벤트를 수집하고 쿼리할 수 있습니다.

- AWS CloudTrail 관리 이벤트 버전 1.0 이상
- Amazon Virtual Private Cloud(Amazon VPC) 흐름 로그 버전 1.0 이상
- Amazon Elastic Kubernetes Service(Amazon EKS) 감사 로그 버전 2.0

> **Note**
>
> Detective에서 원시 데이터 로그를 쿼리하는 데 대한 추가 비용은 없습니다. Amazon Athena를 포함한 다른 AWS 서비스에 대한 사용 요금은 여전히 게시된 요금으로 적용됩니다.

원시 로그를 쿼리하려면

1. 범위 시간에 대한 세부 정보 표시를 선택합니다.
2. 여기에서 원시 로그 쿼리를 시작할 수 있습니다.
3. 원시 로그 미리 보기 테이블을 통해 Security Lake에서 데이터를 쿼리하여 검색한 로그 및 이벤트를 볼 수 있습니다. 원시 이벤트 로그에 대한 자세한 내용은 Amazon Athena에 표시된 데이터를 참조하세요.

   원시 로그 쿼리 테이블에서 쿼리 요청을 취소하고, Amazon Athena에서 결과를 확인하고, 결과를 쉼표로 구분된 값(.csv) 파일로 다운로드할 수 있습니다.

Detective에 로그가 표시되지만 쿼리 결과가 반환되지 않는 경우 다음과 같은 이유 때문일 수 있습니다.

- 원시 로그는 Security Lake 로그 테이블에 표시되기 전에 Detective에 제공될 수 있습니다. 나중에 다시 시도해 주세요.
- Security Lake에서 로그가 누락되었을 수 있습니다. 오랜 시간 기다린 경우 Security Lake에서 로그가 누락된 것으로 표시됩니다. Security Lake 관리자에게 문의하여 이 문제를 해결하세요.

지리적 위치에 대한 활동 세부 정보

새로 관찰된 지리적 위치의 활동 세부 정보에는 범위 기간 동안 지리적 위치에서 실행된 API 직접 호출이 표시됩니다. API 직접 호출에는 지리적 위치에서 실행된 모든 호출이 포함됩니다. 이는 조사 결과 또는 프로필 엔터티를 사용한 호출에만 국한되지 않습니다. S3 버킷의 경우 활동 호출은 S3 버킷에 대한 API 직접 호출입니다.

Detective는 MaxMind GeoIP 데이터베이스를 사용하여 요청 위치를 결정합니다. MaxMind는 국가 수준에서 매우 높은 데이터 정확도를 보고하지만, 정확도는 국가 및 IP 유형과 같은 요인에 따라 다릅니다. MaxMind에 대한 자세한 내용은 MaxMind IP 지리적 위치를 참조하세요. GeoIP 데이터가 잘못되었다고 생각되면 Maxmind(MaxMind Correct GeoIP2 Data)에 정정 요청을 제출할 수 있습니다.

API 직접 호출은 호출을 실행한 서비스별로 그룹화됩니다. S3 버킷의 경우 서비스는 항상 Amazon S3입니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.

활동 세부 정보를 표시하려면 다음 중 하나를 수행합니다.

- 맵에서 지리적 위치를 선택합니다.
- 목록에서 지리적 위치의 세부 정보를 선택합니다.

활동 세부 정보가 지리적 위치 목록을 대체합니다. 지리적 위치 목록으로 돌아가려면 모든 결과로 돌아가기를 선택합니다.

참고로 Detective는 2021년 7월 14일부터 API 직접 호출에 대한 서비스 이름을 저장하고 표시하기 시작했습니다. 해당 날짜 이전에 발생한 활동의 경우 서비스 이름은 알 수 없는 서비스로 표시됩니다.

활동 세부 정보 내용

각 탭은 범위 시간 동안 지리적 위치에서 실행된 모든 API 직접 호출에 대한 정보를 제공합니다.

각 IP 주소, 리소스, API 메서드의 경우 목록에는 성공한 API 직접 호출과 실패한 API 직접 호출 수가 표시됩니다.

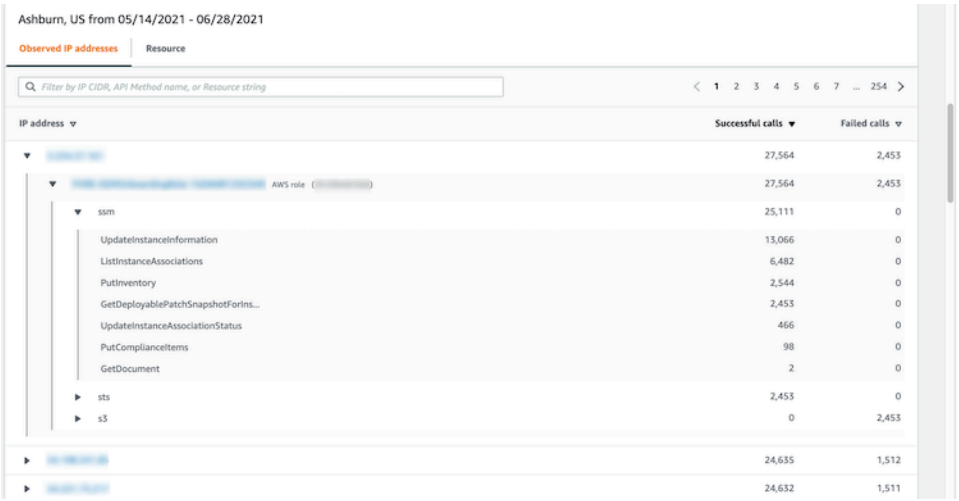
활동 세부 정보에는 다음과 같은 탭이 있습니다.

관찰된 IP 주소

처음에는 선택한 지리적 위치에서 API 직접 호출을 실행하는 데 사용된 IP 주소 목록을 표시합니다.

각 IP 주소를 확장하여 해당 IP 주소에서 API 직접 호출을 실행한 리소스를 표시할 수 있습니다. 목록에는 리소스 이름이 표시됩니다. 보안 주체 ID를 보려면 이름 위에 마우스를 갖다 댑니다.

그런 다음 각 리소스를 확장하여 해당 리소스가 해당 IP 주소에서 실행한 특정 API 직접 호출을 표시할 수 있습니다. API 직접 호출은 호출을 실행한 서비스별로 그룹화됩니다. S3 버킷의 경우 서비스는 항상 Amazon S3입니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.

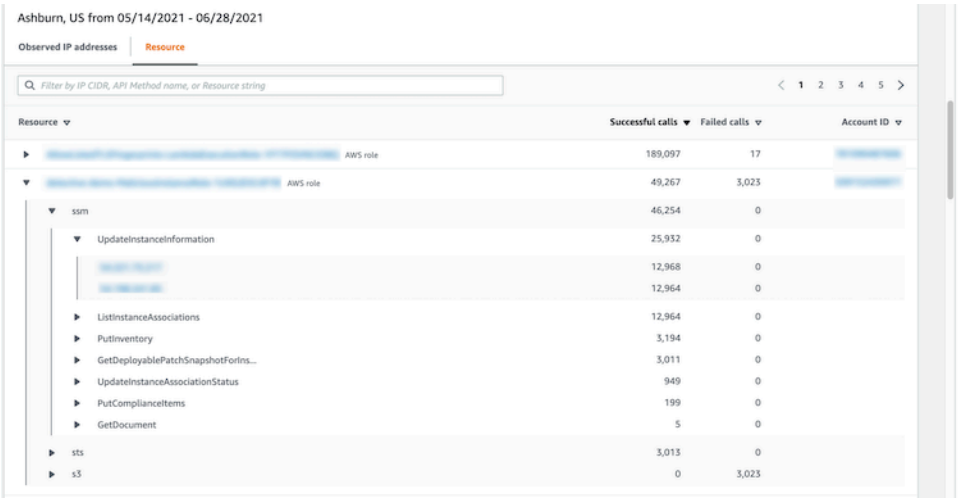


리소스

처음에는 선택한 지리적 위치에서 API 직접 호출을 실행한 리소스 목록이 표시됩니다. 목록에는 리소스 이름이 표시됩니다. 보안 주체 ID를 확인하려면 이름에서 일시 정지합니다. 각 리소스의 경우 리소스 탭에는 AWS 계정와 관련된 리소스도 표시됩니다.

각 사용자 또는 역할을 확장하여 해당 리소스에서 실행한 API 직접 호출 목록을 표시할 수 있습니다. API 직접 호출은 호출을 실행한 서비스별로 그룹화됩니다. S3 버킷의 경우 서비스는 항상 Amazon S3입니다. Detective에서 호출한 서비스를 확인할 수 없는 경우 해당 호출은 알 수 없는 서비스 아래에 나열됩니다.

그런 다음 각 API 직접 호출을 확장하여 리소스가 API 직접 호출을 실행한 IP 주소 목록을 표시할 수 있습니다.



활동 세부 정보 정렬

목록 열을 기준으로 활동 세부 정보를 정렬할 수 있습니다.

첫 번째 열을 사용하여 정렬하면 최상위 목록만 정렬됩니다. 하위 수준 목록은 항상 성공한 API 직접 호출 수를 기준으로 정렬됩니다.

활동 세부 정보 필터링

필터링 옵션을 사용하여 활동 세부 정보에 표시된 활동의 특정 서브넷 또는 측면에 초점을 맞출 수 있습니다.

모든 탭에서 첫 번째 열의 값을 기준으로 목록을 필터링할 수 있습니다.

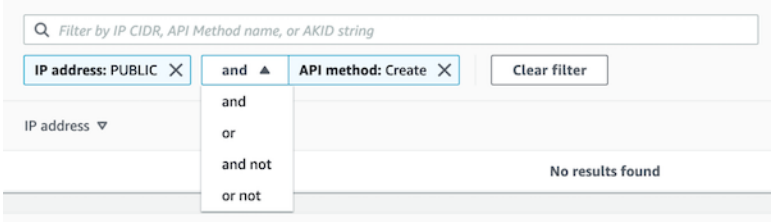
필터 추가

1. 필터 상자를 선택합니다.
2. 속성에서 필터링에 사용할 속성을 선택합니다.
3. 필터링에 사용할 값을 입력합니다. 필터는 부분 값을 지원합니다. 예를 들어 API 메서드별로 필터링할 때 **`Instance`** 기준으로 필터링하면 이름에 `Instance`가 있는 모든 API 작업이 결과에 포함됩니다. 따라서 `ListInstanceAssociations` 및 `UpdateInstanceInformation` 모두 일치합니다.

   서비스 이름, API 메서드, IP 주소의 경우 값을 지정하거나 내장된 필터를 선택할 수 있습니다.

   일반 API 하위 문자열의 경우 작업 유형을 나타내는 하위 문자열(예: `List`, `Create`, `Delete`)을 선택합니다. 각 API 메서드 이름은 작업 유형으로 시작합니다.

   CIDR 패턴의 경우 퍼블릭 IP 주소, 프라이빗 IP 주소 또는 특정 CIDR 패턴과 일치하는 IP 주소만 포함하도록 선택할 수 있습니다.
4. 필터가 여러 개 있는 경우 부울 옵션을 선택하여 해당 필터의 연결 방식을 설정합니다.



5. 필터를 제거하려면 태그의 오른쪽 상단에 있는 x 아이콘을 선택합니다.
6. 모든 필터를 지우려면 필터 지우기를 선택합니다.

전체 VPC 흐름량에 대한 활동 세부 정보

EC2 인스턴스의 경우 전체 VPC 흐름량의 활동 세부 정보에는 선택한 시간 범위 동안의 EC2 인스턴스와 IP 주소 간의 상호 작용이 표시됩니다.

Kubernetes 포드의 경우 전체 VPC 흐름량은 모든 대상 IP 주소에 대해 Kubernetes 포드에 할당된 IP 주소로 들어오고 나가는 전체 바이트 볼륨을 표시합니다. Kubernetes 포드의 IP 주소는 `hostNetwork:true`의 경우 고유하지 않습니다. 이 경우 패널에는 동일한 구성을 가진 다른 포드와 이를 호스팅하는 노드에 대한 트래픽이 표시됩니다.

IP 주소의 경우 전체 VPC 흐름량의 활동 세부 정보에는 선택한 시간 범위 동안의 IP 주소 및 EC2 인스턴스 간의 상호 작용이 표시됩니다.

단일 시간 간격의 활동 세부 정보를 표시하려면 차트에서 시간 간격을 선택합니다.

현재 범위 시간에 대한 활동 세부 정보를 표시하려면 범위 시간 세부 정보 표시를 선택합니다.

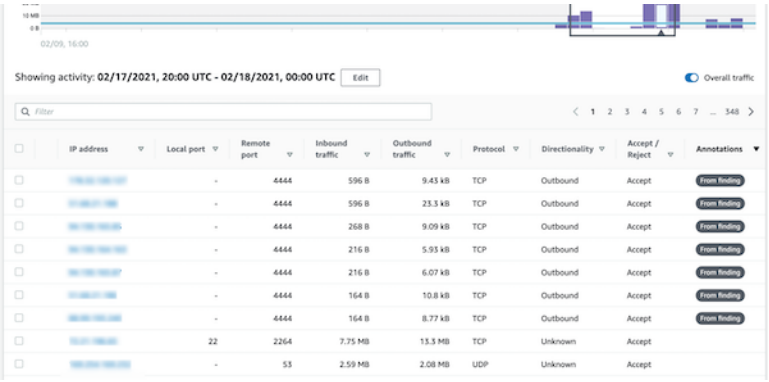
활동 세부 정보 내용

내용은 선택한 시간 범위 동안의 활동을 반영합니다.

EC2 인스턴스의 경우 활동 세부 정보에는 IP 주소, 로컬 포트, 원격 포트, 프로토콜 및 방향의 고유한 각 조합에 대한 항목이 포함됩니다.

IP 주소의 경우 활동 세부 정보에는 EC2 인스턴스, 로컬 포트, 원격 포트, 프로토콜 및 방향의 고유한 각 조합에 대한 항목이 포함됩니다.

각 항목에는 인바운드 트래픽의 양, 아웃바운드 트래픽의 양, 액세스 요청의 수락 또는 거부 여부가 표시됩니다. 조사 결과 프로필에서 주석 열에는 IP 주소가 현재 조사 결과와 관련이 있는 경우가 표시됩니다.



활동 세부 정보 정렬

목록 열을 기준으로 활동 세부 정보를 정렬할 수 있습니다.

기본적으로 활동 세부 정보는 먼저 주석을 기준으로 정렬된 다음 인바운드 트래픽을 기준으로 정렬됩니다.

활동 세부 정보 필터링

특정 활동에 집중하기 위해 다음 값을 기준으로 활동 세부 정보를 필터링할 수 있습니다.

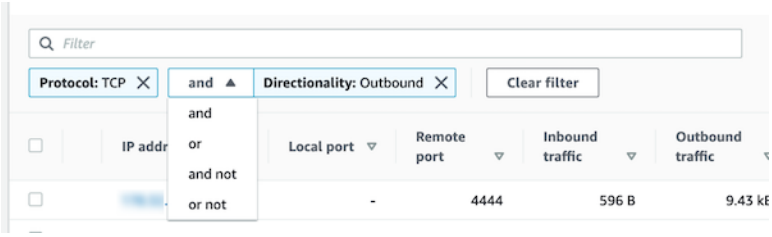
- IP 주소 또는 EC2 인스턴스
- 로컬 또는 원격 포트
- Direction
- 프로토콜
- 요청 수락 또는 거부 여부

필터 추가 및 제거

1. 필터 상자를 선택합니다.
2. 속성에서 필터링에 사용할 속성을 선택합니다.
3. 필터링에 사용할 값을 입력합니다. 필터는 부분 값을 지원합니다.

   IP 주소를 기준으로 필터링하려면 값을 지정하거나 내장 필터를 선택할 수 있습니다.

   CIDR 패턴의 경우 퍼블릭 IP 주소, 프라이빗 IP 주소 또는 특정 CIDR 패턴과 일치하는 IP 주소만 포함하도록 선택할 수 있습니다.
4. 필터가 여러 개 있는 경우 부울 옵션을 선택하여 해당 필터의 연결 방식을 설정합니다.



5. 필터를 제거하려면 태그의 오른쪽 상단에 있는 x 아이콘을 선택합니다.
6. 모든 필터를 지우려면 필터 지우기를 선택합니다.

활동 세부 정보의 시간 범위 선택

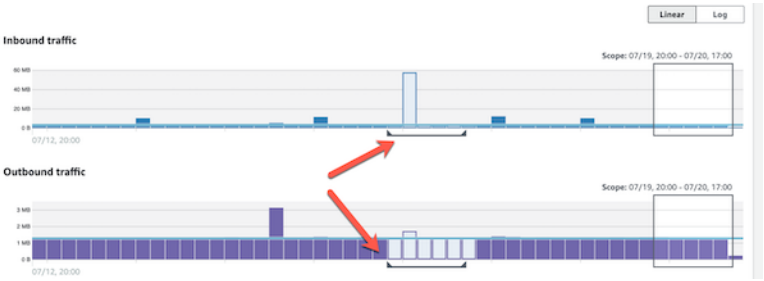
활동 세부 정보를 처음 표시할 때 시간 범위는 범위 시간 또는 선택한 시간 간격입니다. 활동 세부 정보의 시간 범위를 변경할 수 있습니다.

활동 세부 정보의 시간 범위 변경

1. 편집을 선택합니다.
2. 시간 편집 창에서 사용할 시작 및 종료 시간을 선택합니다.

   기간을 프로필의 기본 범위 시간으로 설정하려면 기본 범위 시간으로 설정을 선택합니다.
3. 기간 업데이트를 선택합니다.

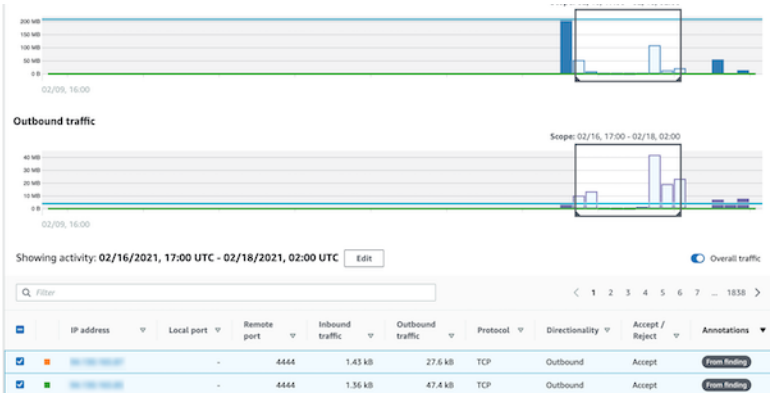
활동 세부 정보의 시간 범위는 프로필 패널 차트에 강조 표시됩니다.



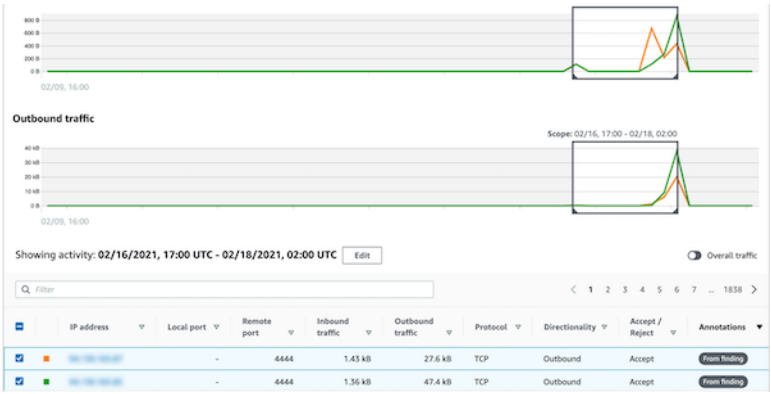
선택한 행의 트래픽 볼륨 표시

관심 있는 행을 식별하면 해당 행의 시간 경과에 따른 트래픽 양을 기본 차트에 표시할 수 있습니다.

차트에 추가할 각 행에 대해 확인란을 선택합니다. 선택한 각 행의 볼륨은 인바운드 또는 아웃바운드 차트에 선으로 표시됩니다.



선택한 항목의 트래픽 볼륨에 집중하기 위해 전체 볼륨을 숨길 수 있습니다. 전체 트래픽을 표시하거나 숨기려면 전체 트래픽픽을 전환합니다.



EKS 클러스터의 VPC 흐름 트래픽 표시

Detective는 Amazon Virtual Private Cloud(VPC) 흐름 로그를 파악할 수 있으며, 이 흐름 로그는 Amazon Elastic Kubernetes Service(Amazon EKS)(Amazon EKS) 클러스터를 통과하는 트래픽을 나타냅니다. Kubernetes 리소스의 경우 VPC 흐름 로그의 내용은 EKS 클러스터에 배포된 Container Network Interface(CNI)에 따라 달라집니다.

기본 구성을 사용한 EKS 클러스터는 Amazon VPC CNI 플러그 인을 사용합니다. 자세한 내용은 Amazon EKS 사용 설명서의 VPC CNI 관리를 참조하세요. Amazon VPC CNI 플러그인은 포드의 IP 주소로 내부 트래픽을 전송하고 외부 통신을 위해 소스 IP 주소를 노드의 IP 주소로 변환합니다. Detective는 내부 트래픽을 캡처하고 올바른 포드와 상호 연결할 수 있지만 외부 트래픽에 대해서는 동일한 작업을 수행할 수 없습니다.

Detective에서 포드의 외부 트래픽을 파악할 수 있게 하려면 외부 소스 네트워크 주소 변환(SNAT)을 활성화합니다. SNAT를 활성화하는 데에는 한계와 단점이 있습니다. 자세한 내용은 Amazon EKS 사용 설명서의 포드용 SNAT를 참조하세요.

다른 CNI 플러그인을 사용하는 경우 Detective는 `hostNetwork:true`를 사용하는 포드에 대한 가시성이 제한됩니다. 이러한 포드의 경우 VPC 흐름 패널에는 포드의 IP 주소로 향하는 모든 트래픽이 표시됩니다. 여기에는 호스트 노드 및 `hostNetwork:true` 구성이 있는 노드의 모든 포드로 향하는 트래픽이 포함됩니다.

Detective는 다음 EKS 클러스터 구성에 대해 EKS 포드의 VPC 흐름 패널에 트래픽을 표시합니다.

- Amazon VPC CNI 플러그인이 있는 클러스터에서 `hostNetwork:false` 구성이 있는 모든 포드는 클러스터의 VPC 내부로 트래픽을 전송합니다.
- Amazon VPC CNI 플러그인 및 `AWS_VPC_K8S_CNI_EXTERNALSNAT=true` 구성이 있는 클러스터에서 `hostNetwork:false` 구성이 있는 모든 포드는 클러스터의 VPC 외부로 트래픽을 전송합니다.

- `hostNetwork:true` 구성이 있는 모든 포드. 노드의 트래픽은 `hostNetwork:true` 구성이 있는 다른 포드의 트래픽과 혼합됩니다.

Detective는 다음과 같은 경우 VPC 흐름 패널에 트래픽을 표시하지 않습 니다.

- Amazon VPC CNI 플러그인 및 `AWS_VPC_K8S_CNI_EXTERNALSNAT=false` 구성이 있는 클러스터에서 `hostNetwork:false` 구성이 있는 모든 포드는 클러스터의 VPC 외부로 트래픽을 전송합니다.
- Kubernetes용 Amazon VPC CNI 플러그인이 없는 클러스터에서 `hostNetwork:false` 구성이 있는 모든 포드.
- 동일한 노드에 호스팅된 다른 포드로 트래픽을 전송하는 모든 포드.

공유된 Amazon VPC에 대한 VPC 흐름 트래픽 표시

Detective는 공유 VPC의 Amazon Virtual Private Cloud(VPC) 흐름 로그에 대한 가시성을 제공합니다.

- Detective 멤버 계정에 공유 Amazon VPC가 있고 이 공유 VPC를 사용하는 다른 비 Detective 계정이 있는 경우 Detective는 해당 VPC에서 들어오는 모든 트래픽을 모니터링하고, VPC 내 모든 트래픽 흐름에 대한 시각화를 제공합니다.
- 공유 Amazon VPC 내에 Amazon EC2 인스턴스가 있고 공유 VPC 소유자가 Detective 멤버가 아닌 경우, Detective는 VPC에서 들어오는 트래픽을 모니터링하지 않습니다. VPC 내의 트래픽 흐름을 보려면 Amazon VPC 소유자를 Detective 그래프의 멤버로 추가해야 합니다.

EKS 클러스터와 관련된 전체 Kubernetes API 활동

EKS 클러스터와 관련된 전체 Kubernetes API 활동의 활동 세부 정보에는 선택한 시간 범위 동안 실행된 성공 및 실패한 Kubernetes API 직접 호출 수가 표시됩니다.

단일 시간 간격의 활동 세부 정보를 표시하려면 차트에서 시간 간격을 선택합니다.

현재 범위 시간에 대한 활동 세부 정보를 표시하려면 범위 시간 세부 정보 표시를 선택합니다.

활동 세부 정보 내용(클러스터, 포드, 사용자, 역할, 역할 세션)

클러스터, 포드, 사용자, 역할 또는 역할 세션의 경우 활동 세부 정보에는 다음 정보가 포함됩니다.

- 각 탭은 선택한 시간 범위 동안 실행된 API 직접 호출 세트에 대한 정보를 제공합니다.

클러스터의 경우 API 직접 호출은 클러스터 내에서 발생했습니다.

포드의 경우 API 직접 호출은 포드를 대상으로 했습니다.

사용자, 역할 및 역할 세션의 경우 해당 사용자, 역할 또는 역할 세션으로 인증된 Kubernetes 사용자가 API 직접 호출을 실행했습니다.

- 각 항목에 대한 활동 세부 정보에는 성공, 실패, 무단, 금지된 호출 수가 표시됩니다.
- 이 정보에는 IP 주소, Kubernetes 호출 유형, 호출의 영향을 받은 엔터티, 호출한 객체(서비스 계정 또는 사용자)가 포함됩니다. 활동 세부 정보에서 IP 주소, 객체 및 영향을 받는 엔터티의 프로필로 피벗할 수 있습니다.

활동 세부 정보에는 다음과 같은 탭이 있습니다.

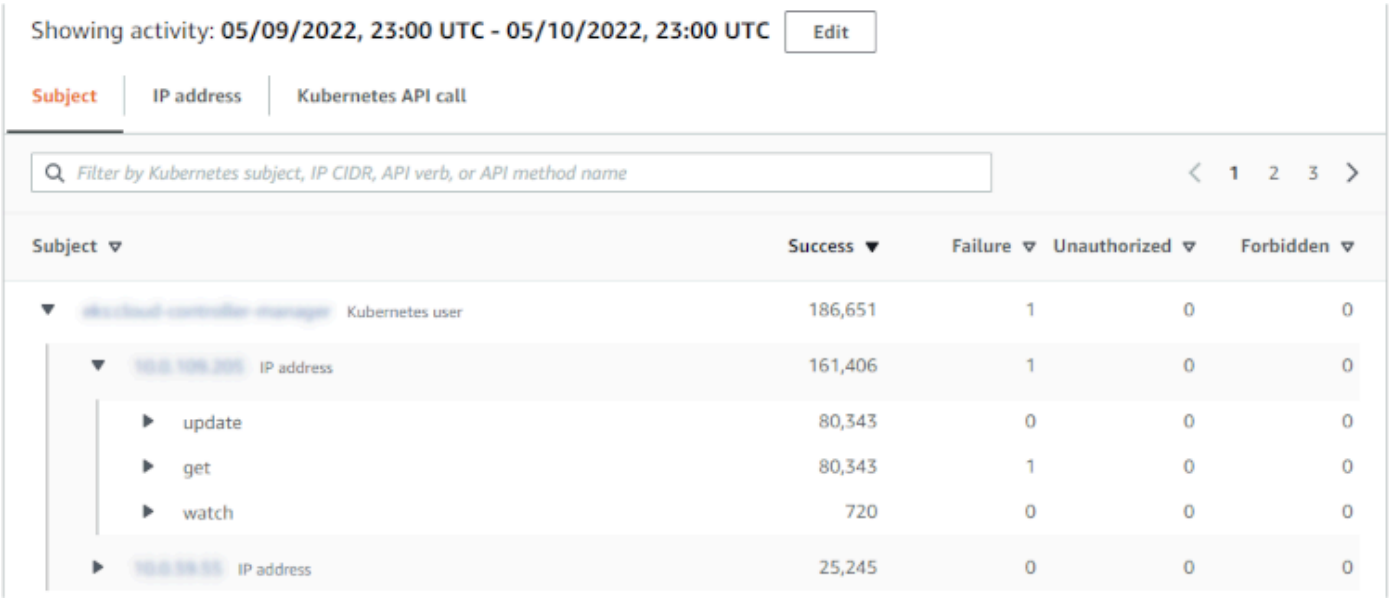
Subject

처음에는 API 직접 호출에 사용된 서비스 계정 및 사용자 목록이 표시됩니다.

각 서비스 계정 및 사용자를 확장하여 계정 또는 사용자가 API 직접 호출을 수행한 IP 주소 목록을 표시할 수 있습니다.

그런 다음 각 IP 주소를 확장하여 해당 계정 또는 사용자가 해당 IP 주소에서 수행한 Kubernetes API 직접 호출을 표시할 수 있습니다.

Kubernetes API 직접 호출을 확장하여 `requestURI` 를 확인하고 수행된 작업을 식별합니다.



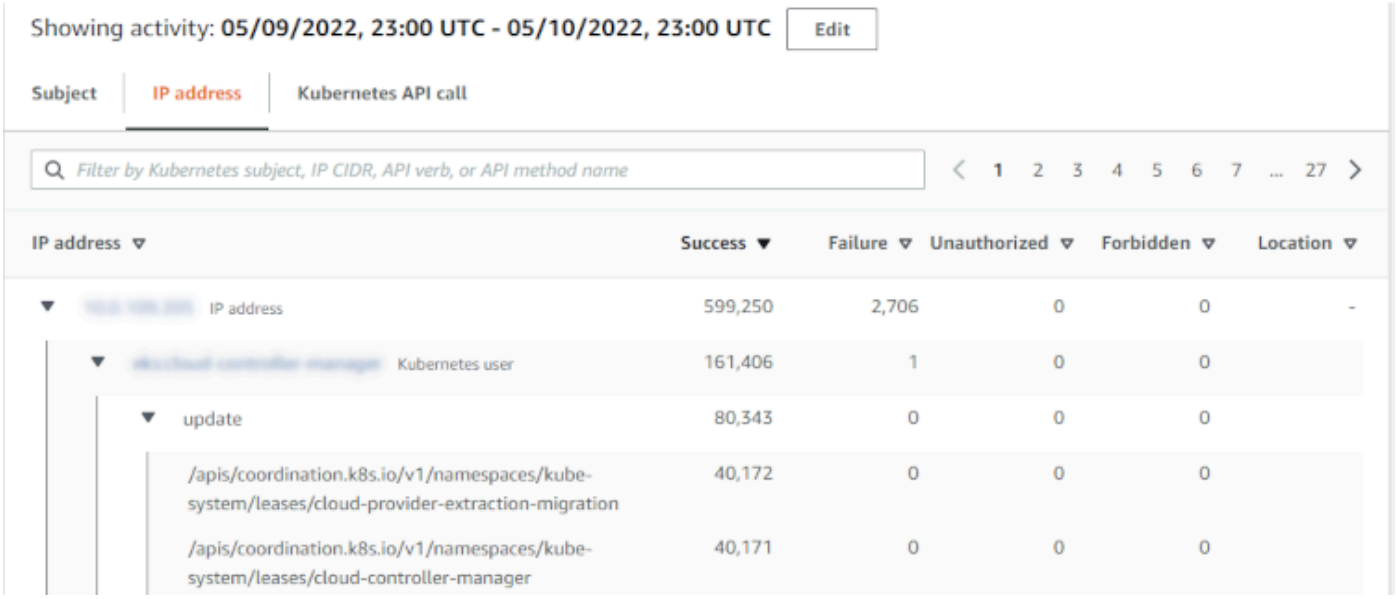
IP 주소

처음에는 API 직접 호출이 이루어진 IP 주소 목록을 표시합니다.

