aws

사용자 가이드

Amazon Macie

Amazon Macie: 사용자 가이드

Table of Contents

Amazon Macie란 무엇인가요?

Amazon Macie는 기계 학습과 패턴 일치를 사용하여 민감한 데이터를 검색하고, 데이터 보안 위험에 대한 가시성을 제공하며, 이러한 위험에 대한 자동 보호를 지원하는 데이터 보안 서비스입니다.

조직의 Amazon Simple Storage Service (Amazon S3) 데이터 자산의 보안 상태를 관리할 수 있도록 Macie는 S3 범용 버킷의 인벤토리를 제공하고 보안 및 액세스 제어를 위해 버킷을 자동으로 평가 및 모니터링합니다. 버킷에 퍼블릭 액세스가 가능해지는 등 Macie가 데이터의 보안이나 프라이버시와 관련된 잠재적 문제를 탐지하면 Macie가 결과를 조사 생성하며, 필요에 따라 사용자가 검토하고 수정할 수 있습니다.

또한 Macie는 민감한 데이터의 검색 및 보고를 자동화하기 때문에 조직이 Amazon S3에 저장하는 데이터를 더 잘 이해할 수 있도록 도와줍니다. 민감한 데이터를 탐지하려면 Macie에서 제공하는 기본 제공 기준 및 기법, 사용자가 정의한 사용자 지정 기준 또는 이 둘의 조합을 사용할 수 있습니다. Macie가 S3 객체에서 민감한 데이터를 감지하면 Macie는 검색 결과를 생성하여 찾은 민감한 데이터를 사용자에게 알립니다.

조사 결과 외에도 Macie는 Amazon S3 데이터의 보안 상태와 민감한 데이터가 데이터 자산의 어디에 위치할 수 있는지에 대한 통찰력을 제공하는 통계 및 정보를 제공합니다. 통계 및 정보는 특정 S3 버킷 및 객체를 심층적으로 조사하기 위한 결정을 내리는 데 지침이 될 수 있습니다. Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 결과, 통계 및 기타 정보를 검토하고 분석할 수 있습니다. 또한 Macie와 EventBridge Amazon의 통합을 활용하여 다른 서비스, 애플리케이션 및 시스템을 사용하여 결과를 모니터링, 처리 및 수정할 수 있습니다. AWS Security Hub

주제

Amazon Macie의 기능

Amazon Macie가 Amazon S3의 민감한 데이터를 검색, 모니터링 및 보호하는 데 도움을 줄 수 있는 몇 가지 주요 방법은 다음과 같습니다.

민감한 데이터 검색 자동화

Macie를 사용하면 민감한 데이터 자동 검색을 수행하도록 Macie를 구성하는 방법과 민감한 데이터 검색 작업을 생성 및 실행하는 방법으로 민감한 데이터의 검색 및 보고를 자동화할 수 있습니다. Macie가 S3 객체에서 민감한 데이터를 탐지하면 Macie가 민감한 데이터 조사 결과물을 생성합니다. 조사 결과는 Macie가 탐지한 민감한 데이터에 대한 자세한 보고서를 제공합니다.

민감한 데이터 자동 검색을 통해 Amazon S3 데이터 자산에서 민감한 데이터가 어디에 있는지 폭넓게 파악할 수 있게 해줍니다. 이 옵션을 사용하여 Macie는 계속해서 S3 버킷 인벤토리를 평가하고 샘플링 기법을 사용하여 버킷의 대표적인 S3 객체를 식별하고 선택합니다. 그런 다음 Macie는 선택한 객체를 검색 및 분석하여 민감한 데이터가 있는지 검사합니다.

민감한 데이터 검색 작업은 심층적이고 표적화된 분석을 제공합니다. 이 옵션을 사용하면 분석할 S3 버킷, 샘플링 깊이, S3 객체의 속성에서 파생되는 사용자 지정 기준 등 분석의 범위와 심도를 정의합니다. 온디맨드 분석 및 평가를 위해 한 번만 실행하거나 주기적 분석, 평가 및 모니터링을 위해 반복적으로 실행하도록 작업을 구성할 수도 있습니다.

두 옵션 모두 조직이 Amazon S3에 저장하는 데이터와 해당 데이터에 대한 보안 또는 규정 준수 위험을 포괄적으로 파악하고 유지하는 데 도움이 됩니다.

다양한 민감한 데이터 유형 살펴보기

Macie를 사용하여 민감한 데이터를 검색하려면 기계 학습과 패턴 일치와 같은 기본 기준 및 기법을 사용하여 S3 버킷에서 객체를 분석할 수 있습니다. 총칭하여 관리형 데이터 식별자라고 하는 이러한 기준 및 기술은 여러 유형의 개인 식별 정보(PII), 금융 정보, 자격 증명 데이터를 포함하여 점점 증가하는 민감한 데이터 유형 목록을 많은 국가 및 리전에서 탐지할 수 있습니다.

사용자 지정 데이터 식별자를 사용할 수도 있습니다. 사용자 지정 데이터 식별자는 민감한 데이터를 탐지하기 위해 정의하고 선택적으로 문자 시퀀스와 결과를 세분화하는 근접성 규칙을 정의하고 정규 표현식(regex)을 정의하고 선택적으로 문자 시퀀스와 결과를 세분화하는 근접성 규칙을 정의하는 기준 세트입니다. 이 유형의 식별자를 사용하면 특정 시나리오, 지적 재산 또는 독점 데이터를 반영하는 민감한 데이터를 탐지할 수 있습니다. Macie에서 제공하는 관리형 데이터 식별자를 보완할 수 있습니다.

분석을 세밀하게 조정하기 위해 허용 목록을 사용할 수도 있습니다. 허용 목록은 Macie가 S3 객체에서 무시할 특정 텍스트 및 텍스트 패턴을 정의합니다. 이는 일반적으로 특정 시나리오나 환경에 대한 민감한 데이터 예외입니다. 예를 들어 조직의 공공 담당자 이름, 조직의 공용 전화번호, 조직에서 테스트에 사용하는 샘플 데이터 등이 이에 해당합니다.