각 호출을 확장하여 호출한 Kubernetes 객체(서비스 계정 및 사용자)의 목록을 표시할 수 있습니다.

그런 다음 각 객체를 확장하여 범위 시간 동안 객체가 만든 API 직접 호출 유형 목록으로 확장할 수 있습니다.

API 직접 호출 유형을 확장하여 requestURI를 확인하고 수행된 작업을 식별합니다.



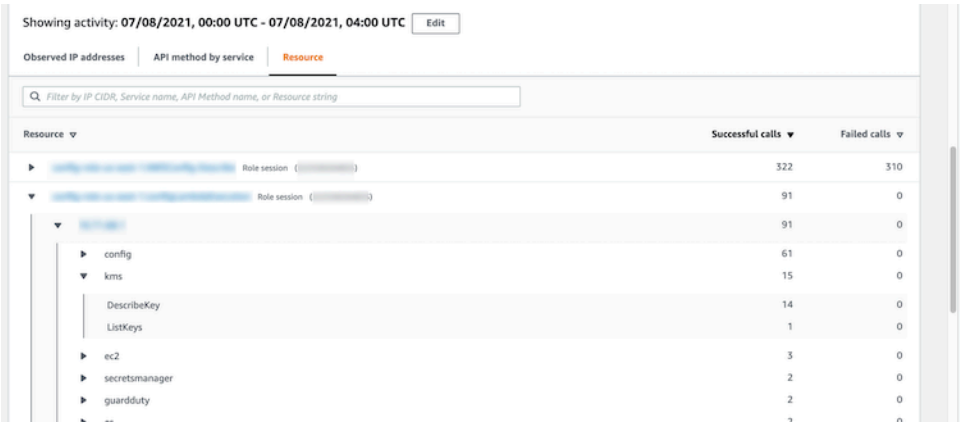
Kubernetes API 직접 호출

처음에는 Kubernetes API 직접 호출 동사 목록을 표시합니다.

각 API 동사를 확장하여 해당 작업과 관련된 requestURI를 표시할 수 있습니다.

그런 다음 각 requestURI를 확장하여 API 직접 호출을 수행한 Kubernetes 객체(서비스 계정 및 사용자)를 볼 수 있습니다.

객체를 확장하여 해당 객체가 API 직접 호출을 수행하는 데 사용한 IP를 확인합니다.



활동 세부 정보 정렬

목록 열을 기준으로 활동 세부 정보를 정렬할 수 있습니다.

첫 번째 열을 사용하여 정렬하면 최상위 목록만 정렬됩니다. 하위 수준 목록은 항상 성공한 API 직접 호출 수를 기준으로 정렬됩니다.

활동 세부 정보 필터링

필터링 옵션을 사용하여 활동 세부 정보에 표시된 활동의 특정 서브넷 또는 측면에 초점을 맞출 수 있습니다.

모든 탭에서 첫 번째 열의 값을 기준으로 목록을 필터링할 수 있습니다.

활동 세부 정보의 시간 범위 선택

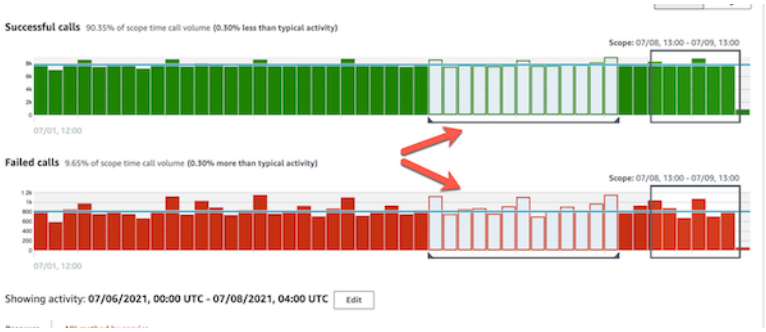
활동 세부 정보를 처음 표시할 때 시간 범위는 범위 시간 또는 선택한 시간 간격입니다. 활동 세부 정보의 시간 범위를 변경할 수 있습니다.

활동 세부 정보의 시간 범위 변경

1. 편집을 선택합니다.
2. 시간 편집 창에서 사용할 시작 및 종료 시간을 선택합니다.

   기간을 프로필의 기본 범위 시간으로 설정하려면 기본 범위 시간으로 설정을 선택합니다.
3. 기간 업데이트를 선택합니다.

활동 세부 정보의 시간 범위는 프로필 패널 차트에 강조 표시됩니다.



조사 중 프로필 패널 지침 사용

각 프로필 패널은 조사를 수행하고 관련 엔터티의 활동을 분석할 때 발생하는 특정 질문에 대한 답변을 제공하도록 설계되었습니다.

각 프로필 패널에 제공된 지침은 이러한 답변을 찾는 데 도움이 됩니다.

프로필 패널 지침은 패널 자체에 대한 한 문장으로 시작됩니다. 이 지침은 패널에 표시된 데이터에 대한 간략한 설명을 제공합니다.

패널에 대한 자세한 지침을 표시하려면 패널 제목에서 추가 정보를 선택합니다. 이 확장 지침은 도움말 창에 표시됩니다.

이 지침에서는 다음과 같은 유형의 정보를 제공할 수 있습니다.

- 패널 내용 개요
- 패널을 사용하여 관련 질문에 답변하는 방법
- 답변을 기반으로 제안된 다음 단계

범위 시간 관리

엔터티 프로필에 표시되는 데이터를 제한하는 데 사용되는 범위 시간을 사용자 지정합니다.

엔터티 프로필에 표시되는 차트, 타임라인 및 기타 데이터는 모두 현재 범위 시간을 기반으로 합니다. 범위 시간은 시간 경과에 따른 엔터티 활동의 요약입니다. 이는 Amazon Detective 콘솔의 각 프로필 오른쪽 상단에 표시됩니다. 해당 차트, 타임라인 및 기타 시각화에 표시되는 데이터는 범위 시간을 기반으로 합니다. 일부 프로필 패널의 경우 범위 시간 전후에 컨텍스트를 제공하기 위해 추가 시간이 추가됩니다. Detective에서는 기본적으로 모든 타임스탬프가 UTC로 표시됩니다. 타임스탬프 기본 설정을 변경하여 현지 시간대를 선택할 수 있습니다. 타임스탬프 기본 설정을 업데이트하려면 the section called “타임스탬프 형식 설정” 섹션을 참조하세요.

Detective 분석은 범위 시간을 사용하여 비정상적인 활동을 확인합니다. 분석 프로세스는 범위 시간 동안의 활동을 가져온 다음, 범위 시간 전 45일 동안의 활동과 비교합니다. 또한 이 45일의 기간을 사용하여 활동 기준선을 생성합니다.

조사 결과 개요에서 범위 시간은 조사 결과가 처음으로 관찰된 시간과 마지막으로 관찰된 시간을 반영합니다. 조사 결과 개요에 대한 자세한 내용은 the section called “조사 결과 개요” 섹션을 참조하세요.

조사를 진행하면서 범위 시간을 조정할 수 있습니다. 예를 들어, 원래 분석이 하루의 활동을 기반으로 한 것이라면 이를 일주일 또는 한 달로 확장하는 것이 좋습니다. 기간을 확장하면 활동이 정상 패턴에 맞는지 아니면 비정상적인지 더 잘 파악할 수 있습니다.

또한 현재 엔터티에 대한 관련 조사 결과와 일치하도록 범위 시간을 설정할 수 있습니다.

범위 시간을 변경하면 Detective는 분석을 반복하고 새 범위 시간을 기준으로 표시된 데이터를 업데이트합니다.

범위 시간은 1시간 이상이며 1년을 초과할 수 없습니다. 시작 시간과 종료 시간은 1시간이어야 합니다.

특정 시작 및 종료 날짜 및 시간 설정

Detective 콘솔에서 범위 시간 시작 및 종료 날짜를 설정할 수 있습니다.

새 범위 시간의 특정 시작 및 종료 시간 설정

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. 엔터티 프로필에서 범위 시간을 선택합니다.
3. 범위 시간 편집 패널의 시작에서 범위 시간의 새 시작 날짜 및 시간을 선택합니다. 새 시작 시간에는 시간만 선택합니다.
4. 종료에서 범위 시간의 새 종료 날짜 및 시간을 선택합니다. 새 종료 시간에는 시간만 선택합니다. 종료 시간은 시작 시간에서 최소 1시간 내여야 합니다.
5. 편집을 마친 경우 변경 내용을 저장하고 표시된 데이터를 업데이트하려면 범위 시간 업데이트를 선택합니다.

범위 시간의 시간 길이 편집

범위 시간 길이를 설정하면 Detective는 범위 시간을 현재 시간으로부터 해당 시간으로 설정합니다.

범위 시간의 시간 길이 편집

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.

2. 엔터티 프로필에서 범위 시간을 선택합니다.
3. 범위 시간 편집 패널의 기록 옆에서 범위 시간의 길이를 선택합니다.

   시간 범위를 지정하면 시작 및 종료 설정이 업데이트됩니다.
4. 편집을 마친 경우 변경 내용을 저장하고 표시된 데이터를 업데이트하려면 범위 시간 업데이트를 선택합니다.

범위 시간을 조사 결과 기간으로 설정

각 조사 결과에는 해당 조사 결과가 처음 관찰된 시간과 마지막으로 관찰된 시간을 반영하는 관련 기간이 있습니다. 조사 결과 개요를 볼 때 범위 시간은 조사 결과 기간으로 변경됩니다.

엔터티 프로필에서 범위 시간을 관련 조사 결과에 대한 기간에 맞출 수 있습니다. 이를 통해 해당 기간 동안 발생한 활동을 조사할 수 있습니다.

범위 시간을 조사 결과 기간에 맞추려면 관련 조사 결과 패널에서 사용하려는 조사 결과를 선택합니다.

Detective는 조사 결과 세부 정보를 채우고 범위 시간을 조사 결과 기간으로 설정합니다.

요약 페이지에서 범위 시간 설정

요약 페이지를 검토하면서 범위 시간을 조정하여 이전 365일 중 24시간 동안의 활동을 볼 수 있습니다.

요약 페이지에서 범위 시간 설정

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 요약을 선택합니다.
3. 범위 시간 패널의 요약 옆에서 시작 날짜 및 시간을 변경할 수 있습니다. 시작 시간은 지난 365일 이내여야 합니다.

   시작 날짜 및 시간을 변경하면 종료 날짜 및 시간이 선택한 시작 시간으로부터 24시간 후로 자동 업데이트됩니다.

> **Note**
>
> Detective를 사용하면 최대 1년 분량의 과거 이벤트 데이터에 액세스할 수 있습니다. Detective의 소스 데이터에 대한 자세한 내용은 동작 그래프에 사용된 소스 데이터를 참조하세요.

4. 편집을 마친 경우 변경 내용을 저장하고 표시된 데이터를 업데이트하려면 범위 시간 업데이트를 선택합니다.

Detective에서 관련 조사 결과에 대한 세부 정보 보기

각 엔터티 프로필에는 현재 범위 시간 기간 동안 해당 엔터티와 관련된 조사 결과를 나열하는 관련 조사 결과 패널이 포함되어 있습니다. 엔터티가 침해되었음을 나타내는 한 가지 징후는 여러 조사 결과에 관여했다는 것입니다. 조사 결과 유형을 통해 우려해야 할 활동 유형에 대한 인사이트를 얻을 수도 있습니다.

관련 조사 결과 패널은 엔터티 세부 정보 프로필 패널 바로 아래에 표시됩니다.

각 조사 결과의 경우 테이블에는 다음에 대한 정보가 포함되어 있습니다.

- 조사 결과 개요로 연결되는 링크이기도 한 조사 결과 제목.
- 조사 결과와 연결된 AWS 계정으로, 계정 프로필에 대한 링크이기도 합니다.
- 조사 결과 유형
- 조사 결과가 관찰된 가장 빠른 시간
- 조사 결과가 관찰된 가장 최근 시간
- 조사 결과 심각도

조사 결과에 대한 세부 정보를 표시하려면 조사 결과에 대한 라디오 버튼을 선택합니다. Detective는 페이지 오른쪽에 있는 조사 결과 세부 정보 패널을 채웁니다. 또한 Detective는 범위 시간을 조사 결과 기간으로 변경합니다. 이를 통해 해당 기간 동안 발생한 활동에 초점을 맞출 수 있습니다.

조사 결과 개요에서 엔터티 프로필로 이동한 경우 해당 조사 결과가 자동으로 선택되고 조사 결과에 대한 세부 정보가 표시됩니다.

조사 결과 세부 정보에서 조사 결과 개요로 돌아가려면 관련 엔터티 모두 보기를 선택합니다.

조사 결과를 보관할 수도 있습니다. 자세한 내용은 Amazon GuardDuty 결과 보관을 참조하세요.

Detective에서 대용량 엔터티에 대한 세부 정보 보기

동작 그래프에서 Amazon Detective는 엔터티 간의 관계를 추적합니다. 예를 들어 각 동작 그래프는 AWS 사용자가 AWS 역할을 생성할 때와 EC2 인스턴스가 IP 주소에 연결할 때를 추적합니다.

일정 기간 동안 엔터티에 너무 많은 관계가 있는 경우 Detective는 모든 관계를 저장할 수 없습니다. 현재 범위 시간 중에 이런 일이 발생하면 Detective에서 알려줍니다. Detective는 대용량 엔터티 발생 목록도 제공합니다.

대용량 엔터티란 무엇입니까?

주어진 시간 간격 동안 엔터티는 매우 많은 연결의 출발지 또는 목적지일 수 있습니다. 예를 들어, EC2 인스턴스에는 수백만 개의 IP 주소에서의 연결이 있을 수 있습니다.

Detective는 각 시간 간격 동안 수용할 수 있는 연결 수를 제한합니다. 엔터티가 이 제한을 초과하면 Detective는 해당 시간 간격 동안 연결을 삭제합니다.

예를 들어 시간 간격당 연결 수가 100,000,000이라고 가정해 보겠습니다. 일정 기간 동안 EC2 인스턴스가 100,000,000개 이상의 IP 주소로 연결된 경우 Detective는 해당 시간 간격의 연결을 삭제합니다.

하지만 관계의 반대편에 있는 엔터티를 기반으로 해당 활동을 분석할 수 있을 수도 있습니다. 예제를 계속하자면, EC2 인스턴스가 수백만 개의 IP 주소에서 연결될 수도 있지만 단일 IP 주소는 훨씬 적은 수의 EC2 인스턴스에 연결됩니다. 각 IP 주소 프로필은 해당 IP 주소가 연결된 EC2 인스턴스에 대한 세부 정보를 제공합니다.

프로필에서 대용량 엔터티 알림 보기

Detective는 범위 시간에 엔터티의 연결이 많은 시간 간격이 포함된 경우 조사 결과 또는 엔터티 프로필 상단에 알림을 표시합니다. 조사 결과 프로필은 관련 엔터티를 위한 알림입니다.

이 알림에는 대용량 시간 간격의 관계 목록이 포함되어 있습니다. 각 목록 항목에는 관계에 대한 설명과 대용량 시간 간격의 시작이 포함됩니다.

대용량 시간 간격은 의심스러운 활동을 나타내는 지표일 수 있습니다. 동시에 어떤 다른 활동이 발생했는지 파악하려면 대용량 시간 간격에 대한 조사에 집중할 수 있습니다. 대용량 엔터티 알림에는 범위 시간을 해당 시간 간격으로 설정하는 옵션이 포함되어 있습니다.

범위 시간을 대용량 시간 간격으로 설정

1. 대용량 엔터티 알림에서 시간 간격을 선택합니다.
2. 팝업 메뉴에서 범위 시간 적용을 선택합니다.

현재 범위 시간의 대용량 엔터티 목록 보기

대용량 엔터티 페이지에는 현재 범위 시간 동안의 대용량 시간 간격 및 엔터티 목록이 포함되어 있습니다.

대용량 엔터티 페이지 표시

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 대용량 엔터티를 선택합니다.

로그 스트림의 항목에는 다음 정보가 있습니다.

- 대용량 시간 간격의 시작
- 엔터티의 식별자 및 유형
- 관계에 대한 설명(예: “IP 주소에서 연결된 EC2 인스턴스”)

원하는 열을 기준으로 목록을 필터링하고 정렬할 수 있습니다. 관련 엔터티의 엔터티 프로필로 이동할 수도 있습니다.

엔터티의 프로필로 이동

1. 대용량 엔터티 목록에서 탐색할 행을 선택합니다.
2. 대용량 범위 시간이 포함된 프로필 보기를 선택합니다.

이 옵션을 사용하여 엔터티 프로필로 이동하면 범위 시간이 다음과 같이 설정됩니다.

- 범위 시간은 대용량 시간 간격 30일 전에 시작됩니다.
- 범위 시간은 대용량 시간 간격이 끝날 때 종료됩니다.

Detective에서 결과 또는 개체 검색

Amazon Detective 검색 기능을 사용하면 조사 결과 또는 엔터티를 조사할 수 있습니다. 검색 결과에서 엔터티 프로필 또는 조사 결과 개요로 이동할 수 있습니다. 조사 결과가 10,000개를 초과하는 경우 상위 10,000개의 결과만 표시됩니다. 정렬 순서를 변경하면 반환된 결과가 변경됩니다.

검색 결과를 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. 이 파일에는 검색 페이지에 반환된 데이터가 들어 있습니다. 데이터는 쉼표로 구분된 값(CSV) 형식으로 내보내집니다. 내보낸 데이터의 파일 이름은 패턴 detective-page-panel-yyyy-mm-dd.csv 형식을 따릅니다. CSV 가져오기를 지원하는 다른 AWS 서비스, 타사 애플리케이션 또는 스프레드시트 프로그램을 사용하여 데이터를 조작하여 보안 조사를 강화할 수 있습니다.

> **Note**
>
> 현재 내보내기가 진행 중인 경우 내보내기가 완료될 때까지 기다렸다가 추가 데이터를 내보냅니다.

검색 완료

검색을 완료하려면 검색할 엔터티 유형을 선택합니다. 그런 다음 와일드카드 문자 * 또는 ?를 사용하여 정확한 식별자 또는 식별자를 제공합니다. IP 주소 범위를 검색하려면 CIDR 또는 점 표기법을 사용할 수도 있습니다. 다음 예제 검색 문자열을 참조하세요.

IP 주소의 경우:

- `1.0.*.*`
- `1.0.133.*`
- `1.0.0.0/16`
- `0.239.48.198/31`

기타 모든 유형의 엔터티의 경우:

- `Admin`
- `ad*`
- `ad*n`

- `ad*n*`
- `adm?n`
- `a?m*`
- `*min`

각 엔터티 유형에는 다음과 같은 식별자가 지원됩니다.

- 조사 결과, 조사 결과 식별자 또는 조사 결과 Amazon 리소스 이름(ARN).
- AWS 계정의 경우 계정 ID입니다.
- AWS 역할 및 AWS 사용자의 경우 보안 주체 ID, 이름 또는 입니다ARN.
- 컨테이너 클러스터의 경우 클러스터 이름 또는 ARN.
- 컨테이너 이미지의 경우 리포지토리 또는 컨테이너 이미지의 전체 다이제스트입니다.
- 컨테이너 포드 또는 작업의 경우 포드 이름 또는 포드UID의 입니다.
- EC2 인스턴스의 경우 인스턴스 식별자 또는 입니다ARN.
- 조사 결과 그룹의 경우 조사 결과 그룹 식별자입니다.
- IP 주소의 경우 CIDR 또는 점 표기법의 주소입니다.
- Kubernetes 객체(서비스 계정 또는 사용자)의 경우 이름입니다.
- 역할 세션의 경우 다음 값 중 하나를 사용하여 검색할 수 있습니다.
  - 역할 세션 식별자.

    역할 세션 식별자는 *<rolePrincipalID>*:*<sessionName>* 형식을 사용합니다.

    예: `AROA12345678910111213:MySession`
  - 역할 세션 ARN
  - 세션 이름
  - 수임된 역할의 보안 주체 ID
  - 수임된 역할의 이름
- S3 버킷의 경우 버킷 이름 또는 버킷 입니다ARN.
- 페더레이션 사용자의 경우 보안 주체 ID 또는 사용자 이름입니다. 보안 주체 ID는 *<identityProvider>*:*<username>* 또는 *<identityProvider>*:*<audience>*:*<username>*입니다.
- 사용자 에이전트의 경우 사용자 에이전트 이름입니다.

조사 결과 또는 엔터티 검색

1. AWS Management Console에 로그인합니다. 그런 다음 에서 Detective 콘솔을 엽니다https://console.aws.amazon.com/detective/.
2. 탐색 창에서 검색을 선택합니다.
3. 유형 선택 메뉴에서 찾으려는 항목 유형을 선택합니다.

   사용자를 선택하면 AWS 사용자 또는 페더레이션 사용자를 검색할 수 있다는 점에 유의하세요.

   데이터의 예제에는 동작 그래프 데이터에 있는 선택한 유형의 식별자 샘플 세트가 포함되어 있습니다. 예제 중 하나에 대한 프로필을 표시하려면 해당 식별자를 선택합니다.
4. 검색할 식별자를 정확히 입력하거나 와일드카드 문자가 포함된 식별자를 입력합니다.

   검색은 대/소문자를 구분하지 않습니다.
5. 검색을 선택하거나 Enter 키를 누릅니다.

검색 결과 사용

검색을 완료하면 Detective는 최대 10,000개의 일치하는 결과 목록을 표시합니다. 고유 식별자를 사용하는 검색의 경우 일치하는 결과는 하나뿐입니다.

결과에서 엔터티 프로필 또는 조사 결과 개요로 이동하려면 식별자를 선택합니다.

조사 결과, 역할, 사용자 및 EC2 인스턴스의 경우 검색 결과에는 연결된 계정이 포함됩니다. 계정의 프로필로 이동하려면 계정 식별자를 선택합니다.

검색 문제 해결

Detective에서 조사 결과 또는 엔터티를 찾지 못할 경우 먼저 올바른 식별자를 입력했는지 확인합니다. 값이 정확하면 다음 사항도 확인할 수 있습니다.

- 조사 결과 또는 엔터티가 동작 그래프에서 활성화된 멤버 계정에 속합니까? 관련 계정이 멤버 계정으로 동작 그래프에 초대되지 않은 경우 동작 그래프에는 해당 계정에 대한 데이터가 포함되지 않습니다.

  초대된 멤버 계정이 초대를 수락하지 않은 경우 동작 그래프에는 해당 계정에 대한 데이터가 포함되지 않습니다.

- 조사 결과의 경우, 조사 결과가 보관되었습니까? Detective는 Amazon 에서 보관된 조사 결과를 수신하지 않습니다 GuardDuty.
- Detective가 동작 그래프에 데이터를 수집하기 시작하기 전에 조사 결과 또는 엔터티가 있었습니까? Detective가 수집하는 데이터에 해당 조사 결과 또는 엔터티가 없으면 동작 그래프에 해당 데이터가 포함되지 않습니다.
- 조사 결과 또는 엔터티가 정확한 리전에서 나온 결과입니까? 각 동작 그래프는 에 따라 다릅니다 AWS 리전. 동작 그래프에는 다른 리전의 데이터가 포함되지 않습니다.

Detective에서 계정 관리

계정이 Detective를 활성화하면 해당 계정이 동작 그래프의 관리자 계정이 되고 동작 그래프에 사용할 멤버 계정을 선택합니다. 관리자 계정은 계정을 초대하여 동작 그래프에 조인할 수 있습니다. 계정이 초대를 수락하면 Detective는 해당 계정을 멤버 계정으로 활성화합니다. 초대를 통해 추가된 멤버 계정은 동작 그래프에서 자신을 연결 해제할 수 있습니다.

계정이 멤버 계정으로 활성화되면 Detective는 멤버 계정의 데이터를 수집하고 해당 동작 그래프로 추출하기 시작합니다.

각 동작 그래프에는 하나 이상의 계정 데이터가 포함됩니다. 동작 그래프에는 최대 1,200개의 멤버 계정을 포함할 수 있습니다.

와 통합된 경우 AWS Organizations조직 관리 계정은 조직의 Detective 관리자 계정을 지정합니다. 그러면 Detective 관리자 계정이 조직 동작 그래프의 관리자 계정이 됩니다. Detective 관리자 계정은 조직 동작 그래프에서 모든 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 조직 계정은 조직 동작 그래프에서 자신을 제거할 수 없습니다.

Detective는 각 동작 그래프에 기여한 데이터에 대해 각 계정에 요금을 부과합니다. 동작 그래프에서 각 계정의 데이터 볼륨을 추적하는 방법에 대한 자세한 내용은 Amazon Detective 비용 예측 및 모니터링을 참조하세요.

내용

Detective의 계정 제한 및 권장 사항

Amazon Detective에서 계정을 관리할 때 다음 제한 사항에 유의합니다.

멤버 계정 최대 수

Detective는 각 동작 그래프에서 최대 1,200개의 멤버 계정을 허용합니다.

AWS Organizations 를 사용하여 계정을 관리하는 경우 기본적으로 Detective는 계정 관리 페이지에 최대 5,000개의 멤버 계정을 표시합니다. 모든 계정을 보려면 모든 계정 로드를 선택합니다. 모든 결과를 반환하는 데 몇 분 정도 걸릴 수 있습니다.

계정 및 리전

AWS Organizations 를 사용하여 계정을 관리하는 경우 조직 관리 계정은 조직의 Detective 관리자 계정을 지정합니다. Detective 관리자 계정은 조직 동작 그래프의 관리자 계정이 됩니다.

Detective 관리자 계정은 모든 리전에서 동일해야 합니다. 조직 관리 계정은 각 리전에 있는 Detective 관리자 계정을 개별적으로 지정합니다. 또한 Detective 관리자 계정은 각 리전의 조직 동작 그래프와 멤버 계정을 개별적으로 관리합니다.

초대를 통해 생성된 멤버 계정의 경우 초대를 보낸 리전에서만 관리자-멤버 연결이 생성됩니다. 관리자 계정은 각 리전에서 Detective를 활성화해야 하며 각 리전마다 별도의 동작 그래프가 있어야 합니다. 그러면 관리자 계정이 각 계정을 해당 리전의 구성원 계정으로 연결하도록 초대합니다.

계정은 동일한 리전 내 여러 동작 그래프의 멤버 계정일 수 있습니다. 계정은 리전당 하나의 동작 그래프의 관리자 계정만 될 수 있습니다. 계정은 여러 리전의 관리자 계정일 수 있습니다.

Security Hub CSPM 및 GuardDuty와 관리자 계정의 정렬

AWS Security Hub CSPM 및 Amazon GuardDuty와의 통합이 원활하게 작동하도록 하려면 동일한 계정이 이러한 모든 서비스의 관리자 계정인 것이 좋습니다.

the section called “GuardDuty 및 와의 권장 정렬 AWS Security Hub CSPM”을(를) 참조하세요.

관리자 계정에 필요한 권한 부여

관리자 계정이 동작 그래프를 관리하는 데 필요한 권한을 갖도록 하려면 `AmazonDetectiveFullAccess` 관리형 정책을 IAM 보안 주체에 연결합니다.

Detective에 조직 업데이트 반영

조직의 변경 사항은 Detective에 즉시 반영되지 않습니다.

신규 및 제거된 조직 계정과 같은 대부분의 변경 사항은 Detective에 알림이 전송되는 데 최대 1시간이 걸릴 수 있습니다.

Organizations에서 지정된 Detective 관리자 계정을 변경하면 변경 내용을 전파하는 데 시간이 덜 걸립니다.

Organizations를 사용하여 동작 그래프 계정 관리

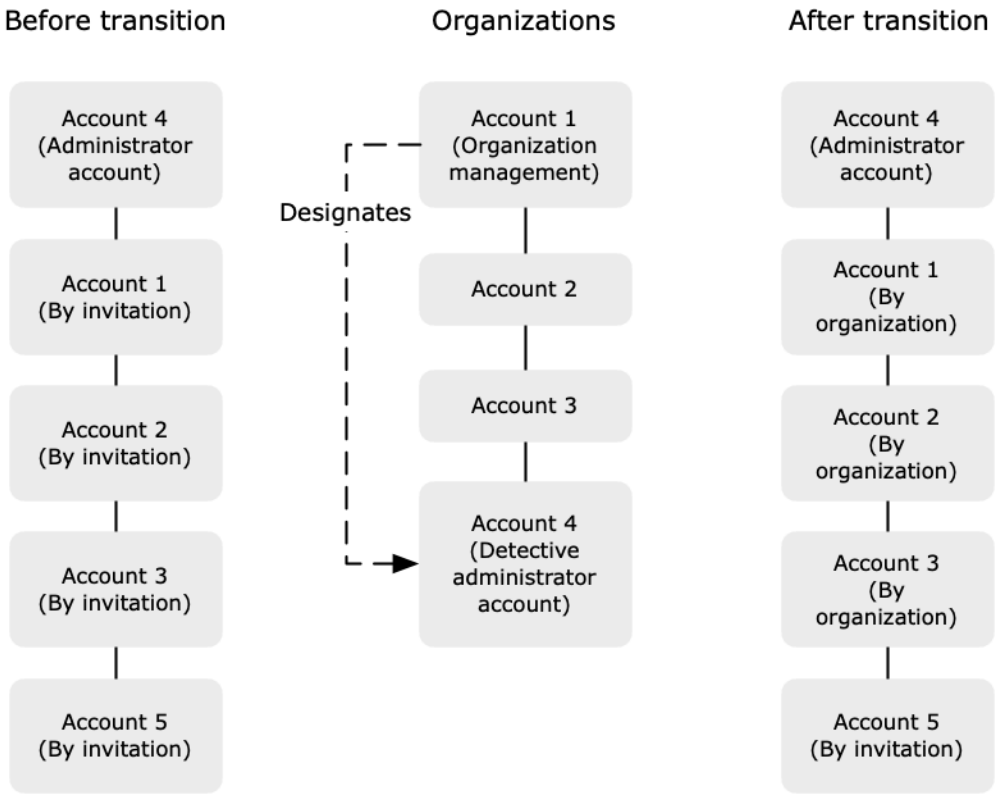
수동 초대를 수락한 멤버 계정이 표시된 기존 동작 그래프가 있을 수 있습니다. 에 등록한 경우 수동 초대 프로세스를 사용하는 대신 AWS Organizations다음 단계에 따라 Organizations를 사용하여 멤버 계정을 활성화하고 관리합니다.

1. 조직을 위해 Detective 관리자 계정을 지정합니다. 그러면 조직 동작 그래프가 생성됩니다.

   Detective 관리자 계정에 이미 동작 그래프가 있는 경우 해당 동작 그래프는 조직 동작 그래프가 됩니다.
2. 조직 동작 그래프에서 조직 계정을 멤버 계정으로 활성화합니다.

   조직 동작 그래프에 조직 계정인 기존 멤버 계정이 있는 경우 해당 계정은 자동으로 활성화됩니다.

다음 다이어그램은 전환 전의 동작 그래프 구조, Organizations의 구성, 전환 후의 동작 그래프 계정 구조에 대한 개요를 보여줍니다.



조직의 Detective 관리자 계정 지정

조직 관리 계정은 조직의 Detective 관리자 계정을 지정합니다. the section called “Detective 관리자 계정 지정”을(를) 참조하세요.

전환을 더 단순하게 만들기 위해 Detective는 현재 관리자 계정을 조직의 Detective 관리자 계정으로 선택할 것을 권장합니다.

Organizations에 Detective에 대해 위임된 관리자 계정이 있는 경우 해당 계정 또는 조직 관리 계정을 Detective 관리자 계정으로 사용해야 합니다.

그렇지 않으면 조직 관리 계정이 아닌 Detective 관리자 계정을 처음 지정할 때 Detective는 Organizations를 호출하여 해당 계정을 Detective의 위임된 관리자 계정으로 설정합니다.

조직 계정을 구성원 계정으로 활성화합니다.

Detective 관리자 계정은 조직 동작 그래프의 관리자 계정입니다. Detective 관리자 계정은 조직 동작 그래프에서 멤버 계정으로 활성화할 조직 계정을 선택합니다. the section called “조직 멤버 계정 관리”을(를) 참조하세요.

계정 페이지에서 Detective 관리자 계정은 조직의 모든 계정을 볼 수 있습니다.

Detective 관리자 계정이 이미 동작 그래프의 관리자 계정인 경우 해당 동작 그래프는 조직 동작 그래프가 됩니다. 동작 그래프에서 이미 멤버 계정이었던 조직 계정은 자동으로 멤버 계정으로 활성화됩니다. 다른 조직 계정의 상태는 멤버가 아님입니다.

조직 계정이 이전에 초대를 통한 구성원 계정이었더라도 조직 계정에는 조직을 통한 유형이 있습니다.

조직에 속하지 않는 멤버 계정의 유형은 초대별 계정입니다.

계정 관리 페이지에는 새 계정이 조직에 추가될 때 자동으로 활성화할 수 있는 새 조직 계정 자동 활성화 옵션도 제공합니다. the section called “새 조직 계정 활성화”을(를) 참조하세요. 이 옵션은 처음에는 꺼져 있습니다.

Detective 관리자 계정이 계정 관리 페이지를 처음 표시하면 모든 조직 계정 활성화 버튼이 포함된 메시지가 표시됩니다. 모든 조직 계정 활성화를 선택하면 Detective는 다음 작업을 수행합니다.

- 현재 조직 계정 전체를 멤버 계정으로 활성화합니다.
- 옵션을 켜면 새 조직 계정을 자동 활성화합니다.

멤버 계정 목록에는 모든 조직 계정 활성화 옵션도 있습니다.

조직의 Detective 관리자 지정

조직 동작 그래프에서 Detective 관리자 계정은 모든 조직 계정의 동작 그래프 멤버십을 관리합니다.

Detective 관리자 계정 관리 방법 - 조직 관리 계정은 각에서 조직의 Detective 관리자 계정을 지정합니다 AWS 리전.

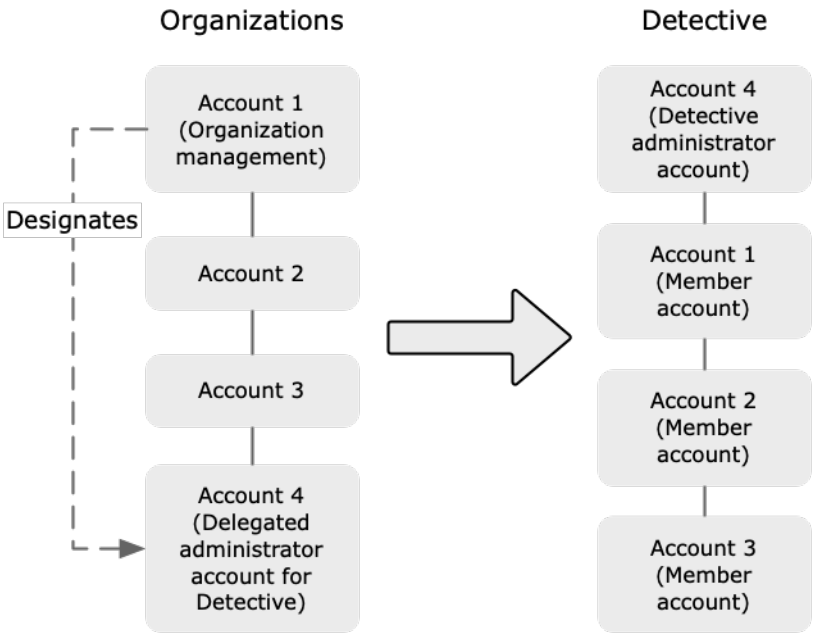
Detective 관리자 계정을 위임된 관리자 계정으로 설정 - Detective 관리자 계정도 Detective의 위임된 관리자 계정이 됩니다 AWS Organizations. 단, 조직 관리 계정이 본인을 Detective 관리자 계정으로 지정한 경우는 예외입니다. 조직 관리 계정은 조직에서 위임된 관리자일 수 있습니다.

조직에 위임된 관리자 계정이 설정되면 조직 관리 계정은 위임된 관리자 계정 또는 자체 계정만 Detective 관리자 계정으로 선택할 수 있습니다. 모든 리전에 위임된 관리자 계정을 선택하는 것을 권장합니다.

조직 동작 그래프 생성 및 관리 - 조직 관리 계정이 Detective 관리자 계정을 선택하면 Detective는 해당 계정에 대한 새 동작 그래프를 생성합니다. 이 동작 그래프는 조직 동작 그래프입니다.

Detective 관리자 계정이 기존 동작 그래프의 관리자 계정인 경우 해당 동작 그래프는 조직 동작 그래프가 됩니다.

Detective 관리자 계정은 조직 동작 그래프에서 멤버 계정으로 활성화할 조직 계정을 선택합니다.



Detective 관리자 계정은 조직에 속하지 않는 계정으로 초대를 보낼 수도 있습니다. 자세한 내용은 the section called “조직 멤버 계정 관리” 및 the section called “초대된 멤버 계정 관리” 섹션을 참조하세요.

Detective 관리자 계정을 구성하는 데 필요한 권한 - 조직 관리 계정이 Detective 관리자 계정을 구성할 수 있도록 (IAM) 엔터티에 `AmazonDetectiveOrganizationsAccess` 관리형 정책을 연결할 수 있습니다 AWS Identity and Access Management .

Detective 관리자 지정

조직 관리 계정은 Detective 콘솔을 사용하여 Detective 관리자 계정을 지정합니다.

Detective 관리자 계정을 관리하기 위해 Detective를 활성화할 필요는 없습니다. Detective 관리자 계정은 Detective 활성화 페이지에서 관리할 수 있습니다.

Enable Detective page (Console)

Detective 활성화 페이지에서 Detective 관리자를 지정하려면 다음 단계를 따르세요.

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Get started를 선택합니다.
3. 관리자 계정에 필요한 권한 패널에서 선택한 계정에 필요한 권한을 부여하여 해당 계정이 Detective의 모든 작업에 대한 전체 액세스 권한을 가진 Detective 관리자로 운영할 수 있도록

합니다. 관리자로 운영하려면 보안 주체에 AmazonDetectiveFullAccess 정책을 연결하는 것이 좋습니다.

4. IAM 콘솔에서 직접 권장 정책을 보려면 IAM에서 정책 연결을 선택합니다.
5. IAM 콘솔에서 권한이 있는지 여부에 따라 다음과 같이 진행합니다.

   - IAM 콘솔에서 운영할 권한이 있는 경우 Detective에 사용하는 보안 주체에 권장 정책을 연결합니다.
   - IAM 콘솔에서 작업할 수 있는 권한이 없는 경우 정책의 Amazon 리소스 이름(ARN)을 복사하여 IAM 관리자에게 제공합니다. 그러면 담당자가 사용자를 대신하여 정책을 연결할 수 있습니다.
6. Detective 관리자에서 Detective 관리자 계정을 선택합니다.

   사용 가능한 옵션은 Organizations의 Detective 관리자 계정을 위임했는지 여부에 따라 달라집니다.

   - Organizations의 Detective에 대한 위임된 관리자 계정이 없는 경우 계정의 계정 식별자를 입력하여 Detective 관리자 계정으로 지정합니다.

     수동 초대 프로세스의 기존 관리자 계정 및 동작 그래프가 있을 수 있습니다. 있는 경우 해당 계정을 Detective 관리자 계정으로 지정하는 것이 좋습니다.

     Organizations for Amazon GuardDuty AWS Security Hub CSPM또는 Amazon Macie에 위임된 관리자 계정이 있는 경우 Detective는 해당 계정 중 하나를 선택하라는 메시지를 표시합니다. 다른 계정을 입력할 수도 있습니다.
   - Organizations의 Detective에 대한 위임된 관리자 계정이 있는 경우 해당 계정 또는 사용자 계정을 선택하라는 메시지가 표시됩니다. 모든 리전에 위임된 관리자 계정을 선택하는 것을 권장합니다.
7. 위임을 선택합니다.

Detective를 활성화했거나 기존 동작 그래프의 멤버 계정인 경우 일반 페이지에서 Detective 관리자 계정을 지정할 수 있습니다.

General page (Console)

일반 페이지에서 Detective 관리자를 지정하려면 다음 단계를 따릅니다.

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창의 설정 아래에서 일반을 선택합니다.

3. 관리형 정책 패널에서 Detective가 지원하는 모든 관리형 정책에 대해 자세히 알아볼 수 있습니다. Detective에서 사용자가 수행하기를 원하는 작업에 따라 계정에 필요한 권한을 부여할 수 있습니다. 관리자로 운영하려면 보안 주체에 `AmazonDetectiveFullAccess` 정책을 연결하는 것이 좋습니다.
4. IAM 콘솔에서 권한이 있는지 여부에 따라 다음과 같이 진행합니다.

   - IAM 콘솔에서 운영할 권한이 있는 경우 Detective에 사용하는 보안 주체에 권장 정책을 연결합니다.
   - IAM 콘솔에서 작업할 수 있는 권한이 없는 경우 정책의 Amazon 리소스 이름(ARN)을 복사하여 IAM 관리자에게 제공합니다. 그러면 담당자가 사용자를 대신하여 정책을 연결할 수 있습니다.

   사용 가능한 옵션은 Organizations의 Detective 관리자 계정을 위임했는지 여부에 따라 달라집니다.

   - Organizations의 Detective에 대한 위임된 관리자 계정이 없는 경우 계정의 계정 식별자를 입력하여 Detective 관리자 계정으로 지정합니다.

     수동 초대 프로세스의 기존 관리자 계정 및 동작 그래프가 있을 수 있습니다. 있는 경우 해당 계정을 Detective 관리자 계정으로 지정하는 것이 좋습니다.

     Organizations for Amazon GuardDuty AWS Security Hub CSPM또는 Amazon Macie에 위임된 관리자 계정이 있는 경우 Detective는 해당 계정 중 하나를 선택하라는 메시지를 표시합니다. 다른 계정을 입력할 수도 있습니다.
   - Organizations의 Detective에 대한 위임된 관리자 계정이 있는 경우 해당 계정 또는 사용자 계정을 선택하라는 메시지가 표시됩니다. 모든 리전에 위임된 관리자 계정을 선택하는 것을 권장합니다.
5. 위임을 선택합니다.

Detective API, AWS CLI

Detective 관리자 계정을 지정하기 위해 API 직접 호출 또는 AWS Command Line Interface를 사용할 수 있습니다. 조직 관리 계정 보안 인증 정보를 사용해야 합니다.

조직에 Detective에 대한 위임된 관리자 계정이 이미 있는 경우 해당 계정 또는 사용자 계정을 선택해야 합니다. 위임된 관리자 계정을 선택하는 것이 좋습니다.

Detective 관리자 계정을 지정하려면(Detective API, AWS CLI)

- Detective API: `EnableOrganizationAdminAccount` 작업을 사용합니다. Detective 관리자 계정의 AWS 계정 식별자를 제공해야 합니다. 계정 식별자를 얻으려면 `ListOrganizationAdminAccounts` 작업을 사용합니다.
- AWS CLI: 명령줄에서 `enable-organization-admin-account` 명령을 실행합니다.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

예제

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Detective 관리자 계정 지정

조직 관리자 계정은 리전의 현재 Detective 관리자 계정을 제거할 수 있습니다. Detective 관리자 계정을 제거하면 Detective는 현재 리전에서만 해당 계정을 제거합니다. Organizations의 위임된 관리자 계정은 변경되지 않습니다.

조직 관리 계정이 리전의 Detective 관리자 계정을 제거하면 Detective는 조직 동작 그래프를 삭제합니다. 제거된 Detective 관리자 계정에 대해 Detective가 비활성화됩니다.

Detective의 현재 위임된 관리자 계정을 제거하려면 Organizations API를 사용합니다. Organizations의 Detective에 대한 위임된 관리자 계정을 제거하면 Detective는 위임된 관리자 계정이 Detective 관리자 계정인 조직 동작 그래프를 모두 삭제합니다. 조직 관리 계정을 Detective 관리자 계정으로 사용하는 조직 동작 그래프는 영향을 받지 않습니다.

Console

Detective 관리자 계정은 Detective 콘솔에서 제거할 수 있습니다.

Detective 관리자 계정을 제거하면 해당 계정에 대해 Detective가 비활성화되고 조직 동작 그래프가 삭제됩니다. Detective 관리자 계정은 현재 리전에서만 제거됩니다.

> **Important**
>
> Detective 관리자 계정을 제거해도 Organizations의 위임된 관리자 계정에는 영향을 미치지 않습니다.

Detective 관리자 계정을 제거(Detective 활성화 페이지)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Get started를 선택합니다.
3. 위임된 관리자에서 Amazon Detective 비활성화를 선택합니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 Amazon Detective 비활성화를 선택합니다.

Detective 관리자 계정 제거(일반 페이지)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 위임된 관리자에서 Amazon Detective 비활성화를 선택합니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 Amazon Detective 비활성화를 선택합니다.

Detective API, AWS CLI

Detective 관리자 계정을 제거하기 위해 API 직접 호출 또는 AWS CLI를 사용할 수 있습니다. 조직 관리 계정 보안 인증 정보를 사용해야 합니다.

Detective 관리자 계정을 제거하면 해당 계정에 대해 Detective가 비활성화되고 조직 동작 그래프가 삭제됩니다.

> **Important**
>
> Detective 관리자 계정을 제거해도 Organizations의 위임된 관리자 계정에는 영향을 미치지 않습니다.

Detective 관리자 계정을 제거하려면(Detective API, AWS CLI)

- Detective API: `DisableOrganizationAdminAccount` 작업을 사용합니다.

  Detective API를 사용하여 Detective 관리자 계정을 제거하면 API 직접 호출 또는 명령이 실행된 리전에서만 해당 계정이 제거됩니다.
- AWS CLI: 명령줄에서 `disable-organization-admin-account` 명령을 실행합니다.

```
aws detective disable-organization-admin-account
```

위임된 관리자 계정 제거

Detective 관리자 계정을 제거해도 Organizations의 위임된 관리자 계정은 자동으로 제거되지 않습니다. Detective의 위임된 관리자 계정을 제거하기 위해 Organizations API를 사용할 수 있습니다.

위임된 관리자 계정을 제거하면 위임된 관리자 계정이 Detective 관리자 계정인 조직 동작 그래프가 모두 삭제됩니다. 또한 해당 리전의 계정에 대해 Detective를 비활성화합니다.

위임된 관리자 계정을 제거하려면(조직 API, AWS CLI)

- 조직 API: `DeregisterDelegatedAdministrator` 작업을 사용합니다. Detective 관리자 계정의 계정 식별자 및 Detective의 서비스 보안 주체인 `detective.amazonaws.com`을 제공해야 합니다.
- AWS CLI: 명령줄에서 `deregister-delegated-administrator` 명령을 실행합니다.

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

예제

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --
service-principal detective.amazonaws.com
```

계정에 사용할 수 있는 작업

관리자 및 구성원 계정은 다음과 같은 Detective 작업에 액세스할 수 있습니다. 테이블에서 값의 의미는 다음과 같습니다.

- 모두 - 이 계정은 동일한 Detective 관리자 계정에 속한 모든 계정에 대해 작업을 수행할 수 있습니다.
- 본인 - 이 계정은 자신의 계정에서만 작업을 수행할 수 있습니다.
- 대시(-) - 해당 계정에서 작업을 수행할 수 없습니다.

조직 동작 그래프에서 Detective 관리자 계정은 멤버 계정으로 활성화할 조직 계정을 결정합니다. 새 조직 계정을 멤버 계정으로 자동 활성화하도록 Detective를 구성하거나 조직 계정을 수동으로 활성화하도록 Detective를 구성할 수 있습니다.

관리자 계정은 동작 그래프에서 계정을 멤버 계정으로 초대할 수 있습니다. 멤버 계정이 초대를 수락하고 활성화되면 Amazon Detective는 멤버 계정의 데이터를 수집하고 해당 동작 그래프로 추출하기 시작합니다.

조직 동작 그래프 이외의 동작 그래프의 경우 모든 멤버 계정은 초대된 계정입니다.

다음 테이블에는 관리자 및 멤버 계정의 기본 권한이 반영되어 있습니다. 사용자 지정 IAM 정책을 사용하여 Detective 기능 및 기능에 대한 추가 액세스를 제한할 수 있습니다.

작업	관리자 계정(조직)	관리자 계정(초대)	멤버(조직)	멤버(초대)
계정 보기	모두	모두	본인(관리자 계정 보기)	본인(관리자 계정 보기)
멤버 계정 제거	모두 초대된 계정이 제거됨 조직 계정 연결 해제됨	모두	–	본인
선택적 데이터 소스 패키지 추가 또는 제거	모두(설정은 모든 멤버 계정에 적용됨)	모두(설정은 모든 멤버 계정에 적용됨)	–	–
Detective 비활성화	본인	본인	–	–
동작 그래프 데이터 보기	모두	모두	–	–
선택적 데이터 소스 패키지 활성화 또는 비활성화	모두	모두	–	–

계정 목록 보기

관리자 계정은 Detective 콘솔 또는 API를 사용하여 계정 목록을 볼 수 있습니다. 목록에는 다음을 포함할 수 있습니다.

- 동작 그래프에 조인하도록 관리자 계정이 초대한 계정. 이러한 계정에는 초대별 유형이 있습니다.

- 조직 동작 그래프의 경우 조직의 모든 계정. 이러한 계정에는 조직별 유형이 있습니다.

초대를 거부했거나 관리자 계정이 동작 그래프에서 제거한 초대된 멤버 계정은 결과에 포함되지 않습니다. 다음 상태의 계정만 포함됩니다.

확인 진행 중

초대된 계정의 경우 Detective는 초대를 보내기 전에 계정 이메일 주소를 확인합니다.

조직 계정의 경우 Detective는 해당 계정이 조직에 속하는지 확인합니다. Detective는 해당 계정을 활성화한 계정이 Detective 관리자 계정인지도 확인합니다.

확인 실패

확인 실패 초대가 전송되지 않았거나 조직 계정이 멤버으로 활성화되지 않았습니다.

초대됨

초대된 계정의 경우. 초대를 보냈지만 멤버 계정이 아직 응답하지 않았습니다.

멤버가 아님

조직 동작 그래프의 조직 계정의 경우. 조직 계정이 현재 멤버 계정이 아닙니다. 조직 동작 그래프에 데이터를 제공하지 않습니다.

활성화됨

초대된 계정의 경우 멤버 계정이 초대를 수락하고 동작 그래프에 데이터를 제공합니다.

조직 동작 그래프의 조직 계정의 경우 Detective 관리자 계정을 통해 해당 계정을 멤버 계정으로 활성화했습니다. 이 계정은 조직 동작 그래프에 데이터를 제공합니다.

활성화되지 않음

초대된 계정의 경우, 멤버 계정이 초대를 수락했지만 활성화할 수는 없습니다.

조직 동작 그래프에 있는 조직 계정의 경우 Detective 관리자 계정이 해당 계정을 활성화하려고 했지만 활성화할 수 없습니다.

초대된 계정의 경우 Detective는 멤버 계정 수를 확인합니다. 동작 그래프의 최대 멤버 계정 수는 1,200개입니다. 동작 그래프에 이미 1,200개의 멤버 계정이 포함된 경우 새 계정을 활성화할 수 없습니다.

Detective는 데이터 볼륨이 Detective 할당량 내에 있는지 확인합니다. 동작 그래프에 입력되는 데이터의 볼륨은 Detective에서 허용하는 최대값보다 작아야 합니다. 현재 수집된 볼륨이 동작 그래프 데이터 볼륨의 일일 10TB 제한을 초과하는 경우 Detective는 멤버 계정을 추가할 수 없습니다.

계정 목록 작성(콘솔)

를 사용하여 계정 목록을 보고 필터링 AWS Management Console 할 수 있습니다.

계정 목록 표시(콘솔)

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.

   멤버 계정 목록에는 다음 계정이 포함됩니다.

   - 계정
   - 동작 그래프에 데이터를 제공하도록 초대한 계정
   - 조직 동작 그래프의 모든 조직 계정

   각 계정의 경우 목록에는 다음 정보가 표시됩니다.

   - AWS 계정 식별자입니다.
   - 조직 계정의 경우, 계정 이름.
   - 계정 유형(초대별 또는 조직별).
   - 초대된 계정의 경우, 계정 루트 사용자 이메일 주소.
   - 계정 상태.
   - 계정의 일일 데이터 볼륨. Detective는 멤버 계정으로 활성화되지 않은 계정의 데이터 볼륨을 검색할 수 없습니다.
   - 계정 상태가 마지막으로 업데이트된 날짜.

테이블 상단의 탭을 사용하여 멤버 계정 상태를 기준으로 목록을 필터링할 수 있습니다. 각 탭에는 일치하는 멤버 계정 수가 표시됩니다.

- 모든 멤버 계정을 보려면 모두를 선택합니다.
- 활성화됨 상태인 계정을 보려면 활성화됨을 선택합니다.
- 활성화됨 외 상태의 계정을 보려면 활성화되지 않음을 선택합니다.

멤버 계정 목록에 다른 필터를 추가할 수도 있습니다.

동작 그래프의 계정 목록에 필터 추가(콘솔)

1. 필터 상자를 선택합니다.
2. 목록에서 필터에 사용할 열을 선택합니다.
3. 지정된 열에 대해 필터에 사용할 값을 선택합니다.
4. 필터를 제거하려면 오른쪽 상단에 있는 x 아이콘을 선택합니다.
5. 목록을 최신 상태 정보로 업데이트하려면 오른쪽 상단에 있는 새로 고침 아이콘을 선택합니다.

멤버 계정 나열(Detective API, AWS CLI)

API 호출 또는를 사용하여 동작 그래프에서 멤버 계정 목록을 AWS Command Line Interface 볼 수 있습니다.

요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

멤버 계정 목록을 검색하려면(Detective API, AWS CLI)

- Detective API: `ListMembers` 작업을 사용합니다. 의도한 동작 그래프를 식별하려면 동작 그래프 ARN을 지정합니다.

  단, 조직 동작 그래프의 경우 `ListMembers`는 멤버 계정으로 활성화하지 않았거나 동작 그래프에서 연결 해제한 조직 계정을 반환하지 않습니다.
- AWS CLI: 명령줄에서 `list-members` 명령을 실행합니다.

```
aws detective list-members --graph-arn <behavior graph ARN>
```

예제:

```
aws detective list-members --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

동작 그래프에서 특정 멤버 계정에 대한 세부 정보를 검색하려면(Detective API, AWS CLI)

- Detective API: `GetMembers` 작업을 사용합니다. 동작 그래프 ARN과 멤버 계정의 계정 식별자 목록을 지정합니다.
- AWS CLI: 명령줄에서 `get-members` 명령을 실행합니다.

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior
 graph ARN>
```

예제:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

조직 계정을 Detective 멤버 계정으로 관리

조직 동작 그래프에서 Detective 관리자 계정은 멤버 계정으로 활성화할 조직 계정을 결정합니다. 기본적으로 새 조직 계정은 멤버 계정으로 활성화되지 않습니다. 해당 멤버의 상태는 멤버가 아님입니다. Detective 관리자 계정은 조직 동작 그래프에서 새 조직 계정을 멤버 계정으로 자동 활성화화도록 Detective를 구성할 수 있습니다.

Detective 관리자는 새 조직 계정을 멤버 계정으로 자동으로 활성화하도록 Detective를 구성할 수 있습니다. 조직 계정을 자동으로 활성화하도록 선택하면 Detective는 새 계정이 조직에 추가될 때 새 계정을 멤버 계정으로 활성화하기 시작합니다. Detective는 아직 활성화되지 않은 기존 조직 계정을 활성화하지 않습니다.

새 조직 계정을 자동으로 활성화하지 않으려면 Detective에서 조직 계정을 수동으로 멤버 계정으로 활성화할 수 있습니다. 연결 해제된 조직 계정을 수동으로 활성화할 수도 있습니다. 조직 동작 그래프에 이미 최대 1,200개의 활성화된 계정이 있는 경우 Detective 관리자는 조직 계정을 멤버 계정으로 활성화할 수 없습니다. 이 경우 조직 계정 상태는 멤버가 아님으로 유지됩니다.

Detective 관리자는 조직 동작 그래프에서 조직 계정의 연결을 해제할 수도 있습니다. 조직 동작 그래프에서 조직 계정의 데이터 수집을 중지하기 위해 계정 연결을 해제할 수 있습니다. 해당 계정의 기존 데이터는 동작 그래프에 그대로 남아 있습니다.

내용

- 새 조직 계정을 Detective 멤버 계정으로 활성화
- 조직 계정을 Detective 멤버 계정으로 활성화
- 조직 계정을 Detective 멤버 계정으로 연결 해제

새 조직 계정을 Detective 멤버 계정으로 활성화

Detective 관리자 계정은 조직 동작 그래프에서 새 조직 계정을 멤버 계정으로 자동 활성화화도록 Detective를 구성할 수 있습니다.

조직에 새 계정을 추가하면 해당 계정이 계정 관리 페이지의 목록에 추가됩니다. 조직 계정의 경우, 유형은 조직별입니다.

기본적으로 새 조직 계정은 멤버 계정으로 활성화되지 않습니다. 해당 멤버의 상태는 멤버가 아님입니다.

조직 계정을 자동으로 활성화하도록 선택하면 Detective는 새 계정이 조직에 추가될 때 새 계정을 멤버 계정으로 활성화하기 시작합니다. Detective는 아직 활성화되지 않은 기존 조직 계정을 활성화하지 않습니다.

Detective는 동작 그래프의 최대 멤버 계정 수가 1,200인 경우에만 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 동작 그래프에 이미 1,200개의 멤버 계정이 있는 경우 새 계정을 활성화할 수 없습니다.

Console

계정 관리 페이지의 새 조직 계정 자동 활성화 설정은 조직에 계정을 추가할 때 계정을 자동으로 활성화할지 여부를 결정합니다.

새 조직 계정을 멤버 계정으로 자동 활성화

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 새 조직 계정 자동 활성화 상태로 전환합니다.

DetectiveAPI/AWS CLI

새 조직 계정을 Detective 멤버 계정으로 자동으로 활성화할지 여부를 결정하기 위해 관리자 계정은 Detective API 또는를 사용할 수 있습니다 AWS Command Line Interface.

구성을 보고 관리하려면 동작 그래프 ARN을 제공해야 합니다. ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

조직 계정 자동 활성화를 위한 현재 구성 보기

- Detective API: `DescribeOrganizationConfiguration` 작업을 사용합니다.

응답에서 새 조직 계정이 자동 활성화되면 AutoEnable은 true입니다.

- AWS CLI: 명령줄에서 describe-organization-configuration 명령을 실행합니다.

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

예제

```
aws detective describe-organization-configuration --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

새 조직 계정 자동 활성화

- Detective API: UpdateOrganizationConfiguration 작업을 사용합니다. 새 조직 계정을 자동 활성화하려면 AutoEnable을 true로 설정합니다.
- AWS CLI: 명령줄에서 update-organization-configuration 명령을 실행합니다.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN>
 --auto-enable | --no-auto-enable
```

예제

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --auto-enable
```

조직 계정을 Detective 멤버 계정으로 활성화

자동으로 새 조직 계정을 자동으로 활성화하지 않는 경우 해당 계정을 수동으로 활성화할 수 있습니다. 또한 연결을 해제한 계정도 수동으로 활성화해야 합니다.

계정 활성화 여부 결정

조직 동작 그래프에 이미 최대 1,200개의 활성 계정이 있는 경우 조직 계정을 멤버 계정으로 활성화할 수 없습니다. 이 경우 조직 계정 상태는 멤버가 아님으로 유지됩니다. 계정은 동작 그래프에 데이터를 제공하지 않습니다.

멤버 계정을 활성화할 수 있게 되면 Detective는 자동으로 멤버 계정 상태를 활성화됨으로 변경합니다. 예를 들어 관리자 계정이 계정 공간을 확보하기 위해 다른 멤버 계정을 제거하면 멤버 계정 상태가 활성화됨으로 변경됩니다.

Console

계정 관리 페이지에서 조직 계정을 멤버 계정으로 활성화할 수 있습니다.

조직 계정을 멤버 계정으로 활성화

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 현재 활성화되지 않은 계정 목록을 보려면 활성화되지 않음을 선택합니다.
4. 특정 조직 계정을 선택하거나 모든 조직 계정을 활성화할 수 있습니다.

   선택한 조직 계정 활성화

   a. 활성화하려는 각 조직 계정을 선택합니다.
   b. 계정 활성화를 선택합니다.

   모든 조직 계정을 활성화하려면 모든 조직 계정 활성화를 선택합니다.

Detective API/AWS CLI

Detective API 또는 AWS Command Line Interface 를 사용하여 조직 동작 그래프에서 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

조직 계정을 멤버 계정으로 활성화

- Detective API: `CreateMembers` 작업을 사용합니다. 그래프 ARN을 제공해야 합니다.

  각 계정에 대해 계정 식별자를 지정합니다. 조직 동작 그래프의 조직 계정은 초대를 받지 않습니다. 이메일 주소 또는 기타 초대 정보는 제공할 필요가 없습니다.
- AWS CLI: 명령줄에서 `create-members` 명령을 실행합니다.

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-
arn <behavior graph ARN>
```

예제

```
aws detective create-members --accounts AccountId=444455556666
 AccountId=123456789012 --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

조직 계정을 Detective 멤버 계정으로 연결 해제

조직 동작 그래프에서 조직 계정의 데이터 수집을 중지하기 위해 계정 연결을 해제할 수 있습니다. 해당 계정의 기존 데이터는 동작 그래프에 그대로 남아 있습니다.

조직 멤버 계정의 연결을 해제하면 해당 계정의 상태가 멤버 아님으로 변경됩니다. Detective는 더 이상 해당 계정의 데이터를 동작 그래프로 수집하지 않습니다. 이 계정의 기존 데이터는 동작 그래프에 남아 있고 계정은 목록에 남아 있습니다.

Console

계정 관리 페이지에서 조직 계정을 멤버 계정 연결과 해제할 수 있습니다.

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 활성화된 계정 목록을 표시하려면 활성화됨을 선택합니다.
4. 연결을 해제할 각 계정의 확인란을 선택합니다.
5. 작업을 선택합니다. 그런 다음 계정 비활성화를 선택합니다.

   연결이 해제된 계정의 계정 상태가 멤버가 아님으로 변경됩니다.

Detective API/AWS CLI

요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

조직 동작 그래프에서 조직 계정의 연결을 해제하려면

- Detective API: `DeleteMembers` 작업을 사용합니다. 연결을 해제할 멤버 계정의 그래프 ARN과 계정 식별자 목록을 지정합니다.
- AWS CLI: 명령줄에서 `delete-members` 명령을 실행합니다.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

예제

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Detective에서 초대된 멤버 계정 관리

Detective 관리자 계정은 동작 그래프에서 계정을 멤버 계정으로 초대할 수 있습니다. 동작 그래프에는 최대 1,200개의 멤버 계정이 포함될 수 있습니다. 멤버 계정이 초대를 수락하고 활성화되면 Amazon Detective는 멤버 계정의 데이터를 수집하고 해당 동작 그래프로 추출하기 시작합니다.

개별 계정을 초대하려면 동작 그래프에 데이터를 제공하도록 초대할 멤버 계정을 수동으로 지정할 수 있습니다. 멤버 계정 목록을 추가하려면 동작 그래프에 초대할 멤버 계정 목록이 포함된 .csv 파일을 제공하도록 선택할 수 있습니다.

조직 동작 그래프 이외의 동작 그래프의 경우 모든 멤버 계정이 초대된 계정입니다. Detective 관리자 계정은 조직 계정이 아닌 계정을 조직 동작 그래프에 초대할 수도 있습니다.