보안 및 액세스 제어를 위한 데이터 평가 및 모니터링

Macie를 활성화하면 Macie는 S3 범용 버킷의 전체 인벤토리를 자동으로 생성하고 유지 관리하기 시작합니다. Macie는 또한 보안 및 액세스 제어를 위한 버킷의 평가 및 모니터링도 시작합니다. Macie가 버킷의 보안 또는 프라이버시와 관련된 잠재적 문제를 탐지하면 Macie가 정책 조사 결과를 생성합니다.

대시보드는 구체적인 조사 결과 외에도 Amazon S3 데이터에 대한 집계된 통계의 스냅샷을 제공합니다. 여기에는 공개적으로 액세스할 수 있거나 다른 사람과 공유된 버킷 수와 같은 주요 지표에 대한 통계가 포함됩니다. AWS 계정각 통계를 자세히 분석하여 지원 데이터를 검토할 수 있습니다.

또한 Macie는 인벤토리의 개별 S3 버킷에 대한 자세한 정보와 통계를 제공합니다. 데이터에는 버킷의 공개 액세스 및 암호화 설정에 대한 분석, Macie가 분석하여 버킷의 민감한 데이터를 탐지할 수 있는 객체의 크기 및 수 등이 포함됩니다. 인벤토리를 찾아보거나 특정 필드를 기준으로 인벤토리를 정렬 및 필터링할 수 있습니다.

조사 결과 검토 및 분석

Macie에서 탐지 결과는 Macie가 S3 객체에서 감지한 민감한 데이터 또는 S3 범용 버킷의 보안 또는 개인 정보 보호와 관련된 잠재적 문제에 대한 자세한 보고서입니다. 각 검색 결과는 심각도 등급, 영향을 받는 리소스에 대한 정보, 추가 세부 정보 (예: Macie가 데이터 또는 문제를 감지한 시기와 방법) 를 제공합니다.

조사 결과를 검토, 분석 및 관리하려면 Amazon Macie 콘솔의 조사 결과 페이지를 사용할 수 있습니다. 이 페이지는 조사 결과를 나열하고 개별 조사 결과에 대한 세부 정보를 제공합니다. 또한 조사 결과를 그룹화, 필터링, 정렬 및 제외하기 위한 여러 옵션을 제공합니다. Amazon Macie API를 사용하여 조사 결과를 쿼리, 검색 및 솜길 수도 있습니다. API를 사용하는 경우 심층 분석, 장기 보관 또는 보고를 위해 데이터를 다른 애플리케이션, 서비스 또는 시스템으로 전달할 수 있습니다.

다른 서비스 및 시스템을 사용하여 조사 결과를 모니터링하고 처리

다른 서비스 및 시스템과의 통합을 지원하기 위해 Macie는 결과를 검색 EventBridge 이벤트로 Amazon에 게시합니다. EventBridge 는 결과 데이터를 AWS Lambda 함수 및 Amazon Simple Notification Service (Amazon SNS) 주제와 같은 대상으로 라우팅할 수 있는 서버리스 이벤트 버스 서비스입니다. 를 사용하면 기존 보안 및 규정 준수 워크플로의 일부로 거의 실시간으로 결과를 모니터링하고 처리할 수 있습니다. EventBridge

Macie가 AWS Security Hub에 조사 결과를 게시하도록 구성할 수도 있습니다. Security Hub는 AWS 환경 전반의 보안 상태를 포괄적으로 파악하고 보안 업계 표준 및 모범 사례와 비교하여 환경을 점검하는 데 도움이 되는 서비스입니다. Security Hub를 사용하면 AWS의 조직 보안 상태에 대한 광범위한 분석의 일부로 결과를 더 쉽게 모니터링하고 처리할 수 있습니다. 또한 여러 AWS 리전

조사 결과를 집계한 다음 단일 지역의 집계된 조사 결과 데이터를 모니터링하고 처리할 수 있습니다.

여러 Macie 계정을 중앙에서 관리

AWS 환경에 계정이 여러 개 있는 경우 해당 환경의 Macie 계정을 중앙에서 관리할 수 있습니다. Macie를 Macie와 AWS Organizations 통합하거나 Macie에서 회원 초대를 보내고 수락하는 두 가지 방법으로 이 작업을 수행할 수 있습니다.

다중 계정 구성에서는 지정된 Macie 관리자가 특정 작업을 수행하고 동일한 조직의 멤버인 계정에 대한 특정 Macie 설정, 데이터 및 리소스에 액세스할 수 있습니다. 작업에는 멤버 계정이 소유한 S3 버킷에 대한 정보 검토, 해당 버킷에 대한 정책 조사 결과 검토, 버킷의 민감한 데이터 검사 등이 포함됩니다. 계정을 통해 연결된 경우 Macie 관리자는 AWS Organizations조직의 구성원 계정에 대해 Macie를 활성화할 수도 있습니다.

프로그래밍 방식으로 리소스를 개발하고 관리

Amazon Macie 콘솔 외에도 Amazon Macie API를 사용하여 Macie와 상호 작용할 수 있습니다. Amazon Macie API를 사용하면 Macie 계정 설정, 데이터 및 리소스에 포괄적이고 프로그래밍 방식으로 액세스할 수 있습니다.

프로그래밍 방식으로 Macie와 상호 작용하려면 HTTPS 요청을 Macie에 직접 보내거나 최신 버전의 AWS 명령줄 도구 또는 SDK를 사용할 수 있습니다. AWS AWS 는 Java, Go, Python, C++, .NET 과 같은 PowerShell 다양한 언어 및 플랫폼에 대한 라이브러리 및 샘플 코드로 구성된 도구 및 SDK를 제공합니다.

Amazon Macie 액세스

Amazon Macie는 대부분 사용할 수 있습니다. AWS 리전현재 Macie를 사용할 수 있는 모든 리전 목록은 AWS 일반 참조의 Amazon Macie 및 엔드포인트 및 할당량을 참조하세요. 사용자 AWS 계정관리에 AWS 리전 대한 자세한 내용은 AWS Account Management 참조 안내서에서 사용할 수 있는 AWS 리전 계정 지정을 참조하십시오.