상위 수준에서 동작 그래프에 제공하도록 계정을 초대하는 프로세스는 다음과 같습니다.

1. 추가할 각 멤버 계정에 대해 관리자 계정은 AWS 계정 식별자와 루트 사용자 이메일 주소를 제공합니다.
2. Detective는 이메일 주소가 계정의 루트 사용자 이메일 주소인지 확인합니다. 계정 정보가 유효하면 Detective는 멤버 계정으로 초대를 보냅니다.

   Detective는이 검증을 수행하지 않거나 다음 리전의 멤버 계정에 이메일 초대를 보냅니다.

   - AWS GovCloud(미국 동부) 리전
   - AWS GovCloud(미국 서부) 리전

   다른 리전의 경우 Detective API의 CreateMembers 작업을 `DisableEmailNotification` 사용할 수 있습니다. `DisableEmailNotification`가 true로 설정된 경우 Detective는 멤버 계정에 초대를 보내지 않습니다. 이는 중앙에서 관리되는 계정에 유용한 설정입니다.
3. 멤버 계정은 초대를 수락 또는 거부합니다.

관리자 계정이 초대 이메일을 보내지 않더라도 멤버 계정은 초대에 응답해야 합니다.

4. 멤버 계정이 초대를 수락하면 Detective는 멤버 계정의 데이터를 동작 그래프로 수집하기 시작합니다.
5. 멤버 계정을 활성화할 수 있게 되면 Detective는 자동으로 멤버 계정 상태를 활성화됨으로 변경합니다.

   예를 들어 관리자 계정이 계정 공간을 확보하기 위해 다른 멤버 계정을 제거하면 멤버 계정 상태가 활성화됨으로 변경됩니다.

   둘 이상의 계정이 활성화되지 않음 상태인 경우 Detective는 초대된 순서대로 계정을 활성화합니다. 활성화되지 않음 상태의 계정을 활성화할지 여부를 확인하는 프로세스가 1시간마다 실행됩니다.

   또한 관리자 계정은 자동 프로세스를 기다리지 않고 수동으로 계정을 활성화할 수 있습니다. 예를 들어 관리자 계정은 활성화할 계정을 선택하려고 할 수 있습니다. 멤버 계정을 활성화하는 방법에 대한 자세한 내용은 섹션을 참조하세요the section called “활성화되지 않은 멤버 계정 활성화”.

   참고로 Detective는 2021년 5월 12일부터 활성화되지 않음 상태의 계정을 자동으로 활성화하기 시작했습니다. 이전에 활성화되지 않음 상태의 계정은 자동으로 활성화되지 않습니다. 관리자 계정이 수동으로 활성화해야 합니다.

관리자 계정의 동작 그래프에서 초대된 멤버 계정을 제거할 수 있습니다. Detective는 멤버 계정 전체의 데이터를 집계하는 동작 그래프에서 기존 데이터를 제거하지 않습니다.

내용

동작 그래프에 개별 계정 초대

동작 그래프에 데이터를 제공하도록 초대할 멤버 계정을 수동으로 지정할 수 있습니다.

Console

Detective 콘솔을 사용하여 초대할 멤버 계정을 수동으로 선택합니다.

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 작업을 선택합니다. 그런 당므 계정 초대를 선택합니다.
4. 계정 추가에서 개별 계정 추가를 선택합니다.
5. 초대 목록에 멤버 계정을 추가하려면 다음 단계를 수행합니다.

   a. 계정 추가를 선택합니다.

   b. AWS 계정 ID에 AWS 계정 ID를 입력합니다.

   c. 이메일 주소에 계정의 루트 사용자 이메일 주소를 입력합니다.
6. 목록에서 계정을 제거하려면 해당 계정에 대해 제거를 선택합니다.
7. 초대 이메일 개인화에서 초대 이메일에 포함할 사용자 지정 콘텐츠를 추가합니다.

   예를 들어 이 영역을 사용하여 연락처 정보를 제공할 수 있습니다. 또는 이를 사용하여 멤버 계정에 필요한 IAM 정책을 사용자 또는 역할에 연결해야 초대를 수락할 수 있음을 알릴 수 있습니다.
8. 멤버 계정 IAM 정책에는 멤버 계정에 필요한 IAM 정책 텍스트가 포함되어 있습니다. 이메일 초대에는 이 정책 텍스트가 포함되어 있습니다. 정책 텍스트를 복사하려면 복사를 선택합니다.
9. 초대를 선택합니다.

Detective API/AWS CLI

Detective API 또는를 사용하여 멤버 계정을 초대 AWS Command Line Interface 하여 동작 그래프에 데이터를 제공할 수 있습니다. 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

멤버 계정을 동작 그래프에 초대하려면(Detective API, AWS CLI)

- Detective API: `CreateMembers` 작업을 사용합니다. 그래프 ARN을 제공해야 합니다. 각 계정에 대해 계정 식별자와 루트 사용자 이메일 주소를 지정합니다.

  멤버 계정에 초대 이메일을 보내지 않으려면 `DisableEmailNotification`을 true로 설정합니다. 기본적으로 `DisableEmailNotification`은 false입니다.

초대 이메일을 보내는 경우 초대 이메일에 추가할 사용자 지정 텍스트를 선택적으로 제공할 수 있습니다.

- AWS CLI: 명령줄에서 `create-members` 명령을 실행합니다.

```
aws detective create-members --accounts AccountId=<AWS account
 ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --
message "<Custom message text>"
```

예제

```
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."
```

멤버 계정에 초대 이메일을 보내지 않도록 지정하려면 `--disable-email-notification`을 포함합니다.

```
aws detective create-members --accounts AccountId=<AWS account
 ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --
disable-email-notification
```

예제

```
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
```

동작 그래프에 멤버 계정 목록 초대

Detective 콘솔에서 동작 그래프에 초대할 멤버 계정 목록이 포함된 `.csv` 파일을 제공할 수 있습니다.

파일의 첫 번째 행은 헤더 행입니다. 그러면 각 계정이 별도의 행에 나열됩니다. 각 멤버 계정 항목에는 AWS 계정 ID와 계정의 루트 사용자 이메일 주소가 포함됩니다.

예제:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

계정 상태가 확인 실패가 아닌 한 Detective는 파일을 처리할 때 이미 초대된 계정을 무시합니다. 이 상태는 계정에 제공된 이메일 주소가 계정의 루트 사용자 이메일 주소와 일치하지 않았음을 나타냅니다. 이 경우 Detective는 원래 초대장을 삭제하고 이메일 주소를 확인하고 초대장을 보내려고 다시 시도합니다.

이 옵션은 계정 목록을 생성하는 데 사용할 수 있는 템플릿도 제공합니다.

.csv 목록에서 멤버 계정 초대(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 작업을 선택합니다. 그런 당므 계정 초대를 선택합니다.
4. 계정 추가에서 .csv에서 추가를 선택합니다.
5. 작업할 템플릿 파일을 다운로드하려면 .csv 템플릿 다운로드를 선택합니다.
6. 계정 목록이 포함된 파일을 선택하려면 .csv 파일 선택을 선택합니다.
7. 멤버 계정 검토에서 Detective가 파일에서 찾은 멤버 계정 목록을 확인합니다.
8. 초대 이메일 개인화에서 초대 이메일에 포함할 사용자 지정 콘텐츠를 추가합니다.

   예를 들어 연락처 정보를 제공하거나 멤버 계정에 필요한 IAM 정책을 상기시킬 수 있습니다.
9. 멤버 계정 IAM 정책에는 멤버 계정에 필요한 IAM 정책 텍스트가 포함되어 있습니다. 이메일 초대에는 이 정책 텍스트가 포함되어 있습니다. 정책 텍스트를 복사하려면 복사를 선택합니다.
10. 초대를 선택합니다.

리전 간 멤버 계정 목록 추가

Detective는 GitHub에서 다음을 수행할 수 있는 오픈 소스 Python 스크립트를 제공합니다.

- 지정된 리전 목록 전반에서 관리자 계정의 동작 그래프에 지정된 멤버 계정 목록을 추가합니다.

- 관리자 계정의 리전에 동작 그래프가 없는 경우 스크립트는 또한 Detective를 활성화하고 해당 리전에 동작 그래프를 생성합니다.
- 멤버 계정에 초대 이메일을 전송합니다.
- 멤버 계정에 대한 초대를 자동으로 수락합니다.

GitHub 스크립트를 구성하고 사용하는 방법에 대한 자세한 내용은 the section called “Amazon Detective Python 스크립트” 섹션을 참조하세요.

활성화되지 않은 멤버 계정 활성화

멤버 계정이 초대를 수락하면 Amazon Detective는 멤버 계정 수를 확인합니다. 동작 그래프의 최대 멤버 계정 수는 1,200개입니다. 동작 그래프에 이미 1,200개의 멤버 계정이 있는 경우 새 계정을 활성화할 수 없습니다. Detective에서 멤버 계정을 활성화할 수 없는 경우 멤버 계정 상태를 활성화되지 않음으로 설정합니다.

활성화되지 않음 상태의 멤버 계정은 동작 그래프에 데이터를 제공하지 않습니다.

Detective는 동작 그래프가 계정을 수용할 수 있도록 계정을 자동으로 활성화합니다.

활성화되지 않음 상태의 멤버 계정을 수동으로 활성화할 수도 있습니다. 예를 들어 기존 멤버 계정을 제거하여 데이터 볼륨을 줄일 수 있습니다. 계정이 활성화되는 자동 프로세스를 기다리는 대신 활성화되지 않음 상태의 멤버 계정을 활성화해 볼 수 있습니다.

Console

멤버 계정 목록에는 활성화되지 않음 상태의 멤버 계정을 선택하여 활성화할 수 있는 옵션이 포함되어 있습니다.

활성화되지 않은 멤버 계정 활성화

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 내 멤버 계정에서 활성화할 각 멤버 계정의 확인란을 선택합니다.

   활성화되지 않음 상태인 멤버 계정만 활성화할 수 있습니다.
4. 계정 활성화를 선택합니다.

Detective는 멤버 계정을 활성화할 수 있는지 여부를 결정합니다. 멤버 계정을 활성화할 수 있는 경우 상태가 활성화됨으로 변경됩니다.

Detective API/CLI

API 호출 또는를 사용하여 활성화되지 않은 단일 멤버 계정을 활성화 AWS Command Line Interface 할 수 있습니다. 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

활성화되지 않은 멤버 계정 활성화

- Detective API: `StartMonitoringMember` API 작업을 사용합니다. 동작 그래프 ARN을 제공해야 합니다. 멤버 계정을 식별하려면 AWS 계정 식별자를 사용합니다.
- AWS CLI: `start-monitoring-member` 명령을 실행합니다.

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account
 ID>
```

예제:

```
start-monitoring-member --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --account-id 444455556666
```

동작 그래프에서 멤버 계정 제거

관리자 계정은 언제든지 동작 그래프에서 초대된 멤버 계정을 제거할 수 있습니다.

Detective는 AWS GovCloud(미국 동부) 및 AWS GovCloud(미국 서부) 리전을 AWS제외하고 종료된 멤버 계정을 자동으로 제거합니다.

초대된 멤버 계정이 동작 그래프에서 제거되면 다음과 같은 상황이 발생합니다.

- 멤버 계정이 내 멤버 계정에서 제거됩니다.
- Amazon Detective는 제거된 계정의 데이터 수집을 중단합니다.

Detective는 멤버 계정 전체의 데이터를 집계하는 동작 그래프에서 기존 데이터를 제거하지 않습니다.

Console

AWS Management Console 를 사용하여 동작 그래프에서 초대된 멤버 계정을 제거할 수 있습니다.

멤버 계정 제거(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 계정 목록에서 제거할 각 멤버 계정의 확인란을 선택합니다.

   목록에서 자신의 계정은 제거할 수 없습니다.
4. 작업을 선택합니다. 그런 다음 계정 비활성화를 선택합니다.

Detective API/CLI

Detective API 또는 AWS Command Line Interface 를 사용하여 동작 그래프에서 초대된 멤버 계정을 제거할 수 있습니다. 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

동작 그래프에서 초대된 멤버 계정을 제거하려면(Detective API, AWS CLI)

- Detective API: `DeleteMembers` 작업을 사용합니다. 그래프 ARN 및 제거할 멤버 계정의 계정 식별자 목록을 지정합니다.
- AWS CLI: 명령줄에서 `delete-members` 명령을 실행합니다.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

예제:

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Python script

Detective는 GitHub에서 오픈 소스 스크립트를 제공합니다. 이 스크립트를 사용하여 지정된 리전 목록에 대한 관리자 계정의 동작 그래프에서 지정된 멤버 계정 목록을 제거할 수 있습니다.

GitHub 스크립트를 구성하고 사용하는 방법에 대한 자세한 내용은 the section called “Amazon Detective Python 스크립트” 섹션을 참조하세요.

멤버 계정의 경우: 동작 그래프 초대 및 멤버십 관리

Amazon Detective는 기여하는 각 동작 그래프에 대해 수집된 데이터에 대해 각 멤버 계정에 요금을 부과합니다.

계정 관리 페이지에서는 멤버 계정이 자신이 속한 동작 그래프의 관리자 계정을 볼 수 있습니다.

동작 그래프에 초대된 멤버 계정은 초대를 보고 초대에 응답할 수 있습니다. 동작 그래프에서 계정을 제거할 수도 있습니다.

조직 동작 그래프의 경우 조직 계정은 해당 계정이 멤버 계정인지 여부를 제어할 수 없습니다. Detective 관리자 계정은 멤버 계정으로 활성화하거나 비활성화할 조직 계정을 선택합니다.

내용

멤버 계정의 필수 IAM 정책

멤버 계정에서 초대를 보고 관리하려면 먼저 필수 IAM 정책을 보안 주체에 연결해야 합니다. 보안 주체는 기존 사용자 또는 역할일 수도 있고, Detective에 사용할 새 사용자 또는 역할을 만들 수도 있습니다.

관리자 계정에 IAM 관리자가 필수 정책을 연결하도록 하는 것이 가장 좋습니다.

멤버 계정 IAM 정책은 Amazon Detective에서의 멤버 계정 작업에 대한 액세스 권한을 부여합니다. 동작 그래프에 기여하라는 이메일 초대장에는 해당 IAM 정책의 텍스트가 포함되어 있습니다.

이 정책을 사용하려면 *<behavior graph ARN>*을 그래프 ARN으로 대체합니다.

JSON

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

```
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "arn:aws:detective:us-east-1:123456789012:graph/*"
    },
   {
    "Effect":"Allow",
    "Action":[
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

단, 조직 동작 그래프의 조직 계정은 초대를 받지 않으므로 조직 동작 그래프에서 해당 계정을 분리할 수 없습니다. 다른 동작 그래프에 속하지 않는 경우에는 `ListInvitations` 권한만 있으면 됩니다. `ListInvitations`는 동작 그래프의 관리자 계정을 볼 수 있습니다. 초대를 관리하고 멤버십을 분리할 수 있는 권한은 초대를 통한 멤버십에만 적용됩니다.

동작 그래프 초대 목록 보기

Amazon Detective 콘솔, Detective API 또는 AWS Command Line Interface멤버 계정에서 동작 그래프 초대를 볼 수 있습니다.

동작 그래프 초대 보기(콘솔)

에서 동작 그래프 초대를 볼 수 있습니다 AWS Management Console.

동작 그래프 초대 보기(콘솔)

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.

계정 관리 페이지의 내 관리자 계정에는 현재 리전에서 열려 있고 수락된 동작 그래프 초대가 포함되어 있습니다. 조직 계정의 경우 내 관리자 계정에는 조직 동작 그래프도 포함됩니다.

계정이 현재 무료 평가 기간 중이면 이 페이지에 무료 평가판 사용 기간이 남은 일수도 표시됩니다.

이 목록에는 거부한 초대, 탈퇴된 멤버십 또는 관리자 계정으로 제거된 멤버십이 포함되어 있지 않습니다.

각 초대에는 관리자 계정 번호, 초대를 수락한 날짜, 초대의 현재 상태가 표시됩니다.

- 응답하지 않은 초대의 경우 상태는 초대됨으로 표시됩니다.
- 수락한 초대의 상태는 활성화됨 또는 활성화되지 않음입니다.

  상태가 활성화됨 경우 계정이 동작 그래프에 데이터를 재공하는 것입니다.

  상태가 비활성화됨 경우 계정은 동작 그래프에 데이터를 제공하지 않습니다.

  처음에는 계정 상태가 활성화되지 않음으로 설정되지만, Detective는 GuardDuty를 활성화했는지 여부 및 활성화된 경우 사용자 계정으로 인해 동작 그래프의 데이터 볼륨이 Detective 할당량을 초과하는지 여부를 확인합니다.

  사용자 계정으로 인해 동작 그래프가 할당량을 초과하지 않는 경우 Detective는 계정 상태를 활성화됨으로 업데이트합니다. 그렇지 않으면 상태가 활성화되지 않음으로 유지됩니다.

  동작 그래프가 계정의 데이터 볼륨을 수용할 수 있게 되면 Detective는 자동으로 해당 그래프를 활성화됨으로 업데이트합니다. 예를 들어 관리자 계정은 계정을 활성화하기 위해 다른 멤버 계정을 제거할 수 있습니다. 관리자 계정은 계정을 수동으로 활성화할 수도 있습니다.

동작 그래프 초대 보기(Detective API, AWS CLI)

Detective API 또는 AWS Command Line Interface에서 동작 그래프 초대를 나열할 수 있습니다.

동작 그래프에 대한 열린 초대 및 수락된 초대 목록을 검색하려면(Detective API, AWS CLI)

- Detective API: `ListInvitations` 작업을 사용합니다.
- AWS CLI: 명령줄에서 `list-invitations` 명령을 실행합니다.

```
aws detective list-invitations
```

동작 그래프 초대에 응답

초대를 수락하면 Detective는 멤버 계정 수를 확인합니다. 동작 그래프의 최대 멤버 계정 수는 1,200개입니다. 동작 그래프에 이미 1,200개의 멤버 계정이 있는 경우 새 계정을 활성화할 수 없습니다.

초대를 수락하면 계정에서 Detective가 활성화됩니다. Detective는 데이터 볼륨이 Detective 할당량 내에 있는지 확인합니다. 동작 그래프에 입력되는 데이터의 볼륨은 Detective에서 허용하는 최대값보다 작아야 합니다. 현재 수집된 볼륨이 일일 10TB 제한을 초과하는 경우 계정을 더 추가할 수 없으며 Detective는 데이터 추가 수집을 비활성화합니다. Detective 콘솔에 데이터 볼륨이 너무 크고 상태가 활성화되지 않음으로 유지됨을 나타내는 알림이 표시됩니다.

초대를 거부하면 초대 목록에서 제거되며 Detective는 동작 그래프에서 계정 데이터를 사용하지 않습니다.

동작 그래프 초대에 응답(콘솔)

AWS Management Console 를 사용하여 Detective 콘솔에 대한 링크가 포함된 이메일 초대에 응답할 수 있습니다. 초대됨 상태인 초대에만 응답할 수 있습니다.

동작 그래프 초대에 응답(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 내 관리자 계정에서 초대를 수락하고 동작 그래프에 데이터를 제공하기 시작하려면 초대 수락을 선택합니다.

   초대를 거절하고 목록에서 제거하려면 거절을 선택합니다.

동작 그래프 초대에 응답(Detective API, AWS CLI)

Detective API 또는 AWS Command Line Interface에서 동작 그래프 초대에 응답할 수 있습니다.

동작 그래프 초대를 수락하려면(Detective API, AWS CLI)

- Detective API: `AcceptInvitation` 작업을 사용합니다. 그래프 ARN을 지정해야 합니다.
- AWS CLI: 명령줄에서 `accept-invitation` 명령을 실행합니다.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

예제:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

동작 그래프 초대를 거부하려면(Detective API, AWS CLI)

- Detective API: RejectInvitation 작업을 사용합니다. 그래프 ARN을 지정해야 합니다.
- AWS CLI: 명령줄에서 reject-invitation 명령을 실행합니다.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

예제:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

동작 그래프에서 계정 제거

초대를 수락한 후에는 언제든지 동작 그래프에서 계정을 제거할 수 있습니다. 동작 그래프에서 계정을 제거하면 Amazon Detective는 계정에서 동작 그래프로 데이터를 수집하는 것을 중지합니다. 기존 데이터는 동작 그래프에 그대로 남아 있습니다.

초대된 계정만 동작 그래프에서 계정을 제거할 수 있습니다. 조직 계정은 조직 동작 그래프에서 해당 계정을 제거할 수 없습니다.

동작 그래프에서 계정 제거(콘솔)

AWS Management Console 를 사용하여 동작 그래프에서 계정을 제거할 수 있습니다.

동작 그래프에서 계정 제거(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 내 관리자 계정에서 탈퇴하려는 동작 그래프에 대해 탈퇴를 선택합니다.

동작 그래프에서 계정 제거(Detective API, AWS CLI)

Detective API 또는 AWS Command Line Interface 를 사용하여 동작 그래프에서 계정을 제거할 수 있습니다.

동작 그래프에서 계정을 제거하려면(Detective API, AWS CLI)

- Detective API: `DisassociateMembership` 작업을 사용합니다. 그래프 ARN을 지정해야 합니다.
- AWS CLI: 명령줄에서 `disassociate-membership` 명령을 실행합니다.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

예제:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

계정 활동이 동작 그래프에 미치는 영향

이러한 업은 Amazon Detective 데이터 및 액세스에 다음과 같은 영향을 미칩니다.

Detective 비활성화

관리자 계정이 Detective를 비활성화하면 다음과 같은 상황이 발생합니다.

- 동작 그래프가 삭제됩니다.
- Detective는 관리자 계정 및 해당 동작 그래프의 멤버 계정에서 데이터 수집을 중단합니다.

동작 그래프에서 멤버 계정이 제거됩니다.

멤버 계정이 동작 그래프에서 제거되면 Detective는 해당 계정의 데이터 수집을 중단합니다.

동작 그래프의 기존 데이터는 영향을 받지 않습니다.

초대된 계정의 경우 해당 계정이 내 멤버 계정 목록에서 제거됩니다.

조직 동작 그래프에서 조직 계정의 경우 계정 상태가 멤버 아님으로 변경됩니다.

멤버 계정이 조직을 떠남

멤버 계정이 조직을 떠나면 다음과 같은 상황이 발생합니다.

- 해당 계정이 조직 동작 그래프의 내 멤버 계정 목록에서 제거됩니다.
- Detective는 해당 계정의 데이터 수집을 중단합니다.

동작 그래프의 기존 데이터는 영향을 받지 않습니다.

AWS 계정이 일시 중지됨

관리자 계정이 일시 중지되면 AWS계정은 Detective에서 동작 그래프를 볼 수 있는 권한을 잃게 됩니다. Detective는 동작 그래프에 데이터를 수집하는 것을 중단합니다.

멤버 계정이 일시 중지되면 AWS Detective는 해당 계정에 대한 데이터 수집을 중지합니다.

90일이 지나면 계정이 해지되거나 다시 활성화됩니다. 관리자 계정이 다시 활성화되면 Detective 권한이 복원됩니다. Detective는 계정에서 데이터 수집을 재개합니다. 멤버 계정이 다시 활성화되면 Detective는 계정에서 데이터 수집을 재개합니다.

AWS 계정 해지

AWS 계정이 해지되면 Detective는 해지에 다음과 같이 응답합니다.

- 관리자 계정의 경우 Detective는 동작 그래프를 삭제합니다.
- 멤버 계정의 경우 Detective는 해당 계정을 동작 그래프에서 제거합니다.

AWS 는 관리자 계정 해지 발효일로부터 90일 동안 계정의 정책 데이터를 보관합니다. 90일 기간이 끝나면는 계정의 모든 정책 데이터를 AWS 영구적으로 삭제합니다.

- 정책을 보관하면 결과를 90일 넘게 유지할 수 있습니다. 또한 EventBridge 규칙에 사용자 지정 작업을 사용하여 결과를 S3 버킷에 저장할 수 있습니다.
- 가 정책 데이터를 AWS 보존하는 한, 해지된 계정을 다시 열면는 해당 계정을 서비스 관리자로 AWS 재할당하고 계정에 대한 서비스 정책 데이터를 복구합니다.
- 자세한 내용은 계정 해지를 참조하십시오.

> **Important**
>
> AWS GovCloud (US) 리전의 고객:
>
> - 계정을 해지하기 전에 계정 리소스를 백업한 다음 삭제합니다. 계정을 해지한 뒤에는 더 이상 해당 계정에 액세스할 수 없습니다.

Detective Python 스크립트를 사용하여 계정 관리

Amazon Detective는 GitHub 리포지토리 amazon-detective-multiaccount-scripts에서 오픈 소스 Python 스크립트 세트를 제공합니다. 스크립트에는 Python 3이 필요합니다.

이를 사용하여 다음 작업을 수행할 수 있습니다.

- 여러 리전의 관리자 계정에 대해 Detective를 활성화합니다.

  Detective를 활성화하면 동작 그래프에 태그 값을 할당할 수 있습니다.
- 리전별 관리자 계정의 동작 그래프에 멤버 계정을 추가합니다.
- 선택적으로 멤버 계정에 초대 이메일을 보낼 수 있습니다. 초대 이메일을 보내지 않도록 요청을 구성할 수도 있습니다.
- 관리자 계정의 리전별 동작 그래프에서 멤버 계정을 제거합니다.
- 여러 리전의 관리자 계정에 대해 Detective를 비활성화합니다. 관리자 계정이 Detective를 비활성화하면 각 리전의 관리자 계정 동작 그래프가 비활성화됩니다.

`enableDetective.py` 스크립트 개요

`enableDetective.py` 스크립트는 다음 작업을 수행합니다.

1. 지정된 각 리전의 관리자 계정에 Detective가 아직 활성화되어 있지 않은 경우, 해당 리전의 관리자 계정에 대해 Detective를 활성화합니다.

   스크립트를 사용하여 Detective를 활성화하면 동작 그래프에 태그 값을 할당할 수 있습니다.
2. 선택적으로 관리자 계정에서 각 동작 그래프의 지정된 멤버 계정으로 초대를 보냅니다.

   초대 이메일 메시지는 기본 메시지 콘텐츠를 사용하며 사용자 지정할 수 없습니다.

   초대 이메일을 보내지 않도록 요청을 구성할 수도 있습니다.

3. 멤버 계정에 대한 초대를 자동으로 수락합니다.

   스크립트가 초대를 자동으로 수락하므로 멤버 계정은 이러한 메시지를 무시할 수 있습니다.

   초대가 자동으로 수락된다는 사실을 멤버 계정에 직접 문의하여 알리는 것이 좋습니다.

`disableDetective.py` 스크립트 개요

`disableDetective.py` 스크립트는 지정된 리전의 관리자 계정 동작 그래프에서 지정된 멤버 계정을 삭제합니다.

또한 지정된 리전의 관리자 계정에 대해 Detective를 비활성화하는 옵션도 제공합니다.

스트립트에 필요한 권한

스크립트에는 관리자 계정과 추가하거나 제거하는 모든 멤버 계정에 기존 AWS 역할이 필요합니다.

> **Note**
>
> 역할 이름은 모든 계정에서 동일해야 합니다.

IAM 정책에서 권장하는 모범 사례는 범위가 가장 적은 역할을 사용하는 것입니다. 그래프 생성, 멤버 생성, 그래프에 멤버 추가 등의 스크립트 워크플로를 실행하려면 다음과 같은 권한이 필요합니다.

- detective:CreateGraph
- detective:CreateMembers
- detective:DeleteGraph
- detective:DeleteMembers
- detective:ListGraphs
- detective:ListMembers
- detective:AcceptInvitation

역할 신뢰 관계

역할 신뢰 관계를 통해 인스턴스 또는 로컬 보안 인증 정보가 역할을 맡을 수 있어야 합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/john_doe"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

필수 권한이 포함된 공통 역할이 없는 경우 각 멤버 계정에서 최소한 해당 권한을 가진 역할을 만들어야 합니다. 또한 관리자 계정에서 역할을 만들어야 합니다.

역할을 생성하는 경우 다음을 수행해야 합니다.

- 모든 계정에서 동일한 역할 이름을 사용합니다.
- 위의 필수 권한을 추가하거나(권장) AmazonDetectiveFullAccess 관리형 정책을 선택합니다.
- 위에서 설명한 대로 역할 신뢰 관계 블록을 추가합니다.

이 프로세스를 자동화하려면 `EnableDetective.yaml` CloudFormation 템플릿을 사용할 수 있습니다. 템플릿은 글로벌 리소스만 생성하므로 모든 리전에서 실행할 수 있습니다.

Python 스크립트를 위한 실행 환경 설정

EC2 인스턴스 또는 로컬 시스템에서 스크립트를 실행할 수 있습니다.

EC2 인스턴스 시작 및 구성

스크립트를 실행하는 한 가지 옵션은 EC2 인스턴스에서 스크립트를 실행하는 것입니다.

EC2 인스턴스 시작 및 구성

1. 관리자 계정에서 EC2 인스턴스를 시작합니다. EC2 인스턴스를 시작하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 Linux 인스턴스 시작하기를 참조하세요. Amazon EC2
2. 인스턴스가 관리자 계정 `AssumeRole` 내에서 호출할 수 있도록 허용하는 권한이 있는 IAM 역할을 인스턴스에 연결합니다.

   `EnableDetective.yaml` CloudFormation 템플릿을 사용한 경우 이름이 인 프로파일이 있는 인스턴스 역할이 생성`EnableDetective`되었습니다.

   또는 인스턴스 역할 생성에 대한 자세한 내용은 EC2 콘솔을 사용하여 기존 EC2 인스턴스에 IAM 역할을 쉽게 교체 또는 연결 블로그 게시물을 참조하세요.
3. 필수 소프트웨어 설치:
   - APT: `sudo apt-get -y install python3-pip python3 git`
   - RPM: `sudo yum -y install python3-pip python3 git`
   - Boto(최소 버전 1.15): `sudo pip install boto3`
4. 리포지토리를 EC2 인스턴스에 복제합니다.

   ```
   git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
   ```

스크립트를 실행하도록 로컬 시스템 구성

로컬 시스템에서 스크립트를 실행할 수도 있습니다.

스크립트를 실행하도록 로컬 시스템 구성

1. `AssumeRole` 호출 권한이 있는 관리자 계정의 로컬 시스템 보안 인증 정보를 설정했는지 확인합니다.
2. 필수 소프트웨어 설치:
   - Python 3
   - Boto(최소 버전 1.15)
   - GitHub 스크립트

플랫폼	설치 지침
Windows	1. Python 3(https://www.python.org/downloads/windows/)을 설치합니다. 2. 명령 프롬프트를 엽니다. 3. Boto를 설치하려면 `pip install boto3`을 실행합니다. 4. GitHub(https://github.com/aws-samples/amazon-detective-multiaccount-scripts)에서 스크립트 소스 코드를 다운로드합니다.
Mac	1. Python 3(https://www.python.org/downloads/mac-osx/)을 설치합니다. 2. 명령 프롬프트를 엽니다. 3. Boto를 설치하려면 `pip install boto3`을 실행합니다. 4. GitHub(https://github.com/aws-samples/amazon-detective-multiaccount-scripts)에서 스크립트 소스 코드를 다운로드합니다.
Linux	1. Python 3를 설치하려면 다음 중 하나를 실행합니다. • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. Boto를 설치하려면 `sudo pip install boto3`을 실행합니다. 3. https://github.com/aws-samples/amazon-detective-multiaccount-scripts에서 스크립트 소스 코드를 복제합니다.

추가 또는 제거할 멤버 계정 `.csv` 목록 생성

동작 그래프에 추가하거나 동작 그래프에서 제거할 멤버 계정을 식별하려면 계정 목록이 포함된 `.csv` 파일을 제공합니다.

각 계정을 별도의 줄에 나열합니다. 각 멤버 계정 항목에는 AWS 계정 ID와 계정의 루트 사용자 이메일 주소가 포함됩니다.

다음 예를 참조하세요.

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

enableDetective.py 실행

EC2 인스턴스 또는 로컬 시스템에서 enableDetective.py 스크립트를 실행할 수 있습니다.

enableDetective.py를 실행하려면

1. .csv 파일을 EC2 인스턴스 또는 로컬 시스템의 amazon-detective-multiaccount-scripts 디렉터리에 복사합니다.
2. 디렉터리를 amazon-detective-multiaccount-scripts로 변경합니다.
3. enableDetective.py 스크립트 실행.

   ```
   enableDetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
   disable_email
   ```

스크립트를 실행할 때 다음 값을 바꿉니다.

administratorAccountID

관리자 AWS 계정의 계정 ID입니다.

roleName

관리자 계정 및 각 멤버 계정에서 수임할 AWS 역할의 이름입니다.

inputFileName

관리자 계정의 동작 그래프에 추가할 멤버 계정 목록이 들어 있는 .csv 파일 이름.

tagValueList

(선택 사항) 새 동작 그래프에 할당할 쉼표로 구분된 태그 값 목록.

각 태그 값의 형식은 *key*=*value*입니다. 예제:

```
--tags Department=Finance,Geo=Americas
```

regionList

(선택 사항) 관리자 계정의 동작 그래프에 멤버 계정을 추가할 리전의 쉼표로 구분된 목록입니다. 예제:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

관리자 계정의 경우 리전에서 Detective를 아직 활성화하지 않았을 수 있습니다. 이 경우 스크립트는 Detective를 활성화하고 관리자 계정을 위한 새 동작 그래프를 생성합니다.

리전 목록을 제공하지 않는 경우 스크립트는 Detective가 지원하는 모든 리전에서 작동합니다.

`--disable_email`

(선택 사항) 포함된 경우 Detective는 멤버 계정에 초대 이메일을 보내지 않습니다.

disableDetective.py 실행

EC2 인스턴스 또는 로컬 시스템에서 disableDetective.py 스크립트를 실행할 수 있습니다.

disableDetective.py를 실행하려면

1. .csv 파일을 amazon-detective-multiaccount-scripts 디렉터리로 복사합니다.
2. .csv 파일을 사용하여 지정된 리전 목록에 대한 관리자 계정의 동작 그래프에서 나열된 멤버 계정을 삭제하려면 다음과 같이 disableDetective.py 스크립트를 실행합니다.

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --disabled_regions regionList
```

3. 모든 리전의 관리자 계정에 대해 Detective를 비활성화하려면 --delete-master 플래그를 사용하여 disableDetective.py 스크립트를 실행합니다.

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --disabled_regions regionList --delete_master
```

스크립트를 실행할 때 다음 값을 바꿉니다.

administratorAccountID

관리자 AWS 계정의 계정 ID입니다.

roleName

관리자 계정 및 각 멤버 계정에서 수임할 AWS 역할의 이름입니다.

inputFileName

관리자 계정의 동작 그래프에서 제거할 멤버 계정 목록이 들어 있는 `.csv` 파일 이름.

Detective를 비활성화한 경우에도 `.csv` 파일을 제공해야 합니다.

regionList

(선택 사항) 다음 중 하나를 수행할 수 있는 쉼표로 구분된 리전 목록입니다.

- 관리자 계정의 동작 그래프에서 멤버 계정을 제거합니다.
- `--delete-master` 플래그가 포함된 경우 Detective를 비활성화합니다.

예제:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

리전 목록을 제공하지 않는 경우 스크립트는 Detective가 지원하는 모든 리전에서 작동합니다.

Amazon Security Lake와 Amazon Detective 통합

Amazon Security Lake는 완전 관리형 보안 데이터 레이크 서비스입니다. Security Lake를 사용하여 AWS 환경, SaaS 공급자, 온프레미스 소스, 클라우드 소스 및 타사 소스의 보안 데이터를 AWS 계정에 저장된 전용 데이터 레이크로 자동으로 중앙 집중화할 수 있습니다. Security Lake를 사용하면 보안 데이터를 분석할 수 있으므로 조직 전체의 보안 상태를 더 완벽하게 이해할 수 있습니다. Security Lake를 사용하면 워크로드, 애플리케이션 및 데이터에 대한 보호도 개선할 수 있습니다.

Amazon Detective는 Security Lake와 통합되어 Security Lake에 저장된 원시 로그 데이터를 쿼리하고 검색할 수 있습니다.

이 통합을 사용하면 Security Lake에서 기본적으로 지원하는 다음 소스에서 로그와 이벤트를 수집할 수 있습니다. Detective는 최대 소스 버전 2(OCSF 1.1.0)를 지원합니다.

- AWS CloudTrail 관리 이벤트 버전 1.0 이상
- Amazon Virtual Private Cloud(Amazon VPC) 흐름 로그 버전 1.0 이상
- Amazon Elastic Kubernetes Service(Amazon EKS) 감사 로그 버전 2.0. - Amazon EKS 감사 로그를 소스로 사용하려면 IAM 권한`ram:ListResources`에를 추가해야 합니다. 자세한 내용은 계정에 필요한 IAM 권한 추가를 참조하세요.

Security Lake가 기본적으로 지원되는 AWS 서비스에서 OCSF 스키마로 오는 로그 및 이벤트를 자동으로 변환하는 방법에 대한 자세한 내용은 Amazon Security Lake 사용 설명서를 참조하세요.

Detective를 Security Lake와 통합한 후 Detective는 AWS CloudTrail 관리 이벤트 및 Amazon VPC 흐름 로그와 관련하여 Security Lake에서 원시 로그를 가져오기 시작합니다. 자세한 내용은 원시 로그 쿼리를 참조하세요.

Security Lake와의 Detective 통합 활성화

Detective를 Security Lake와 통합하려면 다음 단계를 완료해야 합니다.

1. 시작하기 전에

   Organizations 관리 계정을 사용하여 조직에 대한 위임된 Security Lake 관리자를 지정해야 합니다. Security Lake가 활성화되어 있는지 확인하고 Security Lake가 AWS CloudTrail 관리 이벤트 및 Amazon Virtual Private Cloud(VPC) 흐름 로그에서 로그와 이벤트를 수집하고 있는지 확인합니다.

보안 참조 아키텍처에 따라 Detective는 로그 아카이브 계정을 사용하고 Security Lake 배포를 위해 Security Tooling 계정 사용을 연기할 것을 권장합니다.

2. Security Lake 구독자 생성

   Amazon Security Lake의 로그와 이벤트를 사용하려면 Security Lake 구독자여야 합니다. Detective 계정 관리자에게 쿼리 액세스 권한을 부여하려면 다음 단계를 따르세요.

3. IAM 자격 증명에 필요한 AWS Identity and Access Management (IAM) 권한 추가.
   - 다음 권한을 추가하여 Security Lake와의 Detective 통합을 생성합니다.
     - 이러한 AWS Identity and Access Management(IAM) 권한을 IAM 자격 증명에 연결합니다. 자세한 내용은 계정에 필요한 IAM 권한 추가 섹션을 참조하세요.
     - CloudFormation 서비스 역할을 전달하는 데 사용할 IAM 보안 주체에이 IAM 정책을 추가합니다. 자세한 내용은 IAM 보안 주체에 권한 추가 섹션을 참조하세요.
   - Detective를 Security Lake와 이미 통합한 경우 통합을 사용하려면 이러한 (IAM) 권한을 IAM 자격 증명에 연결합니다. 자세한 내용은 계정에 필요한 IAM 권한 추가 섹션을 참조하세요.
4. 리소스 공유 ARN 초대 수락 및 통합 활성화

AWS CloudFormation 템플릿을 사용하여 Security Lake 구독자의 쿼리 액세스를 생성하고 관리하는 데 필요한 파라미터를 설정합니다. 스택을 생성하는 자세한 단계는 AWS CloudFormation 템플릿을 사용하여 스택 생성을 참조하세요. 스택 생성을 완료한 후 통합을 활성화합니다.

Detective 콘솔을 사용하여 Amazon Detective를 Amazon Security Lake와 통합하는 방법에 대한 데모를 보려면 Amazon Detective와 Amazon Security Lake 통합 - 설정 방법--> 비디오를 시청하세요.

Detective를 Security Lake와 통합하기 전에

이 주제에서는 조직의 Security Lake 관리자 위임, Detective 관리자 계정에 Security Lake 활성화, Security Lake가 로그 및 이벤트를 수집하고 있는지 확인하는 등의 예비 단계를 설명합니다.

Security Lake는와 통합되어 조직의 여러 계정에서 로그 수집을 AWS Organizations 관리합니다. 조직에 Security Lake를 사용하려면 먼저 AWS Organizations 관리 계정에서 조직의 위임된 Security Lake 관리자를 지정해야 합니다. 그런 다음 위임된 Security Lake 관리자가 Security Lake를 활성화하고 조직의 멤버 계정에 대한 로그 및 이벤트 수집을 활성화해야 합니다.

Security Lake를 Detective와 통합하기 전에 Detective 관리자 계정에 대해 Security Lake가 활성화되어 있는지 확인합니다. 먼저 Security Lake 콘솔을 사용하여 Security Lake를 활성화하여 데이터 레이크 설정을 구성하고 로그 수집을 설정해야 합니다. Security Lake를 활성화하는 자세한 단계는 Amazon Security Lake 사용 설명서의 시작하기를 참조하세요.

또한 Security Lake가 AWS CloudTrail 관리 이벤트 및 Amazon Virtual Private Cloud(VPC) 흐름 로그에서 로그와 이벤트를 수집하고 있는지 확인합니다. Security Lake의 로그 수집에 대한 자세한 내용은 Amazon Security Lake 사용 설명서의 AWS 서비스에서 데이터 수집을 참조하세요.

1단계: Detective에서 Security Lake 구독자 생성

이 주제에서는 Detective 콘솔을 사용하여 Security Lake 구독자를 생성하는 방법을 설명합니다.

Amazon Security Lake의 로그와 이벤트를 사용하려면 Security Lake 구독자여야 합니다. 구독자는 Security Lake가 수집하는 데이터를 쿼리하고 이에 액세스할 수 있습니다. 쿼리 액세스 권한이 있는 구독자는 Amazon Athena와 같은 서비스를 사용하여 Amazon Simple Storage Service(Amazon S3) 버킷에서 직접 AWS Lake Formation 테이블을 쿼리할 수 있습니다. 구독자가 되려면 Security Lake 관리자가 데이터 레이크를 쿼리할 수 있는 구독자 액세스 권한을 제공해야 합니다. 관리자가 이를 수행하는 방법에 대한 자세한 내용은 Amazon Security Lake 사용 설명서의 쿼리 액세스 권한이 있는 구독자 생성을 참조하세요.

다음 단계에 따라 Detective 관리자 계정에 쿼리 액세스 권한을 부여하기 위해 Security Lake 구독자를 생성합니다.

Security Lake에서 Detective 구독자를 생성하려면

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 통합을 선택합니다.
3. Security Lake 구독자 창에서 계정 ID 및 외부 ID 값을 기록해 둡니다.

   Security Lake 관리자에게 이 ID를 사용하여 다음을 수행하도록 요청합니다.

   - Security Lake에서 Detective 구독자 생성.
   - 구독자가 쿼리 액세스 권한을 갖도록 구성.
   - Lake Formation 권한으로 Security Lake 쿼리 구독자가 생성되었는지 확인하려면 Security Lake 콘솔에서 Lake Formation을 데이터 액세스 방법으로 선택합니다.

   Security Lake 관리자가 구독자를 생성하면 Security Lake에서 Amazon 리소스 공유 ARN을 생성합니다. 관리자에게 이 ARN을 보내달라고 요청합니다.
4. Security Lake 구독자 창에 Security Lake 관리자가 제공한 리소스 공유 ARN을 입력합니다.
5. Security Lake 관리자로부터 리소스 공유 ARN을 받은 후 Security Lake 구독자 창의 리소스 공유 ARN 상자에 ARN을 입력합니다.

2단계: Detective에서 계정에 필요한 IAM 권한 추가

이 주제에서는 IAM 자격 증명에 추가해야 하는 AWS Identity and Access Management (IAM) 권한 정책의 세부 정보를 설명합니다.

Security Lake와의 Detective 통합을 활성화하려면 다음 AWS Identity and Access Management (IAM) 권한 정책을 IAM 자격 증명에 연결해야 합니다.

다음 인라인 정책을 역할에 연결합니다. 자체 Amazon S3 버킷을 사용하여 Athena 쿼리 결과를 저장하려면 `athena-results-bucket`을 Amazon S3 버킷 이름으로 바꿉니다. Detective에서 Amazon S3 버킷을 자동으로 생성하여 Athena 쿼리 결과를 저장하도록 하려면 IAM 정책에서 전체 `S3ObjectPermissions`를 제거합니다.

이 정책을 IAM 자격 증명에 연결하는 데 필요한 권한이 없는 경우 AWS 관리자에게 문의하세요. 필요한 권한이 있지만 문제가 발생하는 경우 IAM 사용 설명서의 액세스 거부 오류 메시지 문제 해결을 참조하세요.

JSON

```
{
    "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:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabases",
                "glue:GetPartitions",
                "glue:GetTable",
                "glue:GetTables"
            ],
            "Resource": [
                "arn:aws:glue:*:123456789012:database/amazon_security_lake*",
                "arn:aws:glue:*:123456789012:table/amazon_security_lake*/
amazon_security_lake*",
                "arn:aws:glue:*:123456789012: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:*:123456789012:parameter/Detective/SLI"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:GetTemplateSummary",
```

```
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "securitylake.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

3단계: 리소스 공유 ARN 초대 수락

이 주제에서는 Security Lake와의 Detective 통합을 활성화하기 전에 필요한 단계인 AWS CloudFormation 템플릿을 사용하여 리소스 공유 ARN 초대를 수락하는 단계를 설명합니다.

Security Lake의 원시 데이터 로그에 액세스하려면 Security Lake 관리자가 생성한 Security Lake 계정의 리소스 공유 초대를 수락해야 합니다. 교차 계정 테이블 공유를 설정할 AWS Lake Formation 권한도 필요합니다. 또한 원시 쿼리 로그를 수신할 수 있는 Amazon Simple Storage Service(S3) 버킷을 생성해야 합니다.

이 다음 단계에서는 AWS CloudFormation 템플릿을 사용하여 리소스 공유 ARN 초대를 수락하고, 필요한 AWS Glue 크롤러 리소스를 생성하고, AWS Lake Formation 관리자 권한을 부여하는 스택을 생성합니다.

리소스 공유 ARN 초대를 수락하고 통합을 활성화하려면

1. CloudFormation 템플릿을 사용하여 CloudFormation 스택을 생성합니다. 자세한 내용은 CloudFormation 템플릿을 사용하여 스택 생성 섹션을 참조하세요.
2. 스택 생성을 완료한 후 통합 활성화를 선택하여 Security Lake와의 Detective 통합을 활성화합니다.

CloudFormation 템플릿을 사용하여 스택 생성

Detective는 Security Lake 구독자의 쿼리 액세스를 생성하고 관리하는 데 필요한 파라미터를 설정하는 데 사용할 수 있는 CloudFormation 템플릿을 제공합니다.

1단계: AWS CloudFormation 서비스 역할 생성

CloudFormation 템플릿을 사용하여 스택을 생성하려면 CloudFormation 서비스 역할을 생성해야 합니다. 서비스 역할을 생성하는 데 필요한 권한이 없는 경우 Detective 관리자 계정의 관리자에게 문의합니다. AWS CloudFormation 서비스 역할에 대한 자세한 내용은 AWS CloudFormation 서비스 역할을 참조하세요.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/iam/ IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택하고 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 선택(Select trusted entity)에서 AWS 서비스(service)를 선택합니다.
4. CloudFormation을 선택합니다. 그리고 다음을 선택합니다.
5. 역할 이름을 입력합니다. 예를 들어 `CFN-DetectiveSecurityLakeIntegration`입니다.
6. 다음 인라인 정책을 역할에 연결합니다. 를 AWS 계정 ID<Account ID>로 바꿉니다.

JSON

```
{
    "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::111122223333:role/*-ResourceShareAcceptorLamb-*",
                 "arn:aws:iam::111122223333:role/*-SsmParametersLambdaRole-*",
                 "arn:aws:iam::111122223333:role/*-GlueDatabaseLambdaRole-*",
                 "arn:aws:iam::111122223333:role/*-GlueTablesLambdaRole-*",
                 "arn:aws:iam::111122223333: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:*:111122223333:function:*"
            ]
        },
        {
            "Sid": "CloudwatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:*:111122223333:log-group:*"
        },
        {
            "Sid": "KmsPermission",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:111122223333:key/*"
        }
    ]
}
```

2단계: IAM 보안 주체에 권한 추가.

이전 단계에서 생성한 CloudFormation 서비스 역할을 사용하여 스택을 생성하려면 다음 권한이 필요합니다. CloudFormation 서비스 역할을 전달하는 데 사용할 IAM 보안 주체에 다음 IAM 정책을 추가합니다. 스택을 생성할 때는 이 IAM 보안 주체를 수임해야 합니다. IAM 정책을 추가하는 데 필요한 권한이 없는 경우 Detective 관리자 계정의 관리자에게 문의합니다.

> **Note**
>
> 다음 정책에서 사용되는 `CFN-DetectiveSecurityLakeIntegration`은 이전 `Creating an AWS CloudFormation 서비스 역할` 단계에서 생성한 역할을 나타냅니다. 이름이 다를 경우 이전 단계에서 입력한 역할 이름으로 변경합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "PassRole",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/CFN-
DetectiveSecurityLakeIntegration"
        },
        {
            "Sid": "RestrictCloudFormationAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:UpdateStack"
            ],
            "Resource": "arn:aws:cloudformation:*:111122223333:stack/*",
            "Condition": {
                "StringEquals": {
                    "cloudformation:RoleArn": [
                        "arn:aws:iam::111122223333:role/CFN-
DetectiveSecurityLakeIntegration"
                    ]
                }
            }
        },
        {
            "Sid": "CloudformationDescribeStack",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:GetStackPolicy"
            ],
            "Resource": "arn:aws:cloudformation:*:111122223333:stack/*"
        },
```

```
        {
            "Sid": "CloudformationListStacks",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:111122223333:log-group:*"
        }
    ]
}
```

3단계: CloudFormation 콘솔에서 사용자 지정 값 지정

1. Detective에서 AWS CloudFormation 콘솔로 이동합니다.
2. (선택 사항) 스택 이름을 입력합니다. 스택 이름은 자동으로 입력됩니다. 스택 이름을 기존 스택 이름과 충돌하지 않는 이름으로 변경할 수 있습니다.
3. 다음 파라미터를 입력합니다.

   - AthenaResultsBucket - 값을 입력하지 않는 경우 이 템플릿은 Amazon S3 버킷을 생성합니다. 자체 버킷을 사용하려면 Athena 쿼리 결과를 저장할 버킷 이름을 입력합니다. 자체 버킷을 사용하는 경우 버킷이 리소스 공유 ARN과 동일한 리전에 있어야 합니다. 자체 버킷을 사용하는 경우 선택한 `LakeFormationPrincipals`에 버킷에서 객체를 쓰고 읽을 수 있는 권한이 있는지 확인하세요. 버킷 권한에 대한 자세한 내용은 Amazon Athena 사용 설명서의 쿼리 결과 및 최근 쿼리를 참조하세요.
   - DTRegion - 이 필드는 미리 채워져 있습니다. 이 필드의 값은 변경하지 마세요.
   - LakeFormationPrincipals - Security Lake 통합을 사용할 수 있는 액세스 권한을 부여하려는 IAM 보안 주체의 ARN(예: IAM 역할 ARN)을 쉼표로 구분하여 입력합니다. 이들은 Detective를 사용하는 보안 분석가 및 보안 엔지니어일 수 있습니다.

     이전에 `Step 2: Add the required IAM permissions to your account]`단계에서 IAM 권한을 연결한 IAM 보안 주체만 사용할 수 있습니다.

- ResourceShareARN - 이 필드는 미리 채워져 있습니다. 이 필드의 값은 변경하지 마세요.

4. 권한

   IAM 역할 - `Creating an AWS CloudFormation Service Role` 단계에서 만든 역할을 선택합니다. 현재 IAM 역할에 `Creating an AWS CloudFormation Service Role` 단계의 필수 권한이 모두 있는 경우 이 필드를 비워 둘 수도 있습니다.

5. 승인 상자를 모두 검토하여 선택한 다음 스택 생성 버튼을 클릭합니다. 자세한 내용은 생성될 다음 IAM 리소스를 검토하세요.

```
* ResourceShareAcceptorCustomResourceFunction
    - ResourceShareAcceptorLambdaRole
    - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
    - SsmParametersLambdaRole
    - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
    - GlueDatabaseLambdaRole
    - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
    - GlueTablesLambdaRole
    - GlueTablesLogsAccessPolicy
```

4단계:의 IAM 보안 주체에 Amazon S3 버킷 정책 추가 **`LakeFormationPrincipals`**

(선택 사항) 이 템플릿이 `AthenaResultsBucket`을 자동으로 생성하도록 하려면 `LakeFormationPrincipals`의 IAM 보안 주체에 다음 정책을 연결해야 합니다.

```
{
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}
```

를 AthenaResultsBucket 이름으로 바꿉 athena-results-bucket 니다.는 AWS CloudFormation 콘솔에서 찾을 AthenaResultsBucket 수 있습니다.

1. https://console.aws.amazon.com/cloudformation CloudFormation 콘솔을 엽니다.
2. 스택을 클릭합니다.
3. 리소스 탭을 클릭합니다.
4. 논리적 ID AthenaResultsBucket을 검색하고 해당 물리적 ID를 복사합니다.

Detective 통합 구성 변경

Detective와 Security Lake를 통합하는 데 사용한 파라미터를 변경하려면 해당 파라미터를 편집한 다음 통합을 다시 활성화할 수 있습니다. 템플릿을 편집 CloudFormation 하여 다음 시나리오에서이 통합을 다시 활성화할 수 있습니다.

- Security Lake 구독을 업데이트하려면 새 구독자를 만들거나 Security Lake 관리자가 기존 구독의 데이터 소스를 업데이트할 수 있습니다.
- 원시 쿼리 로그를 저장할 다른 Amazon S3 버킷을 지정하려면
- 다른 Lake Formation 보안 주체를 다르게 지정하려면

Security Lake와의 Detective 통합을 다시 활성화하면 리소스 공유 ARN을 편집하고 IAM 권한을 볼 수 있습니다. IAM 권한을 편집하려면 Detective에서 IAM 콘솔로 이동할 수 있습니다. CloudFormation 템플릿에 이전에 입력한 값을 편집할 수도 있습니다. 통합을 다시 활성화하려면 기존 CloudFormation 스택을 삭제하고 다시 생성해야 합니다.

Security Lake와의 Detective 통합을 다시 활성화하려면

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 통합을 선택합니다.
3. 다음 단계 중 하나를 사용하여 통합을 편집할 수 있습니다.
   - Security Lake 창에서 편집을 선택합니다.
   - Security Lake 창에서 보기를 선택합니다. 보기 창에서 편집을 선택합니다.
4. 새 리소스 공유 ARN을 입력하여 리전의 데이터 소스에 액세스합니다.
5. 현재 IAM 권한을 확인하고 IAM 권한을 편집하려면 IAM 콘솔로 이동합니다.
6. CloudFormation 템플릿에서 값을 편집합니다.

1. 새 스택을 생성하기 전에 먼저 기존 스택을 삭제합니다. 기존 스택을 삭제하지 않고 동일한 리전에 새 스택을 생성하려고 하면 요청이 실패합니다. 자세한 내용은 CloudFormation 스택 삭제 섹션을 참조하세요.

1. 새 CloudFormation 스택을 생성합니다. 자세한 내용은 CloudFormation 템플릿을 사용하여 스택 생성 섹션을 참조하세요.

7. 통합 활성화를 선택합니다.

Detective를 Security Lake와 통합하는 데 지원되는 AWS 리전

다음 AWS 리전에서 Detective를 Security Lake와 통합할 수 있습니다.

리전 이름	리전	엔드포인트	프로토콜
미국 동부(오하이오)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
미국 동부(버지니아 북부)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
미국 서부(캘리포니아 북부)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS
미국 서부(오레곤)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
아시아 태평양(시드니)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS

리전 이름	리전	엔드포인트	프로토콜
아시아 태평양(도쿄)	ap-northeast-1	securitylake.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	securitylake.ca-central-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

Detective에서 원시 로그 쿼리

Detective를 Security Lake와 통합한 후 Detective는 AWS CloudTrail 관리 이벤트 및 Amazon Virtual Private Cloud(VPC) 흐름 로그와 관련하여 Security Lake에서 원시 로그를 가져오기 시작합니다.

> **Note**
>
> Detective에서 원시 로그를 쿼리하는 데 대한 추가 비용은 없습니다. Amazon Athena를 포함한 다른 AWS 서비스에 대한 사용 요금은 여전히 게시된 요금으로 적용됩니다.

AWS CloudTrail 관리 이벤트는 다음 프로파일에 사용할 수 있습니다.

- AWS 계정
- AWS 사용자
- AWS 역할
- AWS 역할 세션
- Amazon EC2 인스턴스
- Amazon S3 버킷
- IP 주소
- Kubernetes 클러스터
- Kubernetes 포드
- Kubernetes 제목
- IAM 역할
- IAM 역할 세션
- IAM 사용자

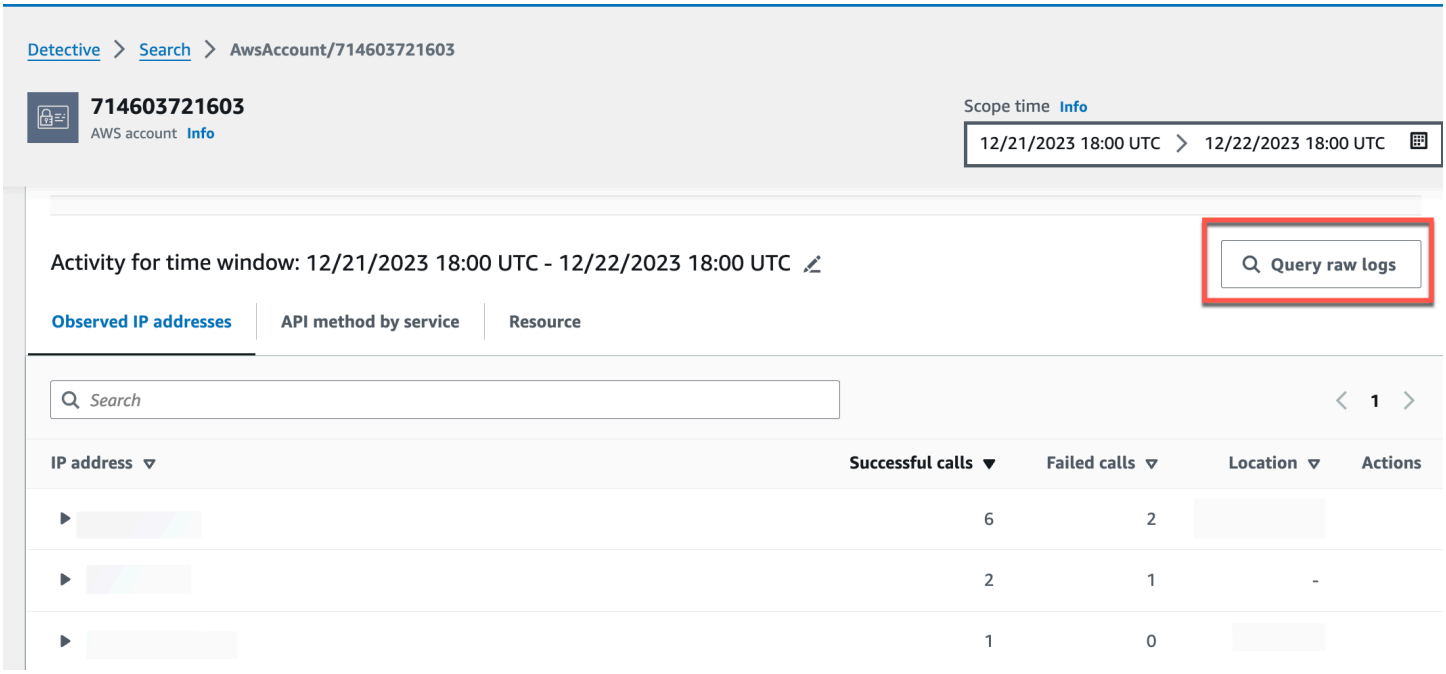
Amazon VPC Flow 로그는 다음 프로필에 사용할 수 있습니다.

- Amazon EC2 인스턴스
- Kubernetes 포드

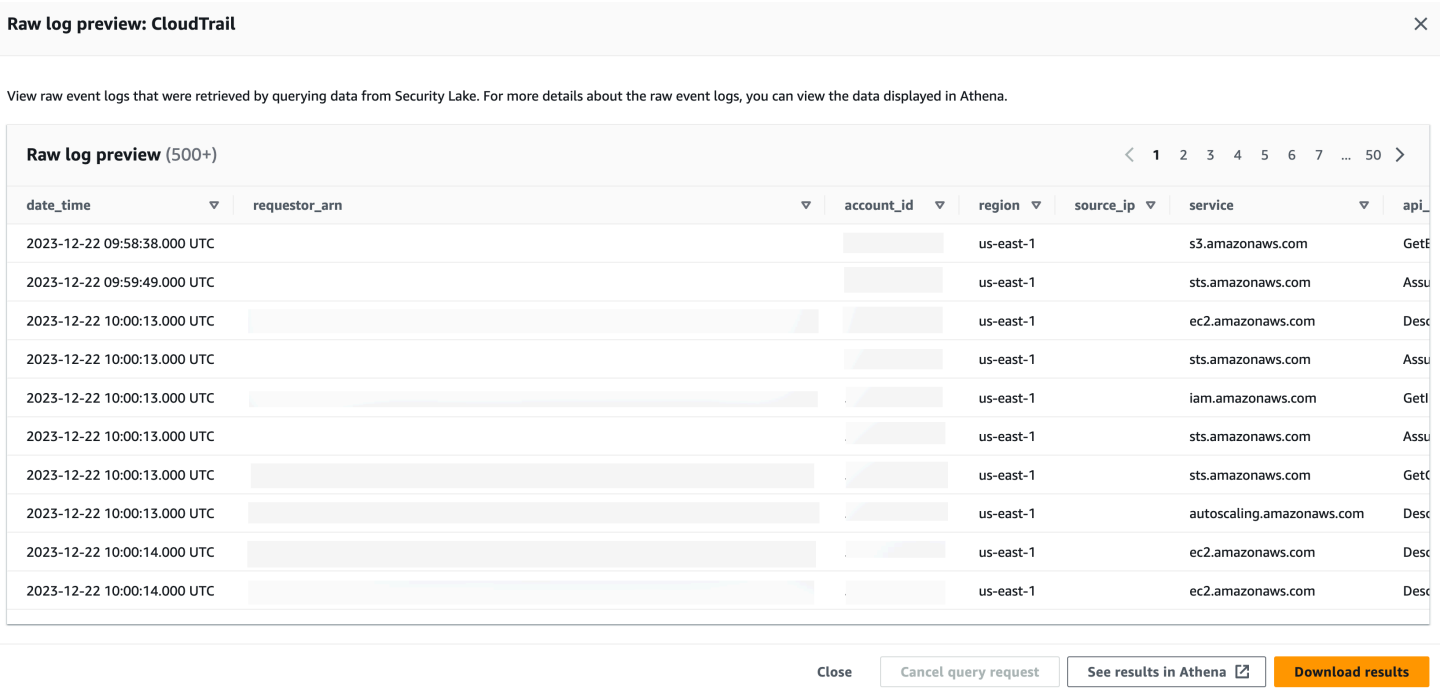
Detective 콘솔을 사용하여 Amazon Detective를 Amazon Security Lake와 통합하는 방법에 대한 데모를 보려면 Amazon Detective와 Amazon Security Lake 통합 - 사용 방법--> 동영상을 시청하세요.