각 리전에서 다음 방법 중 하나로 Macie와 작업할 수 있습니다.

AWS Management Console

리소스를 AWS Management Console 만들고 관리하는 AWS 데 사용할 수 있는 브라우저 기반 인터페이스입니다. 이 콘솔의 일부인 Amazon Macie 콘솔은 Macie 계정, 데이터 및 리소스에 대한 액세스를 제공합니다. Macie 콘솔을 사용하여 S3 버킷에 대한 통계 및 기타 정보를 검토하고, 민감한

데이터 검색 작업을 생성 및 실행하고, 조사 결과를 검토 및 분석하는 등 모든 Macie 작업을 수행할 수 있습니다.

AWS 명령줄 도구

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

AWS 는 두 가지 명령줄 도구 세트, 즉 AWS Command Line Interface (AWS CLI) 와 를 AWS Tools for PowerShell제공합니다. 설치 및 사용에 대한 자세한 내용은 사용 AWS Command Line Interface 설명서를 참조하십시오. AWS CLI도구 설치 및 사용에 대한 자세한 내용은 사용 AWS Tools for PowerShell 설명서를 참조하십시오. PowerShell

AWS SDK

AWS Java, Go, Python, C++, .NET과 같은 다양한 프로그래밍 언어 및 플랫폼에 대한 라이브러리 및 샘플 코드로 구성된 SDK를 제공합니다. SDK를 사용하면 Macie 및 기타 항목에 프로그래밍 방식으로 편리하게 액세스할 수 있습니다. AWS 서비스 SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 포함합니다. AWS SDK 설치 및 사용에 대한 자세한 내용은 빌드 기반 도구를 참조하십시오. AWS

Amazon Macie REST API

Amazon Macie REST API를 사용하면 Macie 계정, 데이터 및 리소스에 대한 포괄적이고 프로그래밍 방식으로 액세스할 수 있습니다. 이 API를 사용하면 HTTPS 요청을 Macie에 직접 보낼 수 있습니다. 하지만 AWS 명령줄 도구 및 SDK와 달리 이 API를 사용하려면 애플리케이션에서 요청에 서명하기 위한 해시 생성과 같은 낮은 수준의 세부 정보를 처리해야 합니다. 이러한 API에 대한 자세한 내용은 Amazon Macie API 참조를 참조하세요.

Amazon Macie 요금

다른 AWS 제품과 마찬가지로 Amazon Macie를 사용하기 위한 계약 또는 최소 약정은 없습니다.

Macie 요금은 보안 및 액세스 제어를 위한 S3 버킷 평가 및 모니터링, 민감한 데이터 자동 검색을 위한 S3 객체 모니터링, 객체에서 민감한 데이터를 발견하고 보고하기 위한 S3 객체 분석 등 여러 차원을 기반으로 합니다. 자세한 내용은 Amazon Macie 요금을 참조하세요.

Macie는 Macie 사용 비용을 이해하고 예측하는 데 도움이 되도록 계정의 예상 사용 비용을 제공합니다. Amazon Macie 콘솔에서 이러한 추정치를 검토하고 Amazon Macie API를 사용하여 이에 액세스할 수 있습니다. 서비스 사용 방식에 따라 Amazon AWS 서비스 S3에서 버킷 데이터를 검색하고 분석을

위해 고객이 관리하는 객체 암호 해독을 사용하는 등 특정 Macie 기능과 함께 다른 기능을 함께 사용하면 추가 비용이 발생할 AWS KMS keys 수 있습니다.

Macie를 처음 활성화하면 Macie의 30일 무료 AWS 계정 평가판에 자동으로 등록됩니다. 여기에는 AWS Organizations에서 조직의 일부로 활성화된 개별 계정도 포함됩니다. 무료 평가판 기간 동안에는 보안 및 액세스 제어를 위해 S3 버킷을 평가하고 모니터링하는 AWS 리전 데 Macie를 무료로 사용할 수 있습니다. 계정 설정에 따라 무료 평가판에는 Amazon S3 데이터에 대한 민감한 데이터 자동 검색 수행도 포함될 수 있습니다. S3 객체에서 민감한 데이터를 검색 및 보고할 민감한 데이터 검색 작업을 실행하는 것은 무료 평가판에 포함되지 않습니다.

Macie는 무료 평가판 종료 후 Macie를 사용하는 데 드는 비용을 이해하고 예측할 수 있도록 평가판 사용 기간 중 Macie를 사용한 금액을 기준으로 예상 사용 비용을 제공합니다. 사용량 데이터에는 무료 평가판이 종료될 때까지 남은 시간도 표시됩니다. Amazon Macie 콘솔에서 이 데이터를 검토하고 Amazon Macie API를 사용하여 데이터에 액세스할 수 있습니다.

관련 서비스

에서 AWS데이터, 워크로드 및 애플리케이션을 더욱 안전하게 보호하려면 Amazon Macie와 함께 다음을 AWS 서비스 사용하는 것이 좋습니다.

AWS Security Hub

AWS Security Hub AWS 리소스의 보안 상태를 포괄적으로 파악하고 보안 업계 표준 및 모범 사례와 비교하여 AWS 환경을 점검하는 데 도움이 됩니다. 이는 여러 제품 (Macie 포함) 및 지원되는 AWS 파트너 네트워크 AWS 서비스 (APN) 제품의 보안 결과를 사용하고, 집계하고, 구성하고, 우선순위를 지정함으로써 부분적으로는 이를 수행합니다. Security Hub를 사용하면 AWS 환경 전반에서 보안 동향을 분석하고 우선 순위가 가장 높은 보안 문제를 식별할 수 있습니다.

에 대한 자세한 내용은 AWS Security Hub 사용 설명서를 참조하세요. Macie와 Security Hub를 함께 사용하는 방법에 대한 자세한 내용은 Amazon Macie와 통합 AWS Security Hub 단원을 참조하세요.