AWS 계정의 원시 로그를 쿼리하려면

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 검색을 선택한 후 `AWS account`을 검색합니다.
3. 전체 API 호출 볼륨 섹션에서 범위 시간에 대한 세부 정보 표시를 선택합니다.
4. 여기에서 원시 로그 쿼리를 시작할 수 있습니다.



원시 로그 미리 보기 테이블을 통해 Security Lake에서 데이터를 쿼리하여 검색한 로그 및 이벤트를 볼 수 있습니다. 원시 이벤트 로그에 대한 자세한 내용은 Amazon Athena에 표시된 데이터를 참조하세요.



원시 로그 쿼리 테이블에서 쿼리 요청을 취소하고, Amazon Athena에서 결과를 확인하고, 결과를 쉼표로 구분된 값(.csv) 파일로 다운로드할 수 있습니다.

Detective에 로그가 표시되지만 쿼리 결과가 반환되지 않는 경우 다음과 같은 이유 때문일 수 있습니다.

- 원시 로그는 Security Lake 로그 테이블에 표시되기 전에 Detective에 제공될 수 있습니다. 나중에 다시 시도해 주세요.
- Security Lake에서 로그가 누락되었을 수 있습니다. 오랜 시간 기다린 경우 Security Lake에서 로그가 누락된 것으로 표시됩니다. Security Lake 관리자에게 문의하여 이 문제를 해결하세요.

예제

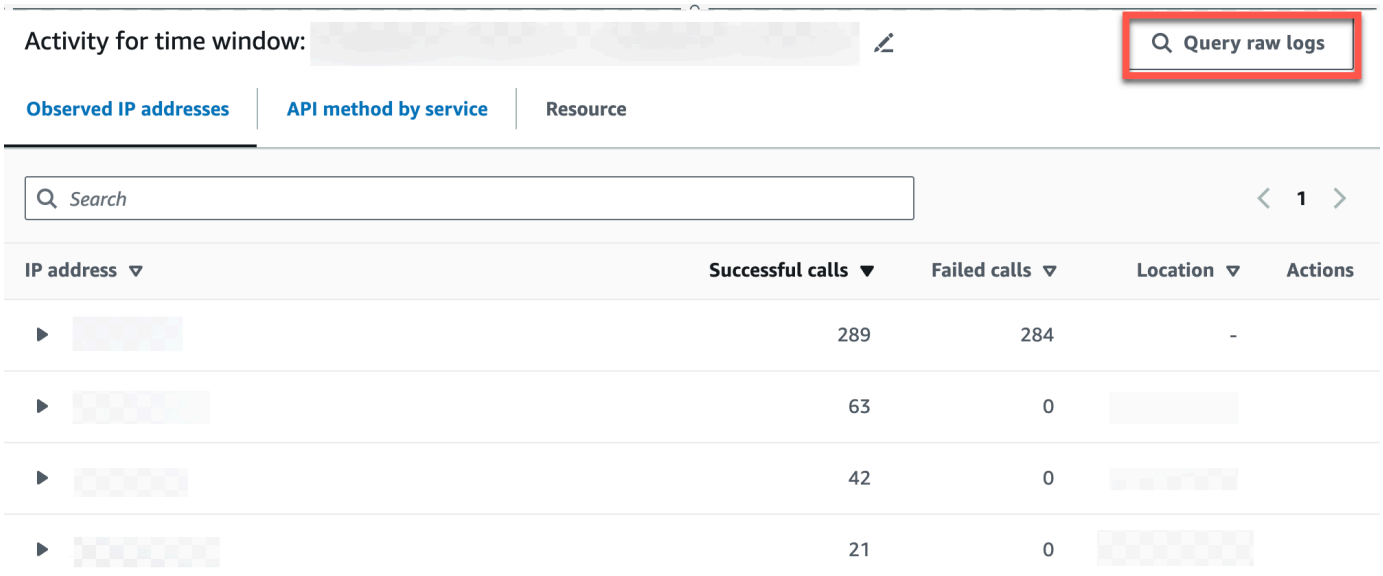
- AWS 역할에 대한 원시 로그 쿼리
- Amazon EKS 클러스터에 대한 원시 로그 쿼리
- Amazon EC2 인스턴스에 대한 원시 로그 쿼리

AWS 역할에 대한 원시 로그 쿼리

새 지리적 위치에서 AWS 역할의 활동을 이해하려면 Detective 콘솔에서 수행할 수 있습니다.

AWS 역할의 원시 로그를 쿼리하려면

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐지 요약 페이지에서 새로 관찰된 지리적 위치 섹션에서 AWS 역할을 기록해 둡니다.
3. 탐색 창에서 검색을 선택한 후 `AWS role`을 검색합니다.
4. AWS 역할의 경우 리소스를 확장하여 해당 리소스가 해당 IP 주소에서 실행한 특정 API 호출을 표시합니다.
5. 조사하려는 API 호출 옆의 돋보기 아이콘을 선택하여 원시 로그 미리 보기 테이블을 엽니다.

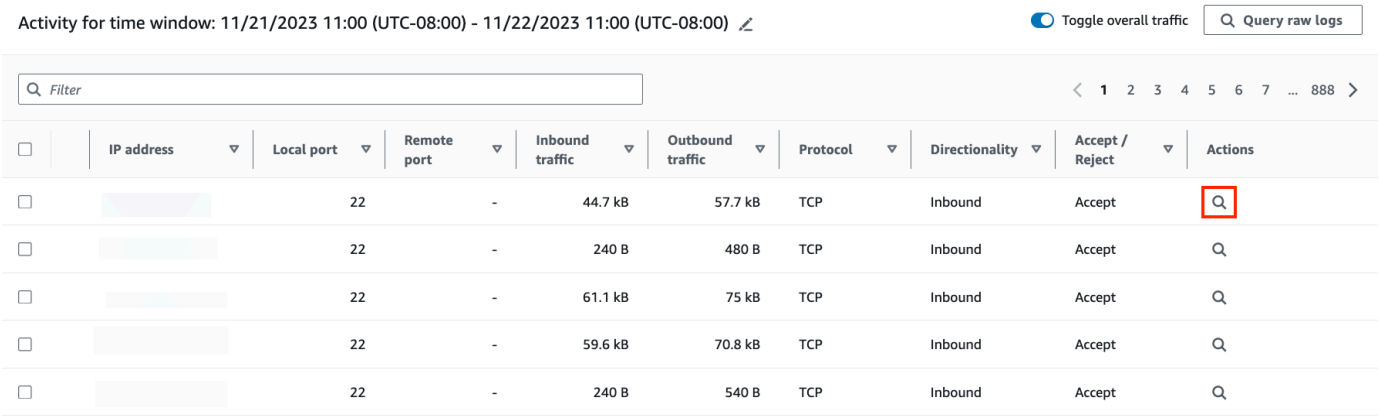


Amazon EKS 클러스터에 대한 원시 로그 쿼리

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 생성된 포드가 가장 많은 컨테이너 클러스터 감지 요약 페이지에서 Amazon EKS 클러스터로 이동합니다.
3. Amazon EKS 클러스터 세부 정보 페이지에서 Kubernetes API 활동 탭을 선택합니다.
4. 이 Amazon EKS 클러스터와 관련된 전체 Kubernetes API 활동 섹션에서 범위 시간에 대한 세부 정보 표시를 선택합니다.
5. 여기에서 원시 로그 쿼리를 시작할 수 있습니다.

Amazon EC2 인스턴스에 대한 원시 로그 쿼리

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 검색을 선택한 후 `Amazon EC2 instance`을 검색합니다.
3. 전체 VPC 흐름 볼륨 섹션에서 조사하려는 API 직접 호출 옆의 돋보기 아이콘을 선택하여 원시 로그 미리 보기 테이블을 엽니다.
4. 여기에서 원시 로그 쿼리를 시작할 수 있습니다.



원시 로그 미리 보기 테이블을 통해 Security Lake에서 데이터를 쿼리하여 검색한 로그 및 이벤트를 볼 수 있습니다. 원시 이벤트 로그에 대한 자세한 내용은 Amazon Athena에 표시된 데이터를 참조하세요.

원시 로그 쿼리 테이블에서 쿼리 요청을 취소하고, Amazon Athena에서 결과를 확인하고, 결과를 쉼표로 구분된 값(.csv) 파일로 다운로드할 수 있습니다.

Security Lake와의 Detective 통합 비활성화

Security Lake와의 Detective 통합을 비활성화하면 더 이상 Security Lake에서 로그 및 이벤트 데이터를 쿼리할 수 없습니다.

Security Lake와의 Detective 통합을 비활성화하려면

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창에서 통합을 선택합니다.
3. 기존 스택을 삭제합니다. 자세한 내용은 CloudFormation 스택 삭제 섹션을 참조하세요.
4. Security Lake 통합 비활성화 창에서 비활성화를 선택합니다.

CloudFormation 스택 삭제

기존 스택을 삭제하지 않으면 동일한 리전에서 새 스택을 생성할 수 없습니다. CloudFormation 콘솔을 사용하거나 AWS CLI를 사용하여 CloudFormation 스택을 삭제할 수 있습니다.

CloudFormation 스택을 삭제하려면(콘솔)

1. https://console.aws.amazon.com/cloudformation AWS CloudFormation 콘솔을 엽니다.
2. CloudFormation 콘솔의 [스택(Stacks)] 페이지에서 삭제할 스택을 선택합니다. 스택이 현재 실행 중이어야 합니다.
3. 스택 세부 정보 창에서 삭제를 선택합니다.
4. 메시지가 나타나면 스택 삭제를 선택합니다.

> **Note**
>
> 스택 삭제가 시작된 후에는 스택 삭제 작업을 중지할 수 없습니다. 스택이 `DELETE_IN_PROGRESS` 상태로 바뀝니다.

스택 삭제가 완료되면 스택의 상태가 `DELETE_COMPLETE`로 바뀝니다.

스택 삭제 오류 문제 해결

`Delete` 버튼을 클릭한 후 `Failed to delete stack` 메시지와 함께 권한 오류가 표시되는 경우, IAM 역할에 스택을 삭제할 CloudFormation 권한이 없는 것입니다. 계정 관리자에게 문의하여 스택을 삭제합니다.

CloudFormation 스택을 삭제하려면(AWS CLI)

AWS CLI 인터페이스에 다음 명령을 입력합니다.

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
      arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

`CFN-DetectiveSecurityLakeIntegration`은 `Creating an AWS CloudFormation Service Role`단계에서 생성한 서비스 역할입니다.

Detective 비용 예측 및 모니터링

Detective 활동을 추적하는 데 도움이 되도록 사용량 페이지에는 수집된 데이터의 양과 예상 비용이 표시됩니다.

- 관리자 계정의 경우 사용량 페이지에 전체 동작 그래프의 데이터 볼륨 및 예상 비용이 표시됩니다.
- 멤버 계정의 경우 사용량 페이지에는 멤버 계정이 제공하는 동작 그래프 전반에서 해당 계정의 데이터 양과 예상 비용이 표시됩니다.

Detective는 AWS CloudTrail 로깅도 지원합니다.

내용

동작 그래프 무료 평가판에 대한 정보

Amazon Detective는 각 리전의 각 계정에 대해 30일 무료 평가판을 제공합니다. 계정의 무료 평가판은 다음 작업 중 하나가 처음 발생할 때 시작됩니다.

- 계정이 Detective를 수동으로 활성화하고 동작 그래프의 관리자 계정이 됩니다.
- 계정이 AWS Organizations에서 조직의 Detective 관리자 계정으로 지정되고 처음으로 Detective가 활성화되었습니다.
- Detective 관리자 계정을 지정하기 전에 이미 Detective를 활성화한 경우에는 새 30일 무료 평가판이 시작되지 않습니다.
- 계정이 동작 그래프에서 멤버 계정으로 가입하라는 초대를 수락하고 멤버 계정으로 활성화됩니다.
- 조직 계정이 Detective 관리자 계정에 의해 멤버 계정으로 활성화됩니다.

무료 평가판은 해당 시점부터 30일 동안 지속됩니다. 해당 기간 동안 처리된 데이터에 대해서는 계정에 요금이 청구되지 않습니다. 평가 기간이 끝나면 Detective는 동작 그래프에 기여한 데이터에 대해 계정에 요금을 청구하기 시작합니다. Detective 활동을 추적하고 사용량을 모니터링하고 예상 비용을 확인

하는 방법에 대한 자세한 내용은 Detective 비용 예측 및 모니터링 섹션을 참조하세요. 요금에 대한 자세한 내용은 Detective 요금을 참조하세요.

해당 리전의 모든 동작 그래프에는 동일한 30일 기간이 사용됩니다. 예를 들어, 계정이 동작 그래프의 멤버 계정으로 활성화되어 있습니다. 그러면 30일 무료 평가판이 시작됩니다. 10일 후 해당 계정은 동일한 리전에서 두 번째 동작 그래프를 생성할 수 있습니다. 두 번째 동작 그래프의 경우 계정에 20일간의 무료 데이터가 제공됩니다.

무료 평가판은 여러 가지 이점을 제공합니다.

- 관리자 계정은 Detective의 기능을 탐색하여 그 가치를 확인할 수 있습니다.
- 관리자 및 멤버 계정은 Detective가 청구를 시작하기 전에 데이터 양과 예상 비용을 모니터링할 수 있습니다. the section called “관리자 계정 사용량 및 비용” 및 the section called “멤버 계정 사용량 추적” 단원을 참조하세요.

선택적 데이터 소스에 대한 무료 평가판

또한 Detective는 선택적 데이터 소스에 대해 30일 무료 평가판을 제공합니다. 이 무료 평가판은 Detective가 처음 활성화되었을 때 핵심 Detective 데이터 소스에 제공되는 무료 평가판과는 별개입니다.

> **Note**
>
> 고객이 선택적 데이터 소스 패키지를 활성화한 후 7일 이내에 비활성화하면 Detective는 해당 데이터 소스 패키지가 다시 활성화되는 경우 해당 데이터 소스 패키지의 무료 평가판을 1회 자동 재설정합니다.

선택적 데이터 소스를 활성화 또는 비활성화하려면 Detective의 선택적 데이터 소스 유형 섹션을 참조하세요.

Detective 관리자 계정의 사용량 모니터링

Amazon Detective는 계정이 속한 각 동작 그래프에 사용된 데이터에 대해 각 계정에 요금을 청구합니다. Detective는 출처에 관계없이 모든 데이터에 대해 GB당 계층화된 고정 요금을 부과합니다.

관리자 계정의 경우 Detective 콘솔의 사용량 페이지를 통해 지난 30일 동안 데이터 소스별 또는 계정별로 수집된 데이터의 볼륨을 볼 수 있습니다. 또한 관리자 계정은 해당 계정 및 전체 동작 그래프에서 일반적인 30일 기간의 예상 비용을 확인할 수 있습니다.

Detective 사용량 정보 보기

1. AWS Management Console에 로그인합니다. 그런 다음 에서 Detective 콘솔을 여십시오. https://console.aws.amazon.com/detective/
2. Detective 탐색 창의 설정 아래에서 사용량을 선택합니다.
3. 탭을 선택하여 데이터 소스별 또는 계정별 사용량 보기 중에서 선택합니다.

각 계정에서 수집된 데이터의 볼륨양

멤버 계정별로 수집된 볼륨은 동작 그래프에 활성 계정을 나열합니다. 제거된 멤버 계정은 나열되지 않습니다.

각 계정에 대해 수집된 볼륨 목록은 다음 정보를 제공합니다.

- AWS 계정 식별자 및 루트 사용자 이메일 주소.
- 계정이 동작 그래프에 데이터를 제공하기 시작한 날짜.

  관리자 계정의 경우 이 날짜는 해당 계정이 Detective를 활성화한 날짜입니다.

  멤버 계정의 경우 이 날짜는 초대를 수락한 후 계정이 멤버 계정으로 활성화된 날짜입니다.
- 지난 30일 동안 계정에서 수집된 데이터의 볼륨. 합계에는 모든 소스 유형이 포함됩니다.
- 계정이 현재 무료 평가판 기간 중인지 여부. 현재 무료 평가 기간이 있는 계정의 경우 목록에 남은 일수가 표시됩니다.

  무료 평가판 기간 중인 계정이 없는 경우 무료 평가판 상태 열이 표시되지 않습니다.

동작 그래프의 예상 비용

이 계정의 예상 비용은 관리자 계정의 30일 데이터 예상 비용을 나타냅니다. 예상 비용은 관리자 계정의 일일 평균 볼륨을 기준으로 합니다.

> **Important**
>
> 이 금액은 예상 비용일 뿐입니다. 이는 일반적인 30일 기간의 관리자 계정 데이터에 대한 총 비용을 예상합니다. 이는 이전 30일간의 사용량을 기준으로 합니다. the section called “Detective가 예상 비용을 계산하는 방법”을 참조하세요.

동작 그래프의 예상 비용

모든 계정의 예상 비용에는 전체 동작 그래프에 대한 30일간의 데이터에 대한 총 예상 비용이 표시됩니다. 예상 비용은 각 계정의 일일 평균 볼륨을 기준으로 합니다.

> **Important**
>
> 이 금액은 예상 비용일 뿐입니다. 이는 일반적인 30일 기간 동안의 동작 그래프 데이터에 대한 총 비용을 예측합니다. 이는 이전 30일간의 사용량을 기준으로 합니다. 예상 비용에는 동작 그래프에서 삭제된 멤버 계정이 포함되지 않습니다. the section called “Detective가 예상 비용을 계산하는 방법”을 참조하세요.

소스 패키지에서 수집한 데이터의 볼륨

동작 그래프에 활성화된 다양한 소스 패키지에서 수집한 데이터 볼륨을 나열하여 보려면 소스 패키지별을 선택합니다.

모든 계정이 해당 계정에 대해 이 데이터를 볼 수 있습니다. 관리자 계정은 각 멤버의 소스 패키지별 사용량을 나열하는 추가 패널을 볼 수 있습니다. 제거된 멤버 계정은 나열되지 않습니다.

Detective 핵심

Detective 코어 패널에는 지난 30일 동안 Detective 핵심 소스 (CloudTrail 로그, VPC Flow 로그 및 GuardDuty 결과) 에서 수집된 데이터의 양이 표시됩니다.

EKS 감사 로그

EKS감사 로그 패널에는 지난 30일간 EKS 감사 로그 소스에서 수집된 데이터의 양이 표시됩니다. 이 소스 패키지의 패널은 동작 그래프에 EKS 감사 로그가 활성화된 경우에만 사용할 수 있습니다.

Detective 회원 계정 사용 모니터링

Amazon Detective는 계정이 속한 각 동작 그래프에 사용된 데이터에 대해 각 계정에 요금을 청구합니다. Detective는 출처에 관계없이 모든 데이터에 대해 GB당 계층화된 고정 요금을 부과합니다.

멤버 계정의 경우 사용량 페이지에는 해당 계정의 데이터 볼륨과 30일 예상 비용만 표시됩니다.

Detective 사용량 정보 보기

1. AWS Management Console에 로그인합니다. 그런 다음 에서 Detective 콘솔을 여십시오. https://console.aws.amazon.com/detective/
2. Detective 탐색 창의 설정 아래에서 사용량을 선택합니다.

각 동작 그래프의 수집 볼륨

이 계정의 수집 볼륨에는 멤버 계정이 제공한 동작 그래프가 나열됩니다. 여기에는 탈퇴된 멤버십 또는 관리자 계정으로 제거된 멤버십이 포함되어 있지 않습니다.

각 동작 그래프의 경우 목록에는 다음과 같은 정보가 포함되어 있습니다.

- 관리자의 계정의 계정 번호
- 지난 30일 동안 멤버 계정에서 수집된 데이터의 볼륨. 합계에는 모든 소스 유형이 포함됩니다.
- 멤버 계정이 동작 그래프에 활성화 날짜.

동작 그래프 전반의 예상 비용

이 계정의 예상 비용에는 해당 계정이 제공하는 모든 동작 그래프에서 해당 멤버 계정의 30일 데이터에 대한 예상 비용이 표시됩니다. 예상 비용은 멤버 계정의 일일 평균 볼륨을 기준으로 합니다.

> **Important**
>
> 이 금액은 예상 비용일 뿐입니다. 이는 일반적인 30일 기간의 관리자 계정 데이터에 대한 총 비용을 예상합니다. 이는 이전 30일간의 사용량을 기준으로 합니다. the section called “Detective가 예상 비용을 계산하는 방법”을(를) 참조하세요.

Amazon Detective가 예상 비용을 계산하는 방법

Detective는 사용량 페이지에 표시되는 예상 비용 값을 계산하기 위해 다음 작업을 수행합니다.

1. 동작 그래프에서 개별 계정의 예상 비용을 구하기 위해 Detective는 다음을 수행합니다.
   a. 일일 평균 볼륨을 계산합니다. 모든 활성 일수의 데이터 볼륨을 더한 다음 계정이 활성화된 기간(일)으로 나눕니다.

계정을 활성화한 지 30일이 지난 경우 남은 일수는 30일입니다. 계정을 활성화한 지 30일이 지나지 않은 경우 남은 일수는 수락 날짜 이후입니다.

예를 들어 계정이 12일 전에 활성화된 경우 Detective는 해당 12일 동안 수집된 볼륨을 더한 다음 이를 12로 나눕니다.

b. 계정의 일일 평균에 30을 곱합니다. 이는 해당 계정의 30일 예상 사용량입니다.

c. 요금 모델을 사용하여 30일 예상 사용량에 대한 30일 예상 비용을 계산합니다.

2. 동작 그래프의 총 예상 비용을 구하기 위해 Detective는 다음을 수행합니다.

a. 동작 그래프에 있는 모든 계정의 30일 예상 사용량을 합산합니다.

b. 요금 모델을 사용하여 30일 총 예상 사용량에 대한 30일 예상 비용을 계산합니다.

3. 동작 그래프에서 멤버 계정의 총 예상 비용을 구하기 위해 Detective는 다음을 수행합니다.

a. 모든 동작 그래프의 30일 예상 사용량을 합산합니다.

b. 요금 모델을 사용하여 30일 총 예상 사용량에 대한 30일 예상 비용을 계산합니다.

4. 공유 Amazon VPC를 사용하는 경우, Detective는 모니터링 활동을 기반으로 예상 비용을 계산합니다. 본인의 환경에 해당하는 조사의 예상 비용을 검토하는 것이 좋습니다.

a. Detective 멤버 계정에 공유 Amazon VPC가 있고 이 공유 VPC를 사용하는 다른 비 Detective 계정이 있는 경우 Detective는 해당 VPC에서 들어오는 모든 트래픽을 모니터링합니다. 사용량과 비용이 증가하고 Detective는 VPC 내의 모든 트래픽 흐름을 시각화합니다.

b. 공유 Amazon VPC 내에 EC2 인스턴스가 있고 공유 소유자가 Detective 멤버가 아닌 경우, Detective는 VPC의 트래픽을 모니터링하지 않으므로 사용량과 비용이 감소합니다. VPC 내의 트래픽 흐름을 보려면 Amazon VPC 소유자를 Detective 그래프의 멤버로 추가해야 합니다.

Amazon Detective의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이를 클라우드의 보안과 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다.

  서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다.

  Amazon Detective에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 범위 내AWS 서비스를 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Detective 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Detective를 구성하는 방법을 보여줍니다. 또한 Detective 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

내용

Amazon Detective의 데이터 보호

AWS 공동 책임 모델 Amazon Detective의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 일반 데이터 보호 규정(GDPR) 센터를 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Detective 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

Detective는 저장 및 전송 중인 모든 데이터를 암호화합니다.

내용

- Amazon Detective의 키 관리

Amazon Detective의 키 관리

Detective는 개인 식별이 가능한 고객 데이터를 저장하지 않기 때문에 AWS 관리형 키를 사용합니다.

이 유형의 KMS 키는 여러 계정에서 사용할 수 있습니다. AWS Key Management Service 개발자 안내서의 AWS 소유 키 설명을 참조하십시오.

이 유형의 KMS 키는 1년마다(약 365일) 자동으로 순환됩니다. AWS Key Management Service 개발자 안내서의 키 순환 설명을 참조하십시오.

Amazon Detective용 Identity and Access Management

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 누가 Detective 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

내용

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조Amazon Detective 자격 증명 및 액세스 문제 해결)
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(Amazon Detective가 IAM과 작동하는 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(Amazon Detective 자격 증명 기반 정책 예제 참조)

자격 증명을 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증해야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자가 필요한 작업 목록은 IAM 사용자 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 IAM 사용 설명서의 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

자격 증명 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

Amazon Detective가 IAM과 작동하는 방식

기본적으로 사용자 및 역할은 Amazon Detective 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI또는 AWS API를 사용하여 작업을 수행할 수 없습니다. Detective 관리자에게는 IAM 사용자 및 역할에 필요한 지정된 리소스에 대해 특정 API 작업을 수행할 수 있는 권한을 부여하는 AWS Identity and Access Management (IAM) 정책이 있어야 합니다. 그런 다음 관리자는 해당 권한이 필요한 보안 주체에 이러한 정책을 연결해야 합니다.

Detective는 IAM 자격 증명 기반 정책을 사용하여 다음 유형의 사용자 및 작업에 권한을 부여합니다.

- 관리자 계정 - 관리자 계정은 계정 데이터를 사용하는 동작 그래프의 소유자입니다. 관리자 계정은 멤버 계정을 초대하여 동작 그래프에 데이터를 제공할 수 있습니다. 또한 관리자 계정은 동작 그래프를 사용하여 해당 계정과 관련된 조사 결과 및 리소스를 분류하고 조사할 수 있습니다.

관리자 계정이 아닌 사용자가 다양한 유형의 작업을 수행할 수 있도록 정책을 설정할 수 있습니다. 예를 들어 관리자 계정의 사용자는 멤버 계정을 관리할 권한만 가질 수 있습니다. 다른 사용자에게는 조사를 위해 동작 그래프를 사용할 권한만 있을 수 있습니다.

- 멤버 계정 - 멤버 계정은 동작 그래프에 데이터를 제공하도록 초대받은 계정입니다. 멤버 계정은 초대에 응답합니다. 초대를 수락한 후 멤버 계정은 동작 그래프에서 자신의 계정을 제거할 수 있습니다.

Detective 및 기타에서 IAM을 AWS 서비스 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 JSON 탭에서 정책 생성을 참조하세요.

Detective 자격 증명 기반 정책

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스는 물론, 작업이 허용되거나 거부되는 조건도 지정할 수 있습니다. Detective는 특정 작업, 리소스 및 조건 키를 지원합니다.

JSON 정책에서 사용하는 모든 요소에 대해 알고 싶다면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

작업

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

정책 설명에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. `Action` 요소는 정책에서 허용되는 작업을 나열합니다. `NotAction` 요소는 허용되지 않는 작업을 나열합니다.

Detective에 정의된 작업은 Detective를 사용하여 수행할 수 있는 작업을 반영합니다. Detective의 정책 작업에는 다음과 같은 접두사가 붙습니다: `detective:`.

예를 들어 `CreateMembers` API 작업으로 멤버 계정을 동작 그래프에 초대할 수 있는 권한을 부여하려면 해당 정책에 `detective:CreateMembers` 작업을 포함합니다.

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다. 예를 들어 멤버 계정의 경우 정책에는 초대 관리와 관련된 일련의 작업이 포함됩니다.

```
"Action": [
      "detective:ListInvitations",
```

```
        "detective:AcceptInvitation",
        "detective:RejectInvitation",
        "detective:DisassociateMembership
]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수도 있습니다. 예를 들어 동작 그래프에 사용되는 데이터를 관리하려면 Detective의 관리자 계정이 다음 작업을 수행할 수 있어야 합니다.

- 멤버 계정 목록 보기(`ListMembers`).
- 선택한 멤버 계정에 대한 정보 가져오기(`GetMembers`).
- 멤버 계정을 동작 그래프에 초대(`CreateMembers`).
- 동작 그래프에서 멤버 삭제(`DeleteMembers`).

이러한 작업을 별도로 나열하는 대신, `Members` 단어로 끝나는 모든 작업에 대한 액세스 권한을 부여할 수 있습니다. 이에 대한 정책에는 다음과 같은 작업이 포함될 수 있습니다.

```
"Action": "detective:*Members"
```

Detective 작업 목록을 보려면 서비스 권한 부여 참조의 Amazon Detective에서 정의한 작업을 참조하세요.

리소스

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

ARN 형식에 대한 자세한 내용은 Amazon 리소스 이름(ARNs) 및 AWS 서비스 네임스페이스를 참조하세요.

Detective의 경우 리소스 유형만 동작 그래프입니다. Detective의 동작 그래프 리소스에는 다음 ARN이 있습니다.

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

예를 들어 동작 그래프는 다음과 같은 값을 가질 수 있습니다.

- 동작 그래프의 리전은 us-east-1입니다.
- 관리자의 계정 ID의 계정 ID는 111122223333입니다.
- 동작 그래프의 그래프 ID는 027c7c4610ea4aacaf0b883093cab899입니다.

Resource 문에서 이 동작 그래프를 식별하려면 다음 ARN을 사용합니다.

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

Resource 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
      "resource1",
      "resource2"
]
```

예를 들어, 둘 이상의 동작 그래프에서 동일한 AWS 계정을 멤버 계정으로 초대할 수 있습니다. 해당 멤버 계정의 정책에서 Resource 문에는 초대를 받은 동작 그래프가 나열되어 있습니다.

```
"Resource": [
      "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

동작 그래프 생성, 동작 그래프 나열, 동작 그래프 초대 목록 작성과 같은 일부 Detective 작업은 특정 동작 그래프에서 수행되지 않습니다. 이러한 작업의 경우 Resource 문에 와일드카드(*)를 사용해야 합니다.

```
"Resource": "*"
```

관리자 계정 작업의 경우 Detective는 요청하는 사용자가 영향을 받는 동작 그래프의 관리자 계정에 속하는지 항상 확인합니다. 멤버 계정 작업의 경우 Detective는 요청하는 사용자가 멤버 계정에 속하는지

항상 확인합니다. IAM 정책에서 동작 그래프에 대한 액세스 권한을 부여하더라도 사용자가 올바른 계정에 속하지 않으면 사용자는 작업을 수행할 수 없습니다.

특정 동작 그래프에서 수행되는 모든 작업에 대해 IAM 정책에는 그래프 ARN이 포함되어야 합니다. 그래프 ARN은 나중에 추가할 수 있습니다. 예를 들어, 계정이 처음으로 Detective를 활성화하면 초기 IAM 정책은 그래프 ARN의 와일드카드를 사용하여 모든 Detective 작업에 대한 액세스를 제공합니다. 이를 통해 사용자는 즉시 멤버 계정을 관리하고 동작 그래프에서 조사를 수행할 수 있습니다. 동작 그래프가 생성된 후 정책을 업데이트하여 그래프 ARN을 추가할 수 있습니다.

조건 키

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Detective는 자체 조건 키 집합을 정의하지 않습니다. 이는 일부 전역 조건 키를 사용하도록 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon Detective에서 정의한 작업을 참조하세요.

예제

Detective 자격 증명 기반 정책의 예를 보려면 Amazon Detective 자격 증명 기반 정책 예제 섹션을 참조하세요.

Detective 리소스 기반 정책(지원되지 않음)

Detective는 리소스 기반 정책을 지원하지 않습니다.

Detective 동작 그래프 태그를 기반으로 한 권한 부여

각 동작 그래프에 태그 값을 할당할 수 있습니다. 조건문에서 이러한 태그 값을 사용하여 동작 그래프에 대한 액세스를 관리할 수 있습니다.

태그 값의 조건문은 다음 형식을 사용합니다.

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

예를 들어, Department 태그의 값이 Finance인 경우 다음 코드를 사용하여 작업을 허용하거나 거부할 수 있습니다.

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

리소스 태그 값을 사용하는 정책의 예는 the section called “관리자 계정: 태그 값을 기반으로 액세스 제한” 섹션을 참조하세요.

Detective IAM 역할

IAM 역할은 특정 권한이 있는 AWS 계정 내 엔터티입니다.

Detective에서 임시 보안 인증 정보 사용

임시 보안 인증을 사용하여 페더레이션을 통해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AssumeRole 또는 GetFederationToken과 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 얻습니다.

Detective는 임시 보안 인증 정보 사용을 지원합니다.

서비스 연결 역할

서비스 연결 역할을 사용하면 AWS 서비스가 다른 서비스의 리소스에 액세스하여 사용자를 대신하여 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 나타나고 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수 없습니다.

Detective 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 the section called “서비스 연결 역할 사용” 섹션을 참조하세요.

서비스 역할(지원되지 않음)

이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 역할을 수임할 수 있습니다. 이 역할을 사용하면 서비스가 다른 서비스의 리소스에 액세스해 사용자를 대신해 작업을 완료할 수 있습니다. 서비스 역할은 IAM 계정에 나타나고, 해당 계정이 소유합니다. 즉, IAM 관리자가 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

Detective는 서비스 역할을 지원하지 않습니다.

Amazon Detective 자격 증명 기반 정책 예제

기본적으로 IAM 사용자 및 역할은 Detective 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI또는 AWS API를 사용하여 작업을 수행할 수 없습니다.

IAM 관리자는 지정된 리소스에서 특정 API 작업을 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음, 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 정책을 연결합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용자 설명서의 JSON 탭에서 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- Detective 콘솔 사용
- 사용자가 자체 권한을 볼 수 있도록 허용
- 관리자 계정: 동작 그래프에서 멤버 계정 관리
- 관리자 계정: 조사를 위한 동작 그래프 사용
- 멤버 계정: 동작 그래프 초대 및 멤버십 관리
- 관리자 계정: 태그 값을 기반으로 액세스 제한

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Detective 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있

는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.

- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Detective 콘솔 사용

Amazon Detective 콘솔을 사용하려면 사용자 또는 역할이 API의 해당 작업과 일치하는 관련 작업에 액세스할 수 있어야 합니다.

Detective를 활성화하고 동작 그래프의 관리자 계정이 되려면 사용자 또는 역할에 `CreateGraph` 작업 권한을 부여해야 합니다.

Detective 콘솔을 사용하여 관리자 계정 작업을 수행하려면 사용자 또는 역할에 `ListGraphs` 작업에 대한 권한을 부여해야 합니다. 그러면 해당 계정이 관리자 계정인 동작 그래프를 검색할 수 있는 권한이 부여됩니다. 또한 특정 관리자 계정 작업을 수행할 수 있는 권한도 부여받아야 합니다.

가장 기본적인 관리자 계정 작업은 동작 그래프에서 멤버 계정 목록을 보고 동작 그래프를 사용하여 조사하는 것입니다.

- 동작 그래프에서 멤버 계정 목록을 보려면 보안 주체에게 해당 `ListMembers` 작업에 대한 권한을 부여해야 합니다.
- 동작 그래프에서 조사를 수행하려면 보안 주체에게 해당 `SearchGraph` 작업에 대한 권한을 부여해야 합니다.

Detective 콘솔을 사용하여 멤버 계정 작업을 수행하려면 사용자 또는 역할에 `ListInvitations` 작업 권한을 부여해야 합니다. 그러면 동작 그래프 초대를 볼 수 있는 권한이 부여됩니다. 그러면 특정 멤버 계정 작업에 대한 권한을 부여받을 수 있습니다.

사용자가 자체 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여 줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "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": "*"
        }
    ]
}
```

관리자 계정: 동작 그래프에서 멤버 계정 관리

이 예제 정책은 동작 그래프에 사용되는 멤버 계정만 관리할 책임이 있는 관리자 계정 사용자를 대상으로 합니다. 또한 사용자가 사용 정보를 보고 Detective를 비활성화할 수 있도록 허용합니다. 이 정책은 조사를 위해 동작 그래프를 사용할 권한을 부여하지 않습니다.

JSON

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:D
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

관리자 계정: 조사를 위한 동작 그래프 사용

이 예제 정책은 조사 목적으로만 동작 그래프를 사용하는 관리자 계정 사용자를 대상으로 합니다. 사용자는 동작 그래프에서 멤버 계정 목록을 보거나 편집할 수 없습니다.

JSON

```
{"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":"*"
  }
 ]
}
```

멤버 계정: 동작 그래프 초대 및 멤버십 관리

이 예제 정책은 멤버 계정에 속한 사용자를 대상으로 합니다. 이 예제에서 멤버 계정은 두 개의 동작 그래프에 속합니다. 이 정책은 초대에 응답하고 동작 그래프에서 멤버 계정을 제거할 권한을 부여합니다.

JSON

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembers
   "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":"*"
  }
 ]
}
```

관리자 계정: 태그 값을 기반으로 액세스 제한

다음 정책은 사용자가 동작 그래프의 `SecurityDomain` 태그가 사용자의 `SecurityDomain` 태그와 일치하는지 여부를 조사하기 위해 동작 그래프를 사용할 수 있도록 허용합니다.

JSON

```
{
    "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": "*"
        }
    ]
}
```

다음 정책은 동작 그래프의 SecurityDomain 태그 값이 Finance인 경우 사용자가 동작 그래프를 조사에 사용할 수 없도록 합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
```

```
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

AWS Amazon Detective에 대한 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용자 가이드의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonDetectiveFullAccess

`AmazonDetectiveFullAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 모든 Amazon Detective 작업에 대한 전체 액세스 권한을 허용하는 관리 권한을 보안 주체에게 부여합니다. 이 정책은 보안 주체가 해당 계정에 대해 Detective를 활성화하기 전에 보안 주체에게 연결할 수 있습니다. 또한 동작 그래프를 생성하고 관리하기 위해 Detective Python 스크립트를 실행하는 데 사용되는 역할에 연결되어야 합니다.

이러한 권한이 있는 보안 주체는 멤버 계정을 관리하고, 동작 그래프에 태그를 추가하고, Detective를 사용하여 조사할 수 있습니다. 또한 GuardDuty 조사 결과를 보관할 수도 있습니다. 이 정책은 Detective 콘솔에 있는 계정의 계정 이름을 표시하는 데 필요한 권한을 제공합니다 AWS Organizations.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `detective` – 보안 주체가 Detective 작업에 대한 모든 액세스 권한을 가질 수 있습니다.
- `organizations` – 보안 주체가 조직의 계정에 대한 AWS Organizations 정보를 검색할 수 있습니다. 계정이 조직에 속한 경우 이러한 권한을 통해 Detective 콘솔은 계정 번호 외에도 계정 이름을 표시할 수 있습니다.
- `guardduty` - 보안 주체가 Detective 내에서 GuardDuty 조사 결과를 가져오고 보관할 수 있습니다.
- `securityhub` - 보안 주체가 Detective 내에서 Security Hub CSPM 조사 결과를 가져올 수 있도록 허용합니다.

JSON

```
{
    "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 관리형 정책: AmazonDetectiveMemberAccess

`AmazonDetectiveMemberAccess` 정책을 IAM 엔터티에 연결할 수 있습니다.

이 정책은 Amazon Detective에 대한 멤버 액세스 권한과 콘솔에 대한 범위 지정 액세스를 제공합니다.

이 정책을 통해 다음을 수행할 수 있습니다.

- Detective 그래프 멤버십 초대를 확인하고 해당 초대를 수락하거나 거부할 수 있습니다.
- 사용 페이지에서 Detective에서의 활동이 이 서비스 사용 비용에 어떻게 기여하는지 확인합니다.
- 그래프로 멤버십에서 탈퇴합니다.

이 정책은 Detective
콘솔에 대한 범위 지정 액세스를 허용하는 읽기 전용 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `detective` - 멤버가 Detective에 액세스할 수 있습니다.

JSON

```
{
  "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 관리형 정책: AmazonDetectiveInvestigatorAccess

`AmazonDetectiveInvestigatorAccess` 정책을 IAM 엔터티에 연결할 수 있습니다.

이 정책은 Detective 서비스에 대한 조사자 액세스 권한과 콘솔 UI 종속성에 대한 범위 지정 액세스 권한을 제공합니다. 이 정책은 IAM 사용자 및 IAM 역할에 대해 Detective에서 Detective 조사를 활성화할 수 있는 권한을 부여합니다. 보안 지표에 대한 분석 및 통찰력을 제공하는 조사 보고서를 사용하여 조사 결과와 같은 손상 지표를 식별할 수 있습니다. 보고서는 Detective의 동작 분석 및 기계 학습을 사용하여 결정되는 심각도에 따라 순위가 매겨집니다. 보고서를 사용하여 리소스 문제 해결의 우선 순위를 정할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `detective` - 보안 주체 조사자가 Detective 작업에 액세스하여 Detective 조사를 활성화하고 조사 결과 그룹 요약을 활성화할 수 있도록 합니다.

- `guardduty` - 보안 주체가 Detective 내에서 GuardDuty 조사 결과를 가져오고 보관할 수 있습니다.
- `securityhub` - 보안 주체가 Detective 내에서 Security Hub CSPM 조사 결과를 가져올 수 있도록 허용합니다.
- `organizations` - 보안 주체가 조직의 계정에 대한 정보를 검색할 수 있도록 허용합니다 AWS Organizations. 계정이 조직에 속하면 이러한 권한을 통해 Detective 콘솔은 계정 번호 외에도 계정 이름을 표시할 수 있습니다.

JSON

```
{
  "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 관리형 정책: AmazonDetectiveOrganizationsAccess

`AmazonDetectiveOrganizationsAccess` 정책을 IAM 엔터티에 연결할 수 있습니다.

이 정책은 조직 내에서 Amazon Detective를 활성화하고 관리할 권한을 부여합니다. 조직 전체에서 Detective를 활성화하고 Detective의 위임된 관리자 계정을 결정할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `detective` – 보안 주체가 Detective 작업에 대한 액세스 권한을 가질 수 있습니다.
- `iam` - Detective가 `EnableOrganizationAdminAccount`를 호출할 때 서비스 연결 역할이 생성되도록 지정합니다.
- `organizations` - 보안 주체가 조직의 계정에 대한 정보를 검색할 수 있도록 허용합니다 AWS Organizations. 계정이 조직에 속하면 이러한 권한을 통해 Detective 콘솔은 계정 번호 외에도 계정 이름을 표시할 수 있습니다. AWS 서비스 통합을 활성화하고, 지정된 멤버 계정을 위임된 관리자로 등록 및 등록 취소할 수 있으며, 보안 주체가 Amazon Detective, Amazon GuardDuty, Amazon Macie, 등의 다른 보안 서비스에서 위임된 관리자 계정을 검색할 수 있습니다 AWS Security Hub CSPM.

JSON

```
{
  "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 관리형 정책: AmazonDetectiveServiceLinkedRole

`AmazonDetectiveServiceLinkedRole` 정책을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Detective에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 내용은 the section called “서비스 연결 역할 사용” 단원을 참조하십시오.

이 정책은 서비스 연결 역할이 조직의 계정 정보를 검색할 수 있도록 하는 관리 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `organizations` - 조직의 계정 정보를 검색합니다.

JSON

```
{
  "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "organizations:DescribeAccount",
              "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책에 대한 Detective 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 Detective의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date
AmazonDetectiveInvestigatorAccess - 기존 정책에 대한 업데이트	Detective 조사 및 조사 결과 그룹 요약 작업을 AmazonDetectiveInvestigatorAccess 정책에 추가했습니다. 이러한 작업을 통해 Detective 조사를 시작, 검색 및 업데이트하고 Detective 내에서 조사 결과 그룹 요약을 얻을 수 있습니다.	2023년 11월 26일
AmazonDetectiveFullAccess 및 AmazonDetectiveInvestigatorAccess - 기존 정책 업데이트	Detective는 Security Hub CSPM GetFindings 작업을 AmazonDetectiveFullAccess 및 AmazonDetectiveInvestigatorAccess 정책에 추가했습니다. 이러한 작업을 통해 Detective 내에서 Security Hub CSPM 조사 결과를 가져올 수 있습니다.	2023년 5월 16일
AmazonDetectiveOrganizationsAccess - 새 정책	Detective는 AmazonDetectiveOrganizationsAccess 정책을 추가했습니다. 이 정책은 조직 내에서 Detective를 활성화하고 관리할 권한을 부여합니다.	2023년 3월 2일
AmazonDetectiveMemberAccess - 새 정책	Detective는 AmazonDetectiveMemberAccess 정책을 추가했습니다. 이 정책은 멤버에게 Detective에 대한 액세스 권한과 콘솔 UI 종속성에	2023년 1월 17일

변경	설명	Date
	대한 범위 지정 액세스 권한을 제공합니다.	
AmazonDetectiveFullAccess - 기존 정책에 대한 업데이트	Detective는 GuardDuty `GetFindings` 작업을 `AmazonDetectiveFullAccess` 정책에 추가했습니다. 이러한 작업을 통해 Detective 내에서 GuardDuty 조사 결과를 가져올 수 있습니다.	2023년 1월 17일
AmazonDetectiveInvestigatorAccess - 새 정책	Detective는 `AmazonDetectiveInvestigatorAccess` 정책을 추가했습니다. 이 정책을 통해 보안 주체가 Detective에서 조사를 수행할 수 있습니다.	2023년 1월 17일
AmazonDetectiveServiceLinkedRole - 새 정책	Detective는 해당 서비스 연결 역할에 대한 새 정책을 추가했습니다. 이 정책은 서비스 연결 역할이 조직의 계정에 대한 정보를 검색할 수 있도록 허용합니다.	2021년 12월 16일
Detective가 변경 사항 추적하기 시작	Detective는 AWS 관리형 정책에 대한 변경 사항을 추적하기 시작했습니다.	2021년 5월 10일

Detective에 서비스 연결 역할 사용

Amazon Detective는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Detective에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은

Detective에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Detective를 더 간편하게 설정할 수 있습니다. Detective에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Detective만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Detective 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Detective에 대한 서비스 연결 역할 권한

Detective는 AWSServiceRoleForDetective라는 서비스 연결 역할을 사용합니다. Detective가 사용자를 대신하여 AWS Organizations 정보에 액세스할 수 있도록 허용합니다.

AWSServiceRoleForDetective 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `detective.amazonaws.com`

AWSServiceRoleForDetective 서비스 역할 연결 역할은 `AmazonDetectiveServiceLinkedRolePolicy`관리형 정책을 사용합니다.

`AmazonDetectiveServiceLinkedRolePolicy` 정책 업데이트에 대한 자세한 내용은 AWS 관리형 정책에 대한 Amazon Detective 업데이트를 참조하세요. 이 정책의 변경 사항에 대한 자동 알림을 받으려면 Detective 문서 기록 페이지에서 RSS 피드를 구독하세요.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Detective에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API에서 조직의 Detective 관리자 계정을 지정하면 Detective가 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 조직의 Detective 관리자 계정을 지정할 때 Detective는 서비스 연결 역할을 다시 생성합니다.

Detective에 대한 서비스 연결 역할 편집

Detective는 AWSServiceRoleForDetective 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Detective에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려 할 때 Detective 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도합니다.

AWSServiceRoleForDetective에서 사용하는 Detective 리소스 삭제

1. Detective 관리자 계정을 제거합니다. the section called “Detective 관리자 계정 지정”을(를) 참조하세요.
2. Detective 관리자 계정을 지정한 각 리전에서 이 절차를 반복합니다.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForDetective 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

Detective 서비스 연결 역할에 대해 지원되는 리전

Detective에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트 섹션을 참조하십시오.

Amazon Detective 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Detective 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다. AWS Identity and Access Management(IAM)로 작업할 때 액세스 거부 문제 또는 유사한 문제가 발생하는 경우 IAM 사용 설명서의 IAM 문제 해결 주제를 참조하세요.

Detective에서 작업을 수행할 권한이 없음

에서 작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 사용자 이름과 암호를 제공한 사람입니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 동작 그래프의 멤버 계정이 되기 위한 초대를 수락하려고 하지만 `detective:AcceptInvitation` 권한이 없는 경우에 발생합니다.

```
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
```

이 경우, Mateo는 `arn:aws:detective:us-east-1:444455556666:graph:567856785678` 작업을 사용하여 `detective:AcceptInvitation` 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Detective에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 Detective에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 `iam:PassRole`작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사람이 내 Detective 리소스에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- Detective에서 이러한 기능을 지원하는지 여부를 알아보려면 Amazon Detective가 IAM과 작동하는 방식 섹션을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 리소스에 대한 액세스 권한을 타사에 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Amazon Detective에 대한 규정 준수 확인

Amazon Detective는 AWS 보증 프로그램의 범위에 있습니다. 자세한 내용은 Health Information Trust Alliance Common Security Framework(HITRUST) CSF참조하세요.

특정 규정 준수 프로그램의 범위에 속하는 AWS 서비스 목록은 규정 준수 프로그램 AWS 범위에 속하는 서비스 규정 준수 프로그램 참조하세요. 일반 정보는 AWS 규정 준수 프로그램 참조하세요.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 AWS 아티팩트에서 보고서 다운로드.

AWS 는 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 - 보안 및 규정 준수 안내서는 아키텍처 고려 사항에 대해 설명하고 에서 보안 및 규정 준수 중심 기준 환경을 배포하기 위한 단계를 제공합니다 AWS.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 - 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.

- AWS Security Hub CSPM - 이 AWS 서비스는 보안 업계 표준 및 모범 사례 준수를 확인하는 데 도움이 AWS 되는 의 보안 상태를 포괄적으로 보여줍니다.

Amazon Detective의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며,이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 외에도 Detective는 Amazon DynamoDB 및 Amazon Simple Storage Service(Amazon S3)에 내장된 복원력을 사용합니다. 자세한 내용은 Amazon DynamoDB의 복원력 및 재해 복구와 Amazon Simple Storage Service의 복원력을 참조하세요.

Detective 아키텍처는 단일 가용 영역의 장애에도 탄력적입니다. 이러한 복원성은 Detective에 내장되어 있으며 구성이 필요하지 않습니다.

Amazon Detective의 인프라 보안

관리형 서비스인 Amazon Detective;는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요 AWS .

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Detective에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

Amazon Detective 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

인터페이스 VPC 엔드포인트를 생성하여 VPC와 Amazon Detective 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 인터넷 게이트웨이AWS PrivateLink, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 비공개로 Detective APIs에 액세스할 수 있는 기술로 구동됩니다. VPC의 인스턴스는 Detective APIs. VPC와 Detective 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 Elastic Network Interfaces로 표현됩니다.

자세한 내용은 AWS PrivateLink 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하십시오.

Detective VPC 엔드포인트에 대한 고려 사항

Detective에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 인터페이스 엔드포인트 속성 및 제한 사항을 검토해야 합니다.

Detective는 VPC에서 모든 API 작업을 호출할 수 있도록 지원합니다.

Detective는 다음 리전에서 FIPS를 지원합니다.

- 미국 동부(버지니아 북부)
- 미국 동부(오하이오)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오레곤)
- 캐나다(중부)

Detective용 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 사용하여 Detective 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 AWS PrivateLink 안내서의 인터페이스 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 사용하여 Detective용 VPC 엔드포인트를 생성합니다.

- com.amazonaws.*region*.detective
- com.amazonaws.*region*.detective-fips

엔드포인트에 대해 프라이빗 DNS를 활성화하는 경우 리전의 기본 DNS 이름, 예를 들어를 사용하여 Detective에 API 요청을 할 수 있습니다`api.detective.us-east-1.amazonaws.com`. 자세한 내용은의 Amazon Detective 엔드포인트를 참조하세요Amazon Web Services 일반 참조.

자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트를 통해 서비스 액세스를 참조하십시오.

Detective에 대한 VPC 엔드포인트 정책 생성

Detective에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 위탁자.
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스

자세한 내용은 AWS PrivateLink 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하십시오.

예: Detective 작업에 대한 VPC 엔드포인트 정책

다음은 Detective에 대한 엔드포인트 정책의 예입니다. 엔드포인트에 연결되면이 정책은 모든 리소스의 모든 보안 주체에 대해 나열된 Detective 작업에 대한 액세스 권한을 부여합니다.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "detective:ListGraphs",
            "detective:ListMembers"
         ],
         "Resource":"*"
      }
   ]
```

```
}
```

공유 서브넷

공유하는 서브넷의 VPC 엔드포인트는 생성, 설명, 수정 또는 삭제할 수 없습니다. 그러나 공유하는 서브넷의 VPC 엔드포인트를 사용할 수는 있습니다. VPC 공유에 관한 자세한 내용은 Amazon VPC 사용 설명서의 다른 계정과 VPC 공유를 참조하십시오.

Detective의 보안 모범 사례

Detective는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 사용자의 환경에 적절하지 않거나 충분하지 않을 수 있으므로 규정이 아닌 참고용으로만 사용하세요.

Detective의 경우 보안 모범 사례는 동작 그래프에서의 계정 관리와 관련이 있습니다.

Detective 관리자 계정 모범 사례

Detective 동작 그래프에 멤버 계정을 초대할 때는 감독하는 계정만 초대합니다.

동작 그래프에 대한 액세스를 제한합니다. AmazonDetectiveFullAccess 정책이 있는 사용자는 모든 Detective 작업에 대한 액세스 권한을 부여할 수 있습니다. 이러한 권한이 있는 보안 주체는 멤버 계정을 관리하고, 동작 그래프에 태그를 추가하고, Detective를 사용하여 조사할 수 있습니다. 동작 그래프에 액세스할 수 있는 사용자는 멤버 계정에 대한 모든 조사 결과를 볼 수 있습니다. 이러한 조사 결과로 인해 민감한 보안 정보가 노출될 수 있습니다.

멤버 계정의 모범 사례

동작 그래프에 대한 초대를 받으면 초대의 출처를 확인해야 합니다.

초대를 보낸 관리자 AWS 계정의 계정 식별자를 확인합니다. 계정이 누구의 소유인지 알고 있는지, 초대 계정에 보안 데이터를 모니터링할 정당한 이유가 있는지 확인합니다.

를 사용하여 Amazon Detective API 호출 로깅 AWS CloudTrail

Detective는 Detective의 사용자 AWS CloudTrail, 역할 또는 서비스에서 수행한 작업에 대한 레코드를 제공하는 AWS 서비스인 와 통합됩니다. 는 Detective에 대한 모든 API 호출을 이벤트로 CloudTrail 캡처합니다. 캡처된 호출에는 Detective 콘솔의 호출과 Detective API 작업에 대한 코드 호출이 포함됩니다.

- 추적을 생성하는 경우 Detective에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다.
- 추적을 구성하지 않은 경우에도 콘솔의 이벤트 기록 에서 CloudTrail 최신 이벤트를 볼 수 있습니다.

에서 수집한 정보를 사용하여 다음을 확인할 CloudTrail수 있습니다.

- Detective에 대한 요청
- 요청을 보낸 IP 주소
- 요청한 사람
- 요청한 시기
- 요청에 대한 추가 세부 정보

에 대한 자세한 내용은 AWS CloudTrail 사용 설명서 섹션을 CloudTrail참조하세요.

의 탐지 정보 CloudTrail

CloudTrail 는 AWS 계정을 생성할 때 계정에서 활성화됩니다. Detective에서 활동이 발생하면 해당 활동이 다른 AWS 서비스 이벤트와 CloudTrail 함께 이벤트 기록 에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록을 사용하여 CloudTrail 이벤트 보기를 참조하세요.

Detective에 대한 이벤트를 포함하여 AWS 계정의 이벤트에 대한 지속적인 기록을 위해 추적을 생성합니다. 추적을 사용하면 CloudTrail 가 Amazon S3 버킷에 로그 파일을 전달할 수 있습니다.

콘솔에서 추적을 생성하면 기본적으로 모든 AWS 지역에 추적이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 기록하고 지정한 Amazon S3 버킷에 로그 파일을 전달합니다. CloudTrail 로

그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 작업하도록 다른 AWS 서비스를 구성할 수도 있습니다.

자세한 내용은 다음 자료를 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

CloudTrail 는 Detective API 참조 에 문서화된 모든 Detective 작업을 기록합니다.

예를 들어 `CreateMembers`, `AcceptInvitation`및 `DeleteMembers` 작업에 대한 호출은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 요청이 이루어졌는지 여부
- 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 다른 AWS 서비스에서 요청을 했는지 여부

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Detective 로그 파일 항목 이해

추적은 사용자가 지정한 Amazon S3 버킷에 로그 파일로 이벤트를 전달할 수 있도록 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함됩니다.

이벤트는 모든 소스로부터 단일 요청을 나타냅니다. 이벤트에는 요청된 작업, 작업 날짜 및 시간, 요청 파라미터 등에 대한 정보가 포함됩니다. on. CloudTrail log 파일은 퍼블릭 API 호출의 정렬된 스택 추적이 아니므로 항목이 특정 순서로 표시되지 않습니다.

다음 예제에서는 `AcceptInvitation` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
    {
```

```
            "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": []
        },
```

Amazon Detective 리전 및 할당량

Amazon Detective를 사용할 때는 이러한 할당량을 숙지합니다.

Detective 리전 및 엔드포인트

Detective를 사용할 수 AWS 리전 있는 위치 목록을 보려면 Detective 서비스 엔드포인트를 참조하십시오.

Detective 할당량

Detective에는 다음과 같은 할당량이 있으며 이는 구성할 수 없습니다.

Resource	할당량	설명
멤버 계정의 수	1,200	관리자 계정이 동작 그래프에 추가할 수 있는 멤버 계정의 수.
동작 그래프 데이터 볼륨 - 볼륨 경고	일일 9TB	동작 그래프 데이터 볼륨이 일일 9TB를 초과하는 경우 Detective는 동작 그래프가 최대 허용 볼륨에 가까워지고 있다는 경고를 표시합니다.
동작 그래프 데이터 볼륨 - 새로운 계정 없음	일일 10TB	동작 그래프 데이터 볼륨이 일일 10TB를 초과하는 경우 동작 그래프에 새 멤버 계정을 추가할 수 없습니다.
동작 그래프 데이터 볼륨 - 동작 그래프에 데이터 수집 중지	일일 15TB	동작 그래프 데이터 볼륨이 일일 15TB를 초과하는 경우 Detective는 동작 그래프에 대한 데이터 수집을 중지합니다. 일일 15TB는 일반적인 데이터 볼륨과 데이터 볼륨 급증을 모두 반영합니다. 데이터 수집을 다시 활성화하려면 지원를 문의해야 합니다.

Internet Explorer 11은 지원되지 않음

Internet Explorer 11에서는 Detective를 사용할 수 없습니다.

동작 그래프의 태그 관리

태그는 특정 유형의 Detective AWS 리소스를 비롯한 리소스에 정의하여 할당할 수 있는 선택적 레이블입니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별, 분류, 관리하는 데 도움이 됩니다. 예를 들어 태그를 사용하여 정책을 적용하고, 비용을 할당하고, 리소스 버전을 구분하거나, 특정 규정 준수 요구 사항 또는 워크플로를 지원하는 리소스를 식별할 수 있습니다.

동작 그래프에 태그를 할당할 수 있습니다. 그런 다음 IAM 정책의 태그 값을 사용하여 Detective의 동작 그래프 기능에 대한 액세스를 관리할 수 있습니다. the section called “Detective 동작 그래프 태그를 기반으로 한 권한 부여”을 참조하세요.

태그를 비용 보고 도구로 사용할 수도 있습니다. 예를 들어 보안과 관련된 비용을 추적하기 위해 Detective 행동 그래프, AWS Security Hub CSPM 허브 리소스 및 Amazon GuardDuty 탐지기에 동일한 태그를 할당할 수 있습니다. AWS Cost Explorer에서는 해당 태그를 검색하여 해당 리소스의 비용을 통합적으로 확인할 수 있습니다.

행동 그래프의 태그 보기

동작 그래프의 태그는 일반 페이지에서 관리할 수 있습니다.

Console

동작 그래프에 할당된 태그 목록 보기

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.

Detective API, AWS CLI

Detective API 또는 AWS Command Line Interface 를 사용하여 행동 그래프의 태그 목록을 가져올 수 있습니다.

행동 그래프의 태그 목록을 가져오려면 (DetectiveAPI,) AWS CLI

- DetectiveAPI: 작전을 사용하세요. `ListTagsForResource` 행동 그래프를 ARN 입력해야 합니다.
- AWS CLI: 명령줄에서 `list-tags-for-resource` 명령을 실행합니다.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

예

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

행동 그래프에 태그 추가

Console

일반 페이지의 태그 목록에서 동작 그래프에 태그 값을 추가할 수 있습니다.

동작 그래프에 태그 추가

1. 새 태그 추가를 선택합니다.
2. 키에는 태그의 이름을 입력합니다.
3. 값에는 태그 값을 입력합니다.

Detective API, AWS CLI

Detective API 또는 를 사용하여 행동 AWS CLI 그래프에 태그 값을 추가할 수 있습니다.

행동 그래프에 태그를 추가하려면 (DetectiveAPI,) AWS CLI

- DetectiveAPI: 작전을 사용하세요. `TagResource` 행동 ARN 그래프와 추가할 태그 값을 입력합니다.
- AWS CLI: 명령줄에서 `tag-resource` 명령을 실행합니다.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior
 graph ARN> --tags '{"TagName":"TagValue"}'
```

예

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

행동 그래프에서 태그 제거

Console

일반 페이지의 목록에서 태그를 제거하려면 해당 태그의 제거 옵션을 선택합니다.

Detective API, AWS CLI

Detective API 또는 를 사용하여 행동 AWS CLI 그래프에서 태그 값을 제거할 수 있습니다.

행동 그래프에서 태그를 제거하려면 (DetectiveAPI,) AWS CLI

- DetectiveAPI: 작전을 사용하세요. `UntagResource` 행동 그래프와 ARN 제거할 태그의 이름을 입력합니다.
- AWS CLI: 명령줄에서 `untag-resource` 명령을 실행합니다.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys
 "TagName"
```

예

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Amazon Detective 비활성화

동작 그래프의 관리자 계정은 Detective 콘솔, Detective API 또는 AWS Command Line Interface에서 Amazon Detective를 비활성화할 수 있습니다. Detective를 비활성화하면 동작 그래프 및 관련 Detective 데이터가 삭제됩니다.

동작 그래프를 삭제한 후에는 복원할 수 없습니다.

내용

- Detective 비활성화(콘솔)
- Detective 비활성화(Detective API, AWS CLI)
- 리전 간 Detective 비활성화(GitHub의 Python 스크립트)

Detective 비활성화(콘솔)

AWS Management Console에서 Amazon Detective를 비활성화할 수 있습니다.

Amazon Detective를 비활성화하려면(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 일반 페이지의 Amazon Detective 비활성화에서 Amazon Detective 비활성화를 선택합니다.
4. 확인 메시지가 나타나면 **`disable`**을 입력합니다.
5. Amazon Detective 비활성화를 선택합니다.

Detective 비활성화(Detective API, AWS CLI)

Detective API 또는 AWS Command Line Interface에서 Amazon Detective를 비활성화할 수 있습니다. 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

Detective(Detective API AWS CLI)를 비활성화하려면

- Detective API: `DeleteGraph` 작업을 사용합니다. 그래프 ARN을 제공해야 합니다.
- AWS CLI: 명령줄에서 `delete-graph` 명령을 실행합니다.

```
aws detective delete-graph --graph-arn <graph ARN>
```

예제:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

리전 간 Detective 비활성화(GitHub의 Python 스크립트)

Detective는 GitHub에서 오픈 소스 스크립트를 제공하여 지정된 리전 목록의 관리자 계정에 대해 Detective를 비활성화할 수 있습니다.

GitHub 스크립트를 구성하고 사용하는 방법에 대한 자세한 내용은 the section called “Amazon Detective Python 스크립트” 섹션을 참조하세요.