아마존 GuardDuty

GuardDuty Amazon은 Amazon S3의 AWS CloudTrail 데이터 이벤트 로그 및 CloudTrail 관리 이벤트 로그와 같은 특정 유형의 AWS 로그를 분석하고 처리하는 보안 모니터링 서비스입니다. 악성 IP 주소 및 도메인 목록과 같은 위협 인텔리전스 피드와 기계 학습을 사용하여 AWS 환경 내에서 예상치 못한 잠재적으로 무단 악의적인 활동을 식별합니다.

자세한 GuardDuty 내용은 Amazon GuardDuty 사용 설명서를 참조하십시오.

추가 AWS 보안 서비스에 대해 알아보려면 보안, ID 및 규정 준수를 참조하십시오 AWS.

Amazon Macie 시작하기

이 자습서에서는 Amazon Macie에 대한 소개를 제공합니다. AWS 계정에 대해 Macie를 활성화하는 방법을 알아봅니다. 또한 Amazon Simple Storage Service (Amazon S3) 보안 상태를 평가하고 S3 버킷에서 민감한 데이터를 검색하고 보고하기 위한 주요 설정 및 리소스를 구성하는 방법을 배우게 됩니다.

Tasks

시작하기 전 준비 사항

Amazon Web Services(AWS)에 가입하면 Amazon Macie를 포함한 AWS 서비스의 모든 서비스에 계정이 자동으로 등록됩니다. 그러나 Macie를 활성화하고 사용하려면 먼저 Amazon Macie 콘솔 및 API 작업에 액세스할 수 있는 권한을 설정해야 합니다. 사용자 또는 AWS 관리자는 AWS Identity and Access Management (IAM) 을 사용하여 이름이 지정된 AWS `AmazonMacieFullAccess` 관리형 정책을 IAM ID에 연결하여 이 작업을 수행할 수 있습니다. 자세한 내용은 Amazon Macie에 대한 AWS 관리형 정책(을)를 참조하세요.

1단계: Amazon Macie 활성화

필요한 권한을 설정한 후 AWS 계정에 대한 Amazon Macie를 활성화할 수 있습니다. 다음 단계에 따라 계정에서 Macie를 활성화하세요.

Macie를 활성화하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 Macie를 활성화하고 사용할 지역을 선택합니다.
3. Amazon Macie 페이지에서 시작하기를 선택합니다.

4. (선택 사항) Macie를 활성화하면 Macie는 다른 사람에게 전화를 걸고 사용자 대신 리소스를 모니터링하는 데 필요한 권한을 Macie에게 부여하는 서비스 연결 역할을 자동으로 생성합니다. AWS 서비스 AWS 이 역할의 권한 정책을 검토하려면 콘솔에서 역할 권한 보기를 선택합니다. 이 역할에 대한 자세한 내용은 Amazon Macie의 서비스 연결 역할(을)를 참조하세요.
5. Macie 활성화를 선택합니다.

몇 분 안에 Macie는 현재 지역에 있는 S3 범용 버킷의 전체 인벤토리를 자동으로 생성하고 유지 관리하기 시작합니다. Macie는 또한 보안 및 액세스 제어를 위한 버킷의 평가 및 모니터링도 시작합니다. 자세한 내용은 Macie가 Amazon S3 데이터 보안을 모니터링하는 방법(을)를 참조하세요.

계정 설정에 따라 Macie는 S3 버킷에 대한 민감한 데이터 자동 검색을 시작하기도 합니다. Macie는 버킷의 대표 객체를 지속적으로 식별, 선택 및 분석하여 객체의 민감한 데이터를 검사합니다. 분석이 진행됨에 따라 Macie는 사용자가 검토할 수 있는 통계 및 기타 결과를 제공합니다. 일반적으로 계정에서 Macie를 활성화한 후 48시간 이내에 검토할 수 있습니다. 계정의 민감한 데이터 자동 검색 설정을 구성하여 분석을 맞춤화할 수 있습니다. 자세한 내용은 민감한 데이터 자동 검색의 작동 방식(을)를 참조하세요.

Amazon S3 데이터에 대한 집계된 통계를 검토하려면 콘솔의 탐색 창에서 [Summary] 를 선택합니다. 인벤토리의 개별 S3 버킷에 대한 세부 정보를 검토하려면 탐색 창에서 S3 버킷을 선택합니다. 그런 다음, 버킷의 세부 정보를 표시하려면 버킷을 선택합니다. 세부 정보 패널에는 버킷 데이터의 보안, 개인 정보 보호 및 민감도에 대한 통찰력을 제공하는 통계 및 기타 정보가 표시됩니다. 이러한 세부 정보에 대해 자세히 알아보려면, S3 버킷 인벤토리 검토을 참조하십시오.

2단계: 민감한 데이터 검색 결과를 위한 리포지토리 구성

Amazon Macie를 사용하면 두 가지 방법으로 S3 버킷의 민감한 데이터를 검색할 수 있습니다. 하나는 민감한 데이터 자동 검색을 수행하도록 Macie를 구성하는 것이고 다른 하나는 민감한 데이터 검색 작업을 실행하는 것입니다. 민감한 데이터 검색 작업은 S3 버킷의 객체를 분석하여 객체에 민감한 데이터가 포함되어 있는지 확인하기 위해 생성하는 작업입니다.

Macie는 민감한 데이터 검색 작업을 실행하거나 자동화된 민감한 데이터 검색을 수행할 때 분석하는 각 S3 객체에 대한 레코드를 생성합니다. 민감한 데이터 검색 결과라고 하는 이러한 레코드는 개별 객체 분석에 대한 세부 정보를 기록합니다. 또한 Macie는 오류나 문제로 인해 분석할 수 없는 객체에 대한 민감한 데이터 검색 결과를 생성합니다. 민감한 데이터 검색 결과에는 데이터 프라이버시 및 보호 감사 또는 조사에 도움이 될 수 있는 분석 기록이 표시됩니다.

Macie는 민감한 데이터 검색 결과를 90일 동안만 저장합니다. 결과에 액세스하고 해당 결과를 장기간 저장 및 보존하려면 결과를 S3 버킷에 저장하도록 Macie를 구성합니다. Macie를 활성화한 후 30일 이

내에 이 작업을 수행해야 합니다. 이렇게 하면 버킷은 모든 민감한 데이터 검색 결과를 위한 확정적이고 장기적인 리포지토리 역할을 할 수 있습니다.

이 리포지토리를 구성하는 방법을 알아보려면 민감한 데이터 검색 결과 저장 및 유지 섹션을 참조하세요.

3단계: 샘플 조사 결과 살펴보기

Amazon Macie에는 정책 조사 결과와 민감한 데이터 조사 결과라는 두 가지 범주의 결과가 있습니다. Macie는 S3 범용 버킷의 정책 또는 설정이 버킷 및 버킷 객체의 보안 또는 개인 정보 보호를 약화시키는 방식으로 변경될 때 이를 확인하는 정책을 생성합니다. Macie는 S3 객체에서 민감한 데이터를 탐지하면 Macie는 민감한 데이터 조사 결과를 생성합니다. 각 범주에는 여러 유형의 조사 결과가 있습니다.

Macie가 제공하는 다양한 범주와 유형의 조사 결과를 탐색하고 자세히 알아보려면 선택적으로 샘플 조사 결과를 만들어 검토할 수 있습니다. 샘플 조사 결과는 예제 데이터와 자리 표시자 값을 사용하여 Macie가 각 조사 결과 유형에 포함할 수 있는 정보의 종류를 보여줍니다.

다음 단계에 따라 샘플 조사 결과를 만들고 검토하세요.

샘플 조사 결과를 생성 및 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 샘플 조사 결과아래에서, 조사 결과 생성을 선택합니다. Macie는 Macie가 지원하는 각 검색 유형에 대해 하나의 샘플 조사 결과를 생성합니다.
4. 탐색 창에서 결과를 선택합니다. 조사 결과 페이지에는 현재 AWS 리전에서 계정의 조사 결과가 표시됩니다. 여기에는 이전 단계에서 만든 샘플 조사 결과가 포함됩니다.
5. 조사 결과 페이지에서 유형이 [SAMPLE]로 시작하는 조사 결과의 위치를 찾습니다.
6. 특정 샘플 조사 결과의 세부 정보를 검토하려면 조사 결과를 선택하세요. 세부 정보 패널에 결과의 세부 정보가 표시됩니다.

조사 결과의 각 유형에 대한 자세한 내용은 조사 결과의 유형을(를) 참조하세요. 샘플 조사 결과 생성 및 검토에 대한 자세한 내용은 조사 결과 다루기을(를) 참조하세요.

4단계: 민감한 데이터를 검색하기 위한 작업 생성

S3 버킷의 민감한 데이터를 검색하고 보고하기 위해 민감한 데이터 검색 작업을 실행할 수 있습니다. 민감한 데이터 검색 작업은 S3 버킷의 객체를 분석하여 객체에 민감한 데이터가 포함되어 있는지 확인

하기 위해 생성하는 작업입니다. 민감한 데이터 자동 검색과 달리 분석의 범위와 깊이를 사용자가 정의합니다. 또한 작업 실행 빈도(일정에 따라 한 번 또는 주기적으로)를 지정할 수 있습니다.

다음 단계에 따라 작업을 생성한 후 바로 한 번 실행되고 기본 설정을 사용하는 작업을 생성하세요. 정기적으로 실행되거나 사용자 정의 설정을 사용하는 작업을 생성하는 방법에 대한 자세한 내용은 민감한 데이터 검색 작업 생성(을)를 참조하세요.

민감한 데이터 검색 작업을 생성하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다.
3. 작업 생성을 선택합니다.
4. S3 버킷 선택 단계에서 특정 버킷 선택을 선택합니다. 그런 다음, 테이블에서 작업이 분석할 각 S3 버킷의 확인란을 선택합니다.

   이 표는 현재 S3 범용 버킷의 전체 인벤토리를 제공합니다. AWS 리전특정 버킷을 더 쉽게 찾으려면 테이블 위의 필터 상자에 필터 기준을 입력합니다. 열 머리글을 선택하여 테이블을 정렬할 수도 있습니다.
5. 버킷 선택을 마치면 다음을 선택합니다.
6. S3 버킷 검토 단계에서 버킷 선택을 검토 및 확인한 후 다음을 선택합니다.
7. 범위 구체화 단계에서 일회성 작업을 선택하고 다음을 선택합니다.
8. 관리형 데이터 식별자 선택 단계에서 권장을 선택합니다. 필요에 따라 작업에 권장하는 관리형 데이터 식별자 테이블을 검토한 후 다음을 선택합니다.

   관리형 데이터 식별자는 특정 유형의 민감한 데이터 (예: 특정 국가 또는 지역의 신용 카드 번호, AWS 보안 액세스 키 또는 여권 번호) 를 탐지하도록 설계된 일련의 기본 제공 기준 및 기술입니다. 자세한 내용은 관리형 데이터 식별자 사용(을)를 참조하세요.
9. 사용자 지정 데이터 식별자 선택 단계에서 다음을 선택합니다.

   사용자 지정 데이터 식별자는 민감한 데이터를 탐지하기 위해 정의하고 선택적으로 문자 시퀀스와 결과를 세분화하는 근접성 규칙을 정의하고 정규 표현식(regex)을 정의하고 선택적으로 문자 시퀀스와 결과를 세분화하는 근접성 규칙을 정의하는 기준 세트입니다. 자세한 내용은 사용자 지정 데이터 식별자 빌드(을)를 참조하세요.
10. 허용 목록 선택 단계에서 다음을 선택합니다.

    Macie에서 허용 목록은 특정 텍스트 또는 텍스트 패턴을 지정하여 Macie가 S3 객체에서 민감한 데이터를 검사할 때 무시하도록 할 수 있습니다. 이는 일반적으로 특정 시나리오나 환경에 대한

민감한 데이터 예외사항입니다. 자세한 내용은 허용 목록을 사용하여 민감한 데이터 예외사항 정의(을)를 참조하세요.

11. 일반 설정 입력 단계에서 작업의 이름과 설명(선택 사항)을 입력합니다. 이후 다음을 선택합니다.
12. 검토 및 생성 단계의 경우, 작업의 구성 설정을 검토하고 해당 내용이 올바른지 확인합니다.