Detective 사용 설명서에 대한 문서 기록

다음 테이블에서는 Detective의 최신 릴리스가 발표된 이후 이 설명서에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

- 최종 설명서 업데이트: 2025년 2월 20일

변경 사항	설명	날짜
새로운 기능 - VPC 엔드포인트에 대한 지원 추가	이제 Detective가와 통합 AWS PrivateLink 되고 VPC 엔드포인트를 지원합니다. AWS PrivateLink 통합에 대한 자세한 내용은 Amazon Detective 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.	2025년 9월 30일
Amazon GuardDuty 공격 시퀀스 결과에 대한 지원 추가	Detective는 GuardDuty 확장 위협 탐지와 관련된 조사 결과 유형에 대한 지원을 추가했습니다. GuardDuty는 API 활동 및 GuardDuty 조사 결과 탐지와 같은 특정 일련의 여러 작업이 잠재적으로 의심스러운 활동과 일치할 때 공격 시퀀스를 탐지합니다. 확장 위협 탐지 및 공격 시퀀스 조사 결과 유형에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 확장 위협 탐지를 참조하세요.	2025년 2월 20일
Amazon GuardDuty IAM 결과에 대한 지원 추가	Detective는 AWS 계정 환경에 나열된에 대해 생성된 제한된 사용자 자격 증명이 요청을 하는 데 사용될 때 경고	2025년 2월 4일

	하는 새로운 GuardDuty 결과 유형에 대한 지원을 추가했습니다 AWS 서비스. 자세한 내용은 Amazon GuardDuty 사용 설명서Policy:IAMUser/ShortTermRootCredentialUsage의 섹션을 참조하세요.	
새로운 특성	Detective Finding 그룹 시각화에 타임라인 레이아웃이 추가되었습니다. 결과에 대한 재생 버튼 기능과 심각도 기반 필터링을 도입했습니다. 이러한 개선 사항을 통해 이벤트 진행 상황을 더 잘 이해하고, 중요한 문제의 우선순위를 정하고, 보다 효율적인 보안 조사를 수행할 수 있습니다.	2024년 12월 27일
Amazon GuardDuty 결과에 대한 지원 추가	Detective는 AWS 환경 내 Amazon EC2 인스턴스 또는 컨테이너 워크로드에서 의심스러운 명령이 실행될 때 알려주는 다음 세 가지 GuardDuty 결과 유형에 대한 지원을 추가했습니다. • Discovery:Runtime/SuspiciousCommand • Persistence:Runtime/SuspiciousCommand • PrivilegeEscalation:Runtime/SuspiciousCommand	2024년 11월 6일

Amazon GuardDuty 결과에 대한 지원 추가	이제 Detective는 다음 GuardDuty 런타임 모니터링 결과 유형에 대한 지원을 제공합니다. • `Execution:Runtime/SuspiciousShell` • `PriviliegeEscalation:Runtime/ElevationToRoot`	2024년 8월 27일
Amazon GuardDuty 결과에 대한 지원 추가	이제 Detective는 S3에 대한 GuardDuty 맬웨어 보호를 지원합니다. 이렇게 하면 Amazon S3 버킷에 새로 업로드된 객체에서 잠재적 멀웨어 및 의심스러운 업로드가 있는지 스캔하고 다운스트림 프로세스에 수집되기 전에 격리 조치를 취할 수 있습니다.	2024년 7월 9일
업데이트된 기능	Detective는 더 쉬운 데이터 해석을 위해 향상된 시각화를 제공하기 위해 조사 결과 그룹 시각화 패널에 새로운 방사형 레이아웃을 추가했습니다.	2024년 6월 26일
새로운 Security Lake 소스 버전	소스 버전 1(OCSF 1.0.0-rc.2) 외에도 Detective는 이제 Detective에서 지원하는 Security Lake 소스에 대해 소스 버전 2(OCSF 1.1.0)의 데이터를 수집합니다.	2024년 5월 15일

새 Security Lake 로그 소스	Security Lake와의 Detective 통합을 사용하여 Amazon EKS 감사 로그에서 로그 및 이벤트를 수집할 수 있습니다.	2024년 5월 15일
문서 업데이트	Amazon Detective 관리 안내서의 콘텐츠가 이제 Amazon Detective 사용 설명서로 통합되었습니다. Amazon Detective 관리 안내서는 2024년 5월 8일에 표준 지원이 종료됩니다.	2024년 4월 15일
Amazon GuardDuty 결과에 대한 지원 추가	Detective는 이제 다음 GuardDuty 런타임 모니터링 결과 유형에 대한 지원을 제공합니다. • `Execution:Runtime/MaliciousFileExecuted` • `Execution:Runtime/SuspiciousTool` • `DefenseEvasion:Runtime/PtraceAntiDebugging` • `Execution:Runtime/SuspiciousCommand` • `DefenseEvasion:Runtime/SuspiciousCommand`	2024년 4월 5일

Amazon GuardDuty 멤버십 요구 사항 제거	Amazon Detective를 활성화하기 위해 더 이상 GuardDuty 고객이 아니어도 됩니다. Detective를 활성화하기 전에 48시간 동안 계정에서 GuardDuty를 활성화해야 하는 요구 사항이 제거되었습니다.	2024년 2월 2일
Amazon GuardDuty 결과에 대한 지원 추가	Detective는 GuardDuty EC2 런타임 모니터링 결과 유형에 대한 지원을 ECS 및 EC2 리소스로 확장합니다.	2024년 1월 30일
업데이트된 기능	이제 조사하려는 특정 리소스에 대해 조사 페이지에서 Detective 조사를 실행할 수 있습니다. Detective는 조사 결과 및 조사 결과 그룹 활동을 기반으로 리소스를 추천합니다. 탐지 조사를 사용하면 침해 지표를 사용하여 IAM 사용자 및 IAM 역할을 조사할 수 있으므로 리소스가 보안 인시던트와 관련이 있는지 확인하는 데 도움이 될 수 있습니다.	2024년 1월 16일
업데이트된 기능	이제 추천 리소스의 조사 페이지에서 Detective 조사를 실행할 수 있습니다. Detective는 조사 결과 및 조사 결과 그룹 활동을 기반으로 리소스를 추천합니다. 탐지 조사를 사용하면 침해 지표를 사용하여 IAM 사용자 및 IAM 역할을 조사할 수 있으므로 리소스가 보안 인시던트와 관련이 있는지 확인하는 데 도움이 될 수 있습니다.	2023년 12월 26일

Detective가 공유 VPC의 흐름 트래픽을 읽는 방식의 변경 사항	공유 Amazon VPC를 사용하는 경우, Detective에서 모니터링하는 트래픽의 변화를 확인할 수 있습니다. 전체 VPC 흐름량에 대한 활동 세부 정보의 변경 사항을 검토하여 적용 범위에 미치는 잠재적 영향을 이해하고, Detective에서 예상 비용을 계산하는 방법을 검토하여 서비스 비용에 어떤 영향을 미칠 수 있는지 이해하는 것이 좋습니다.	2023년 12월 20일
리전별 가용성	Security Lake와의 Detective 통합을 사용할 수 있는 리전 목록에 유럽(스톡홀름), 유럽(파리) 및 캐나다(중부) AWS 리전이 추가되었습니다.	2023년 12월 8일
새로운 특성	Detective 조사를 통해 손상 지표를 사용하여 IAM 사용자 및 IAM 역할을 조사하고 리소스가 보안 인시던트에 연루되어 있는지 확인할 수 있습니다.	2023년 11월 26일
새로운 특성	Detective는 기본적으로 생성형 인공 지능(생성형 AI)을 기반으로 조사 결과 그룹에 대한 조사 결과 그룹 요약을 자동으로 생성합니다. 조사 결과 그룹 요약은 조사 결과와 영향을 받는 리소스 간의 관계를 신속하게 분석한 다음 잠재적 위협을 자연어로 요약합니다.	2023년 11월 26일

새로운 특성	Security Lake와의 Detective 통합을 통해 Security Lake에 저장된 원시 로그 데이터를 쿼리하고 검색할 수 있습니다. 이 통합을 사용하면 CloudTrail 관리 이벤트 및 Amazon Virtual Private Cloud(VPC) 흐름 로그에서 로그와 이벤트를 수집할 수 있습니다.	2023년 11월 26일
보안 장에 관리형 정책 정보 추가	Detective 조사 및 조사 결과 그룹 요약 작업을 `AmazonDetectiveInvestigatorAccess` 정책에 추가했습니다.	2023년 11월 26일
조사 결과 개요 보기	이제 Detective는 조사 결과가 대규모 활동과 상관관계가 있는 경우 해당 조사 결과 그룹으로 이동하라는 알림을 표시합니다.	2023년 9월 18일
Amazon Detective 엔드포인트 및 할당량	이제 이스라엘(텔아비브) 리전에서 Detective를 사용할 수 있습니다.	2023년 8월 25일
향상된 조사 결과 그룹 시각화	이제 Detective 조사 결과 그룹 시각화에 집계된 조사 결과가 포함된 조사 결과 그룹이 포함되므로 관련 증거, 엔터티 및 조사 결과를 더 효율적으로 분석할 수 있습니다.	2023년 8월 8일
향상된 조사 결과 그룹	이제 조사 결과 그룹에는 Amazon Inspector의 취약성 조사 결과가 포함됩니다.	2023년 6월 13일

Amazon GuardDuty 람다 보호에 대한 지원 추가	이제 Detective는 GuardDuty Lambda 보호를 지원합니다.	2023년 5월 26일
AWS 보안 조사 결과를 새로운 선택적 데이터 소스 패키지로 추가했습니다.	이제 Detective는 AWS 보안 조사 결과를 선택적 데이터 소스 패키지로 제공합니다. 이 선택적 데이터 소스 패키지를 사용하면 Detective가 Security Hub CSPM에서 데이터를 수집하고 해당 데이터를 동작 그래프에 추가할 수 있습니다.	2023년 5월 16일
Amazon GuardDuty EKS 런타임 모니터링 조사 결과 유형에 대한 지원 추가	이제 Detective는 GuardDuty EKS 런타임 모니터링 조사 결과 유형을 지원합니다.	2023년 5월 3일
Amazon GuardDuty RDS 보호 조사 결과 유형에 대한 지원 추가	이제 Detective는 GuardDuty RDS 보호 조사 결과 유형을 지원합니다.	2023년 4월 20일
추가 Amazon GuardDuty 조사 결과 유형에 대한 지원 추가	이제 Detective는 `DefenseEvasion: EC2UnusualDNSResolver` , `DefenseEvasion: EvasionEC2UnusualDoHActivity` , `DefenseEvasion: DefenseEvasionEC2UnusualDoTActivity` 같은 추가 GuardDuty 조사 결과 유형에 대한 프로필을 제공합니다.	2023년 8월 12일
사용자가 특정 사용 사례에 적합한 AWS 관리형 정책을 선택할 수 있도록 Detective 콘솔에 새 콘솔 패널이 추가되었습니다.	Detective는 안전한 관리형 정책을 제공합니다. 필요한 권한을 선택합니다.	2023년 4월 3일

EKS 클러스터의 VPC 흐름 트래픽 표시	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 이용한 Amazon Virtual Private Cloud(VPC) 흐름 트래픽에 대한 새로운 섹션을 추가했습니다.	2023년 3월 2일
이제 조사 결과 그룹에 Detective 동작 그래프의 동적 시각적 표현이 포함됨됨	이제 Detective 조사 결과 그룹에는 Detective의 동작 그래프를 동적으로 시각적으로 표현하여 조사 결과 그룹 내 엔터티와 조사 결과 간의 관계를 강조할 수 있습니다.	2023년 2월 28일
Detective 요약 페이지 및 검색 결과 페이지에서 데이터를 내보냅니다. 데이터는 쉼표로 구분된 값(CSV) 형식으로 내보내집니다.	이제 Detective는 Detective 콘솔에서 브라우저로 데이터를 내보내는 옵션을 제공합니다.	2023년 2월 7일
EKS Amazon EKS 워크로드를 위한 전체 VPC 흐름량 추가	이제 Detective는 이제 Amazon Elastic Kubernetes Service(Amazon EKS) 워크로드의 Amazon Virtual Private Cloud(VPC) 흐름 로그에 대한 시각적 요약과 분석을 추가합니다.	2023년 1월 19일

보안 장에 관리형 정책 정보 추가	이제 Detective는 AmazonDetectiveFullAccess 정책을 통해 GuardDuty 조사 결과 가져오기 작업을 지원합니다. 이제 보안 장에서는 Detective의 새로운 관리형 정책인 AmazonDetectiveMemberAccess 및 AmazonDetectiveInvestigatorAccess에 대한 세부 정보를 제공합니다.	2023년 1월 17일
데이터 보존 추가	Detective를 사용하면 최대 1년 분량의 과거 이벤트 데이터에 액세스할 수 있습니다.	2022년 12월 20일
요약 페이지에 범위 시간을 조정하는 옵션을 추가했습니다.	이제 Detective는 범위 시간을 조정할 수 있는 옵션을 제공하므로 이전 365일 중 24시간 동안의 활동을 볼 수 있습니다.	2022년 10월 5일
조사 결과 또는 엔터티 검색	이제 Detective는 대소문자를 구분하지 않는 검색 기능을 제공합니다.	2022년 10월 3일
범위 타임스탬프를 설정하는 기능 추가	이제 Detective는 범위 타임스탬프 형식 기본 설정을 구성하는 방법을 제공합니다. 이 기본 설정은 Detective 내의 모든 타임스탬프에 적용됩니다.	2022년 10월 3일

조사 결과 그룹과 관련된 용어 추가	이제 Detective는 관련 조사 결과를 단일 디스플레이로 연결하는 조사 결과 그룹을 지원하여 사용자 환경의 잠재적 악의적 활동을 조사할 수 있습니다. 조사 결과 그룹 프로필에서 엔터티 프로필 및 해당 그룹과 관련된 조사 결과 개요로 피벗할 수 있습니다.	2022년 8월 3일
Amazon EKS 감사 로그와 관련된 새 프로필 추가	이제 Detective는 Amazon EKS 클러스터, 컨테이너 이미지, Kubernetes 포드, Kubernetes 객체 등 컨테이너 관련 엔터티와 관련된 활동을 조사할 수 있는 프로필을 제공합니다.	2022년 7월 26일
새 선택적 데이터 소스 추가	이제 Detective는 EKS 감사 로그를 선택적 데이터 소스 패키지로 지원합니다. 관리자 계정은 기존 동작 그래프에 이 새 데이터 소스를 활성화할 수 있습니다. 이 날짜 이후에 생성된 그래프에는 이 데이터 소스가 기본적으로 활성화됩니다. 관리자는 언제든지 이 데이터 소스를 수동으로 비활성화할 수 있습니다.	2022년 7월 26일

Detective를 위한 새 서비스 연결 역할 및 관리형 정책	이제 Detective에는 서비스 연결 역할 `AWSServiceRoleForDetective` 가 있습니다. 서비스 연결 역할을 통해 사용자를 대신하여 Organizations 데이터에 액세스할 수 있습니다. 역할은 새 `AmazonDetectiveServiceLinkedRolePolicy` 관리형 정책을 사용합니다.	2021년 12월 16일
와의 통합 추가 AWS Organizations	이제 Detective는 Organizations와 통합됩니다. 조직 관리 계정은 조직의 Detective 관리자 계정을 지정합니다. Detective 관리자 계정은 조직의 모든 계정을 볼 수 있고, 조직 동작 그래프에서 해당 계정을 멤버 계정으로 활성화할 수 있습니다.	2021년 12월 16일
조사 결과 프로필을 조사 결과 개요로 대체	조사 결과 프로필에 관련 리소스의 활동을 분석하는 시각화가 포함되었습니다. 새로운 조사 결과 개요에 GuardDuty에서 수집한 조사 결과 세부 정보와 관련 엔터티 목록이 포함되었습니다. 조사 결과 개요에서 관련 엔터티의 프로필로 피벗할 수 있습니다.	2021년 9월 20일

지원되는 GuardDuty 조사 결과 유형에 대한 제한 제거	Detective는 더 이상 선택된 GuardDuty 조사 결과 유형에만 국한되지 않습니다. Detective는 모든 조사 결과 유형에 대한 조사 결과 세부 정보를 자동으로 수집하고 관련 엔터티의 엔터티 프로필에 대한 액세스를 제공합니다.	2021년 9월 20일
관련 조사 결과 프로필 패널의 조사 결과 세부 정보에 연결	엔터티 프로필에서 관련 조사 결과 목록에서 조사 결과를 선택하면 오른쪽 패널에 조사 결과 세부 정보가 표시됩니다. 범위 시간은 조사 결과 기간으로 설정됩니다.	2021년 9월 20일
Detective에서 사용 가능한 엔터티 유형에 S3 버킷 추가	이제 Detective는 S3 버킷에 대한 프로필을 제공합니다. S3 버킷 프로필은 S3 버킷과 상호 작용한 보안 주체 및 이들이 S3 버킷에서 수행한 API 작업에 대한 세부 정보를 제공합니다.	2021년 9월 20일
Splunk에서 Detective URL을 생성하는 새로운 옵션	Splunk Trumpet 프로젝트를 사용하면 Splunk로 AWS 콘텐츠를 보낼 수 있습니다. 이제 프로젝트에 Detective URL을 추가하여 GuardDuty 조사 결과에 대한 프로필로 이동할 수 있습니다.	2021년 9월 8일

계정 및 역할의 활동 세부 정보에서 AKID 대체	이제 계정 프로필에서 전체 API 직접 호출량의 활동 세부 정보에 액세스 키 식별자(AKID) 대신 사용자 또는 역할이 표시됩니다. 이제 역할 프로필에서 전체 API 직접 호출량의 활동 세부 정보에 AKID 대신 역할 세션이 표시됩니다. 이러한 변경 이전에 발생한 활동의 경우 호출자는 알 수 없는 리소스로 표시됩니다.	2021년 7월 14일
API 직접 호출에 대한 정보에 호출 서비스 추가	이제 Detective 콘솔에서 API 직접 호출 정보에 호출을 실행한 서비스가 포함됩니다. 전체 API 직접 호출량, 새로 관찰된 API 직접 호출, 볼륨이 증가된 API 직접 호출 목록에 서비스 열을 추가했습니다. 전체 API 직접 호출량 및 새로 관찰된 지리적 위치에 대한 활동 세부 정보에서 API 메서드는 해당 메서드를 발행한 서비스 아래에 그룹화됩니다. 이러한 변경 이전에 발생한 활동의 경우 API 메서드는 알 수 없는 서비스 아래에 그룹화됩니다.	2021년 7월 14일
사용자, 역할 및 역할 세션을 위한 새로운 리소스 상호 작용 탭	사용자, 역할 및 역할 세션을 위한 리소스 상호 작용 탭에는 해당 엔터티와 관련된 역할 수임 활동에 대한 정보가 포함되어 있습니다. 역할 세션의 경우 이 탭은 새 탭입니다. 사용자 및 역할을 위한 이 탭은 새 콘텐츠가 포함된 기존 탭입니다.	2021년 6월 29일

동작 그래프 데이터 볼륨 할당량 값 추가	동작 그래프의 데이터 볼륨 할당량이 증가되었습니다. Detective는 일일 3.24TB에서 경고를 보냅니다. 일일 3.6TB에서는 새 계정을 추가할 수 없습니다. Detective는 일일 4.5TB에서 동작 그래프에 데이터를 더 이상 수집하지 않습니다.	2021년 6월 10일
Python 스크립트 옵션에 태그 값 추가	이제 Detective Python script `enableDetective.py` 을 사용하여 Detective를 활성화하면 동작 그래프에 태그 값을 할당할 수 있습니다.	2021년 5월 19일
데이터 볼륨 검사를 통과한 멤버 계정을 자동으로 활성화하는 기능 추가	멤버 계정이 초대를 수락하면 Detective에서 해당 데이터로 인해 동작 그래프 데이터 볼륨이 할당량을 초과하지 않는지 확인할 때까지 멤버 계정의 상태는 수락(활성화되지 않음)으로 표시됩니다. 데이터 볼륨에 문제가 없는 경우 Detective는 자동으로 상태를 수락(활성화)으로 변경합니다. 참고로 현재 수락(활성화되지 않음) 상태인 기존 멤버 계정은 자동으로 활성화할 수 없습니다.	2021년 5월 12일
보안 장에 관리형 정책 정보 추가	보안 장의 새 섹션에서 Detective의 관리형 정책에 대한 세부 정보를 제공합니다. Detective는 현재 단일 관리형 정책 `AmazonDetectiveFullAccess` 를 제공합니다.	2021년 5월 10일

멤버 계정 목록의 데이터 볼륨 값 변경	이제 계정 관리 페이지에서 멤버 계정 목록에 각 멤버 계정의 일일 데이터 볼륨이 표시됩니다. 이전에는 목록에 볼륨이 허용된 전체 볼륨의 백분율로 표시되었습니다.	2021년 4월 29일
멤버 계정 관리 옵션 수정	계정 관리 메뉴를 작업 메뉴로 대체했습니다. 개별 계정을 추가하는 옵션과 .csv 파일에서 계정을 추가하는 옵션을 결합했습니다. 계정 관리에서 계정 활성화를 작업 옆의 별도 옵션으로 이동했습니다.	2021년 4월 5일
동작 그래프 태그 및 태그 기반 권한 부여 추가	Detective를 활성화하면 동작 그래프에 태그를 추가할 수 있습니다. 일반 페이지에서 동작 그래프에 대한 태그를 관리할 수 있습니다. Detective는 태그 값을 기반으로 한 권한 부여도 지원합니다.	2021년 3월 31일

추가 Amazon GuardDuty 조사 결과 유형에 대한 지원 추가	이제 Detective는 `CredentialAccess:IAMUser/AnomalousBehavior`, `DefenseEvasion:IAMUser/AnomalousBehavior`, `Discovery:IAMUser/AnomalousBehavior`, `Exfiltration:IAMUser/AnomalousBehavior`, `Impact:IAMUser/AnomalousBehavior`, `InitialAccess:IAMUser/AnomalousBehavior`, `Persistence:IAMUser/AnomalousBehavior`, `PrivilegeEscalation:IAMUser/AnomalousBehavior` 같은 추가 GuardDuty 조사 결과 유형에 대한 프로필을 제공합니다.	2021년 3월 29일
AWS GovCloud (US) 리전에 대한 차이점 추가	이제 AWS GovCloud (US) 리전에서 Detective를 사용할 수 있습니다. In AWS GovCloud(미국 동부) 및 AWS GovCloud(미국 서부)에서는 Detective가 멤버 계정에 초대 이메일을 보내지 않습니다. 또한 Detective는 AWS에서 종료된 멤버 계정을 자동으로 제거하지 않습니다.	2021년 3월 24일

멤버 계정 상태를 기준으로 멤버 계정 목록을 필터링하는 탭 추가	이제 멤버 계정 목록에 멤버 계정 상태를 기준으로 목록을 필터링하는 데 사용할 수 있는 탭이 표시됩니다. 모든 멤버 계정, 상태가 수락됨(활성화됨)인 계정 또는 상태가 수락됨(활성화됨)이 아닌 멤버 계정을 볼 수 있습니다.	2021년 3월 16일
추가 Amazon GuardDuty 조사 결과 유형에 대한 지원 추가	이제 Detective는 `Backdoor:EC2/C&CActivity.B` , `Impact:EC2/PortSweep` , `Impact:EC2/WinRMBruteForce` , `PrivilegeEscalation:IAMUser/AdministrativePermissions` 같은 추가 GuardDuty 조사 결과 유형에 대한 프로필을 제공합니다.	2021년 3월 4일
초대 이메일을 억제하는 Python 스크립트에 옵션 추가	이제 Detective `enableDetective.py` 스크립트에서 `--disable_email` 옵션을 제공합니다. 해당 옵션을 포함하면 Detective는 멤버 계정에 초대 이메일을 보내지 않습니다.	2021년 2월 26일
“마스터 계정”이 “관리자 계정”으로 변경	‘마스터 계정’이라는 용어가 ‘관리자 계정’으로 변경되었습니다. Detective 콘솔 및 API에서도 이 용어가 변경되었습니다.	2021년 2월 25일
“마스터 계정”이 “관리자 계정”으로 변경	‘마스터 계정’이라는 용어가 ‘관리자 계정’으로 변경되었습니다. Detective 콘솔 및 API에서도 이 용어가 변경되었습니다.	2021년 2월 25일

조사 결과 IP 주소로 들어오고 나가는 VPC 흐름량 프로필 패널에 대한 활동 세부 정보 추가	이제 조사 결과 IP 주소로 들어오고 나가는 VPC 흐름량 프로필 패널에 활동 세부 정보를 표시할 수 있습니다. 활동 세부 정보는 조사 결과가 단일 IP 주소와 연결된 경우에만 사용할 수 있습니다. 활동 세부 정보에는 포트, 프로토콜 및 방향의 각 조합에 대한 볼륨이 표시됩니다.	2021년 2월 25일
멤버 계정으로 초대 이메일을 보내지 않도록 API 옵션 추가	Detective API를 사용하여 멤버 계정을 추가할 때 관리자 계정은 멤버 계정에 초대 이메일을 보내지 않도록 선택할 수 있습니다.	2021년 2월 25일
IP 주소 프로필의 전체 API 직접 호출량 프로필 패널에 대한 새 활동 세부 정보	이제 전체 API 직접 호출량 프로필 패널에서 IP 주소에 대한 활동 세부 정보를 표시할 수 있습니다. 활동 세부 정보에는 IP 주소에서 호출을 실행한 각 리소스의 성공 및 실패 호출 수가 표시됩니다.	2021년 2월 23일
IP 주소 프로필의 전체 VPC 흐름량 프로필 패널 새로 추가	이제 IP 주소 프로필에 전체 VPC 흐름량 프로필 패널이 포함됩니다. 프로필 패널에는 IP 주소로 들어오고 나가는 VPC 흐름 트래픽의 볼륨이 표시됩니다. 활동 세부 정보를 표시하여 IP 주소가 통신한 각 EC2 인스턴스의 볼륨을 표시할 수 있습니다.	2021년 1월 21일

Detective 요약 페이지 추가	Detective 요약 페이지에는 지리적 위치, API 직접 호출 수, Amazon EC2 트래픽 볼륨을 기반으로 분석가를 관심 엔터티로 안내하는 시각화가 포함되어 있습니다.	2021년 1월 21일
Amazon GuardDuty에서 Detective로 피벗할 수 있는 옵션 업데이트	ㅈGuardDuty에서 Detective에서 조사 옵션이 작업 메뉴에서 조사 결과 세부 정보 패널로 이동되었습니다. 관련 엔터티 목록을 표시합니다. 조사 결과 유형이 지원되는 경우 목록에 조사 결과도 포함됩니다. 그런 다음 엔터티 프로필 또는 조사 결과 프로필로 이동하도록 선택할 수 있습니다.	2021년 1월 15일
활동 세부 정보 창을 기본 범위 시간으로 설정하는 옵션 추가	전체 API 직접 호출량 및 전체 VPC 흐름량의 활동 세부 정보에서 활동 세부 정보의 기간을 프로필의 기본 범위 시간으로 설정할 수 있습니다.	2021년 1월 15일
엔터티에 대한 대용량 시간 간격 처리 추가	엔터티에 대용량 시간 간격이 하나 이상 있는 경우 알려주는 새 알림이 추가되었습니다. 새로운 대용량 엔터티 페이지에는 현재 범위 시간의 모든 대용량 간격이 표시됩니다.	2020년 12월 18일
멤버 계정 할당량이 1,200개로 증가	이제 마스터 계정은 최대 1,200개의 멤버 계정을 동작 그래프에 초대할 수 있습니다. 이전에는 할당량이 1,000이었습니다.	2020년 12월 11일

동작 그래프 데이터 볼륨 할당량 값 추가	동작 그래프 데이터 볼륨 할당량에 대한 정보를 업데이트하여 특정 할당량 값을 추가했습니다.	2020년 12월 11일
전체 API 직접 호출량 프로필 패널에 활동 세부 정보를 위한 시간 범위 선택 항목 추가	이제 전체 API 흐름량 패널에서 선택한 시간 범위에 대한 활동 세부 정보를 표시할 수 있습니다. 처음에는 패널에 범위 시간에 대한 활동 세부 정보를 표시하는 옵션이 표시됩니다.	2020년 9월 29일
전체 VPC 흐름량 프로필 패널에 활동 세부 정보를 위한 시간 간격 선택 항목 추가	전체 VPC 흐름량 패널에서 차트의 단일 시간 간격에 대한 활동 세부 정보를 표시할 수 있습니다. 시간 간격에 대한 세부 정보를 표시하려면 시간 간격을 선택합니다.	2020년 9월 25일
새 역할 세션 및 페더레이션 사용자 엔터티	이제 Detective를 사용하여 페더레이션 인증을 탐색하고 조사할 수 있습니다. 어떤 리소스가 각 역할을 맡았는지, 언제 이러한 인증이 발생했는지 확인할 수 있습니다.	2020년 9월 17일
범위 시간 관리 업데이트	범위 시간을 잠그거나 잠금 해제하는 옵션이 제거되었습니다. 항상 잠겨 있습니다. 조사 결과 프로필에서 범위 시간이 조사 결과 기간과 다른 경우 경고가 표시됩니다.	2020년 9월 4일

프로필을 스크롤해도 프로필 헤더 계속 표시	프로필의 경우 탭의 프로필 패널을 스크롤해도 유형, 식별자 및 범위 시간이 계속 표시됩니다. 탭이 보이지 않는 경우 브레드크럼의 탭 드롭다운 목록을 사용하여 다른 탭으로 이동할 수 있습니다.	2020년 9월 4일
검색에 항상 검색 결과가 표시됨	이제 검색을 수행하면 검색 페이지에 결과가 표시됩니다. 결과에서 조사 결과 또는 엔터티 프로필로 피벗할 수 있습니다.	2020년 8월 27일
검색의 허용 기준에 추가됨	허용되는 검색 기준이 확대되었습니다. 이름으로 AWS 사용자 및 AWS 역할을 검색할 수 있습니다. ARN을 사용하여 조사 결과, AWS 역할, AWS 사용자 및 EC2 인스턴스를 검색할 수 있습니다.	2020년 8월 27일
프로필 패널의 다른 콘솔로 연결	EC2 인스턴스 세부 정보 프로필 패널에서 EC2 인스턴스 식별자는 Amazon EC2 콘솔에 연결되어 있습니다. 사용자 세부 정보 및 역할 세부 정보 프로필 패널에는 사용자 이름과 역할 이름이 IAM 콘솔에 연결되어 있습니다.	2020년 8월 14일
VPC 흐름 데이터에 대한 활동 세부 정보	이제 전체 VPC 흐름량 프로필 패널에 활동 세부 정보에 대한 액세스가 제공됩니다. 활동 세부 정보는 선택한 기간 동안의 IP 주소와 EC2 인스턴스 간의 트래픽 흐름을 보여줍니다.	2020년 7월 23일

이제 멤버 계정에서 사용량 및 예상 비용 확인	이제 멤버 계정은 자신의 사용 정보를 볼 수 있습니다. 멤버 계정의 경우 사용량 페이지에는 멤버 계정이 기여한 각 동작 그래프에 수집된 데이터의 양이 표시됩니다. 멤버 계정은 30일 예상 비용도 확인할 수 있습니다.	2020년 5월 26일
이제 무료 평가판이 동작 그래프가 아닌 계정별로 제공	이제 각 계정 Amazon Detective는 각 리전 내에서 별도의 무료 평가판을 받게 됩니다. 무료 평가판은 계정이 Detective를 활성화하거나 계정이 멤버 계정으로 처음 활성화될 때 시작됩니다.	2020년 5월 26일
GitHub의 새로운 오픈 소스 Python 스크립트	GitHub의 새로운 amazon-detective-multiaccount-scripts 리포지토리에서 리전 간 동작 그래프를 관리하는 데 사용할 수 있는 오픈 소스 Python 스크립트 제공 Detective를 활성화하고, 멤버 계정을 추가하고, 멤버 계정을 제거하고, Detective를 비활성화할 수 있습니다.	2020년 1월 21일
Amazon Detective 소개	Detective는 기계 학습과 특수 목적의 시각화를 사용하여 Amazon Web Services(AWS) 워크로드 전반의 보안 문제를 분석하고 조사할 수 있도록 지원합니다.	2019년 12월 2일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.