    또한 작업을 실행하는 예상 총 비용(미국 달러)을 검토할 수 있습니다. 예상치는 작업을 저장하기 전에 작업 설정을 조정할지 여부를 결정하는 데 도움이 될 수 있습니다. 자세한 내용은 민감한 데이터 검색 작업의 비용 예측(을)를 참조하세요.
13. 작업 설정 검토 및 확인을 마치면 제출을 선택합니다.

Macie는 즉시 작업 실행을 시작합니다. 작업을 모니터링하는 방법을 알아보려면 민감한 데이터 검색 작업의 상태 확인을 참조하세요.

5단계: 조사 결과 검토

Amazon Macie는 보안 및 액세스 제어를 위해 S3 범용 버킷을 자동으로 모니터링하고, 정책 결과를 생성하여 버킷의 보안 또는 개인 정보 보호와 관련된 잠재적 문제를 보고합니다. 민감한 데이터 검색 작업을 실행하거나 자동 민감 데이터 검색을 수행하도록 Macie를 구성한 경우 Macie는 민감한 데이터 결과를 생성하여 S3 객체에서 탐지한 민감한 데이터를 보고합니다. 조사 결과에 대한 자세한 내용은 조사 결과 분석을(를) 참조하세요.

다음 단계에 따라 조사 결과를 검토하세요.

조사 결과를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다. 조사 결과 페이지에는 현재 AWS 리전에서 계정의 조사 결과가 표시됩니다.
3. (선택 사항) 조사 결과를 특정 기준으로 필터링하려면 테이블 위의 필터 상자에 기준을 입력합니다.
4. 특정 조사 결과의 세부 정보를 검토하려면 조사 결과를 선택합니다. 세부 정보 패널에 결과의 세부 정보가 표시됩니다.

조사 결과를 그룹화하고 필터링하는 방법을 비롯한 자세한 내용은 결과 검토을(를) 참조하세요.

Amazon Macie 개념 및 용어

Amazon Macie에서는 일반적인 AWS 개념과 용어를 기반으로 이러한 추가 용어를 사용합니다.

account

AWS 리소스와 AWS 계정 해당 리소스에 액세스할 수 있는 ID를 포함하는 표준입니다.

Macie를 사용하려면 AWS 계정 자격 AWS 증명으로 로그인하고 사용할 Macie를 선택한 다음 해당 AWS 리전 지역에서 Macie를 활성화합니다 AWS 계정 . 자세한 정보는 Amazon Macie 시작하기을 참조하세요.

Macie에는 다음 세 가지 유형의 계정이 있습니다.

- 관리자 계정 - 이 유형의 계정은 조직의 Macie 계정을 관리합니다. 조직은 서로 연결되어 있고 특정 AWS 리전의 관련 계정 그룹으로 중앙에서 관리되는 Macie 계정 세트입니다.
- 멤버 계정 – 이 유형의 계정은 조직의 Macie 관리자 계정과 연결되고 관리됩니다.
- 독립형 계정 – 이 유형의 계정은 관리자도 아니고 멤버 계정도 아닙니다. 해당 내용은 조직의 일부가 아닙니다.

Macie를 AWS Organizations 와 통합하거나 Macie 멤버십 초대를 보내고 수락하는 두 가지 방법으로 조직에 Macie 계정을 추가할 수 있습니다. 자세한 내용은 여러 계정 관리 섹션을 참조하세요.

관리자 계정

Macie에서는 조직의 Macie 계정을 관리하는 계정입니다. 조직은 서로 연결되어 있고 특정 AWS 리전의 관련 계정 그룹으로 중앙에서 관리되는 Macie 계정 세트입니다.

Macie 관리자 계정의 사용자는 조직의 모든 계정에 대한 Amazon Simple Storage Service(S3)인벤토리 데이터, 정책 조사 결과, 특정 Macie 설정 및 리소스에 액세스할 수 있습니다. 또한 민감한 데이터 자동 검색을 수행하고 민감한 데이터 검색 작업을 실행하여 계정이 소유한 S3 버킷의 민감한 데이터를 탐지할 수 있습니다. 계정이 관리자 계정으로 지정된 방식에 따라 조직의 다른 계정에 대한 추가 작업을 수행할 수도 있습니다.

자세한 내용은 여러 계정 관리 섹션을 참조하세요.

허용 목록

Macie에서 허용 목록은 특정 텍스트 또는 텍스트 패턴을 지정하여 Macie가 S3 객체에서 민감한 데이터를 검사할 때 무시하도록 할 수 있습니다.

Macie에서는 두 가지 유형의 허용 목록을 만들 수 있습니다. 하나는 무시할 특정 단어 및 기타 유형의 문자 시퀀스를 나열하는 일반 텍스트 파일이고, 다른 하나는 무시할 텍스트 패턴을 정의하는 정규 표현식(regex)입니다. 객체에 허용 목록의 항목 또는 패턴과 일치하는 텍스트가 포함된 경우, Macie는 텍스트가 관리형 데이터 식별자 또는 사용자 지정 데이터 식별자의 기준과 일치하더라도 민감한 데이터 조사 결과, 통계 및 기타 유형의 결과의 텍스트를 보고하지 않습니다.

자세한 내용은 허용 목록을 사용하여 민감한 데이터 예외사항 정의 섹션을 참조하세요.

민감한 데이터 자동 검색

Macie가 S3 버킷에서 대표 객체를 식별 및 선택하고 선택한 객체에서 민감한 데이터를 검사하기 위해 지속적으로 수행하는 일련의 자동 분석 활동입니다.

분석이 진행됨에 따라 Macie는 발견한 민감한 데이터(민감한 데이터 조사 결과)와 수행하는 분석(민감한 데이터 검색 결과)의 기록을 생성합니다. 또한 Macie는 Amazon S3 데이터에 대해 제공하는 통계 및 기타 정보를 업데이트합니다.

자세한 정보는 민감한 데이터 자동 검색 수행을 참조하세요.

AWS 보안 탐지 형식 (ASFF)

에서 게시하거나 에서 생성한 결과 내용을 위한 표준화된 JSON 형식입니다. AWS Security Hub ASFF에는 보안 문제의 출처, 영향을 받은 리소스와 결과의 상태 등에 관한 세부 정보가 포함됩니다.

ASFF에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 AWS 보안 조사 결과 형식(ASFF)을 참조하세요. Macie의 조사 결과를 Security Hub에 게시하는 방법에 대한 자세한 내용은 Amazon Macie와 통합 AWS Security Hub을(를) 참조하세요.

분류 가능한 바이트 또는 크기

Macie가 제공하는 S3 버킷 통계에서 S3 버킷에 있는 모든 분류 가능한 객체의 총 스토리지 크기입니다.

버킷에 대한 버전 관리가 활성화된 경우, 이 값은 버킷에 있는 각 분류 가능한 객체의 최신 버전 스토리지 크기를 기반으로 합니다. 객체가 압축된 파일인 경우, 이 값은 파일 압축이 풀린 후의 파일 콘텐츠의 실제 크기를 반영하지 않습니다.

자세한 정보는 S3 버킷 인벤토리 검토 및 Amazon S3 보안 태세 액세스(을)를 참조하세요.

분류 가능한 객체

Macie가 분석하여 민감한 데이터를 탐지할 수 있는 S3 객체입니다.

S3 버킷 통계를 계산할 때 Macie는 객체의 스토리지 클래스와 파일 이름 확장자을 기반으로 객체를 분류할 수 있다고 판단합니다. 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식의 파일 이름 확장자가 있는 객체는 분류할 수 있습니다.

자세한 정보는 S3 버킷 인벤토리 검토 및 Amazon S3 보안 태세 액세스(을)를 참조하세요.

민감한 데이터 검색의 경우, Macie는 객체의 스토리지 클래스, 파일 이름 확장자 및 콘텐츠를 기반으로 객체를 분류할 수 있다고 판단합니다. 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자가 있고 Macie가 객체에서 데이터를 추출하고 분석할 수 있는지 확인한 경우에는 객체를 분류할 수 있습니다.

자세한 정보는 민감한 데이터 검색 및 비용 예측 및 모니터링(을)를 참조하세요.

사용자 지정 데이터 식별자

민감한 데이터를 감지하기 위해 정의하는 기준 세트입니다.

기준은 일치시킬 텍스트 패턴을 정의하고 선택적으로 문자 시퀀스와 결과를 세분화하는 근접성 규칙을 정의하는 정규 표현식(regex)으로 구성됩니다. 문자 시퀀스는 다음과 같을 수 있습니다.

- regex와 일치하는 텍스트와 근접해야 하는 단어 또는 문구인 키워드입니다.
- 결과에서 제외할 단어 또는 문구인 무시 단어입니다.

탐지 기준 외에도 사용자 지정 데이터 식별자가 생성하는 민감한 데이터 조사 결과에 대한 사용자 지정 심각도 설정을 정의할 수 있습니다.

자세한 내용은 사용자 지정 데이터 식별자 빌드 섹션을 참조하세요.

필터 규칙

Amazon Macie 콘솔에서 조사 결과를 분석하기 위해 생성하고 저장하는 속성 기반 필터 기준 세트입니다. 필터 규칙을 사용하면 특정 유형의 민감한 데이터를 보고하는 심각도가 높은 모든 조사 결과와 같이 특정 특성을 가진 조사 결과를 일관되게 분석할 수 있습니다.

자세한 내용은 조사 결과에 대한 필터 규칙 생성 및 관리 섹션을 참조하세요.

조사 결과

Macie가 S3 객체에서 발견한 민감한 데이터 또는 S3 범용 버킷의 보안 또는 개인 정보 보호와 관련된 잠재적 문제에 대한 자세한 보고서입니다. 각 조사 결과는 심각도 등급, 영향을 받는 리소스에 대한 정보, Macie가 데이터 또는 문제를 발견한 시점과 같은 세부 정보를 제공합니다.

Macie는 두 가지 범주의 조사 결과를 생성합니다. 하나는 Macie가 S3 객체에서 탐지한 민감한 데이터에 대한 민감한 데이터 조사 결과이고, 다른 하나는 Macie가 S3 버킷의 보안 및 액세스 제어 설정에서 탐지한 잠재적 문제에 대한 정책 조사 결과입니다. 각 범주 내에는 특정 유형의 조사 결과가 있습니다.

자세한 내용은 Amazon Macie의 조사 결과 유형 섹션을 참조하세요.

이벤트 찾기

민감한 데이터 검색 결과 또는 정책 조사 결과의 세부 정보가 포함된 Amazon EventBridge 이벤트입니다.

Macie는 민감한 데이터 결과 및 정책 결과를 EventBridge 이벤트로 Amazon에 자동으로 게시합니다. 이벤트는 이벤트 스키마를 준수하는 JSON 객체입니다. EventBridge AWS 이러한 이벤트를 사용하면 다른 응용 프로그램, 서비스 및 시스템을 사용하여 조사 결과를 모니터링 및 처리하고 이에 따라 조치를 취할 수 있습니다.

자세한 정보는 Amazon Macie, Amazon EventBridge와 통합 및 Amazon Macie 조사 결과를 위한 Amazon EventBridge 이벤트 스키마(을)를 참조하세요.

job

민감한 데이터 검색 작업을 참조하세요.

관리형 데이터 식별자

특정 유형의 민감한 데이터를 탐지하도록 설계된 기본 제공 기준 및 기법 세트입니다. 민감한 데이터의 예로는 특정 국가 또는 지역의 신용 카드 번호, AWS 비밀 액세스 키, 여권 번호 등이 있습니다. 데이터 식별자로 통칭되는 이러한 기준과 기술을 통해 많은 국가와 지역에서 점점 늘어나고 있는 민감한 데이터 유형을 탐지할 수 있습니다.

자세한 내용은 관리형 데이터 식별자 사용 섹션을 참조하세요.

멤버 계정

조직의 지정된 Macie 관리자 계정으로 관리되는 Macie 계정입니다. 조직이란 서로 연결되어 있고 특정 지역의 관련 계정 그룹으로 중앙에서 관리되는 일련의 Macie 계정을 말합니다. AWS 리전

계정은 두 가지 방법으로 회원 계정이 될 수 있습니다. 하나는 Macie를 계정의 조직과 AWS Organizations 통합하거나 Macie 멤버십 초대를 수락하는 것입니다.

멤버 계정이 있는 경우, Macie 관리자는 Amazon S3 인벤토리 데이터, 정책 조사 결과, 계정의 특정 Macie 설정 및 리소스에 액세스할 수 있습니다. 또한 관리자는 민감한 데이터 자동 검색을 수행하고 민감한 데이터 검색 작업을 실행하여 S3 버킷의 민감한 데이터를 탐지할 수 있습니다. 또한 계정이 멤버 계정이 된 경위에 따라 계정에 대한 추가 작업을 수행할 수도 있습니다.

자세한 내용은 여러 계정 관리 섹션을 참조하세요.

조직

서로 연결되어 있고 특정 지역의 관련 계정 그룹으로 중앙에서 관리되는 Macie 계정 집합입니다. AWS 리전

각 조직은 지정된 Macie 관리자 계정과 하나 이상의 관련 멤버 계정으로 구성됩니다. 관리자 계정은 멤버 계정의 특정 Macie 설정, 데이터 및 리소스에 액세스할 수 있습니다. 두 가지 방법으로 조직을 만들 수 있습니다. 하나는 Macie를 AWS Organizations 와 통합하거나 Macie에서 회원 초대를 보내고 수락하는 것입니다.

자세한 내용은 여러 계정 관리 섹션을 참조하세요.

정책 조사 결과

S3 범용 버킷의 보안 및 액세스 제어 설정과 관련된 잠재적 정책 위반 또는 문제에 대한 자세한 보고서입니다. 세부 정보에는 심각도 등급, 영향을 받는 리소스에 대한 정보, Macie가 문제를 발견한 시점 등이 포함됩니다.

Macie는 S3 범용 버킷의 정책 또는 설정이 버킷 및 버킷 객체의 보안 또는 개인 정보 보호를 약화시키는 방식으로 변경될 경우 정책 결과를 생성합니다. Macie는 Amazon S3 데이터에 대한 지속적인 모니터링 활동의 일환으로 이러한 조사 결과를 생성합니다. Macie는 여러 유형의 정책 조사 결과를 생성할 수 있습니다.

자세한 정보는 Amazon Macie의 조사 결과 유형 및 데이터 보안 및 개인정보 보호 모니터링(을)를 참조하세요.

샘플 조사 결과

예제 데이터와 자리 표시자 값을 사용하여 조사 결과에 포함될 수 있는 정보의 종류를 설명하는 조사 결과입니다.

자세한 내용은 조사 결과 다루기 섹션을 참조하세요.

민감한 데이터 조사 결과

Macie가 S3 객체에서 발견한 민감한 데이터에 대한 자세한 보고서입니다. 세부 정보에는 심각도 등급, 영향을 받는 리소스에 대한 정보, Macie가 발견한 민감한 데이터의 유형 및 발생 횟수, Macie가 민감한 데이터를 발견한 시점 등이 포함됩니다.

Macie는 민감한 데이터 검색 작업을 실행하거나 민감한 데이터 자동 검색을 수행할 때 분석하는 S3 객체에서 민감한 데이터를 탐지하는 경우 민감한 데이터 조사 결과를 생성합니다. Macie는 여러 유형의 민감한 데이터 조사 결과를 생성할 수 있습니다.

자세한 정보는 Amazon Macie의 조사 결과 유형 및 민감한 데이터 검색(을)를 참조하세요.

민감한 데이터 검색 작업

작업이라고도 하며, Macie가 S3 객체의 민감한 데이터를 탐지하고 보고하기 위해 수행하는 일련의 자동 처리 및 분석 작업입니다. 작업을 생성할 때 원하는 작업 실행 빈도를 지정하고 작업 분석의 범위와 특성을 정의합니다.

작업이 실행되면 Macie는 찾은 민감한 데이터(민감한 데이터 조사 결과) 와 수행한 분석(민감한 데이터 검색 결과)의 기록을 생성합니다. 또한 Macie는 Amazon CloudWatch Logs에 로깅 데이터를 게시합니다.

자세한 정보는 민감한 데이터 검색 작업 실행을 참조하세요.

민감한 데이터 검색 결과

객체에 민감한 데이터가 포함되어 있는지 여부를 확인하기 위해 Macie가 S3 객체에 대해 수행한 분석에 대한 세부 정보를 기록하는 레코드입니다. Macie는 이러한 레코드를 생성하여 JSON 행(.jsonl) 파일에 기록하고, 이 파일은 암호화하여 지정된 S3 버킷에 저장합니다. 레코드는 표준화된 스키마를 따릅니다.

민감한 데이터 검색 작업을 실행하거나 Macie가 민감한 데이터 자동 검색을 수행하는 경우 Macie는 분석 범위에 포함된 각 객체에 대해 민감한 데이터 검색 결과를 생성합니다. 여기에는 다음이 포함됩니다.

- Macie가 민감한 데이터를 발견하여 민감한 데이터 조사 결과를 생성하는 객체입니다.
- Macie가 민감한 데이터를 발견하지 않아 민감한 데이터 조사 결과를 생성하지 않는 객체입니다.
- 권한 설정 또는 지원되지 않는 파일 또는 저장 형식 사용과 같은 오류나 문제로 인해 Macie가 분석할 수 없는 객체입니다.

자세한 내용은 민감한 데이터 검색 결과 저장 및 유지 섹션을 참조하세요.

독립 실행형 계정

조직의 관리자도 아니고 멤버 계정도 아닌 Macie 계정입니다. 계정은 조직의 일부가 아닙니다.

표시되지 않은 결과

금지 규칙에 의해 자동으로 보관된 조사 결과입니다. 즉, Macie가 조사 결과를 생성할 때 조사 결과가 금지 규칙의 기준과 일치했기 때문에 Macie는 조사 결과 상태를 보관됨으로 자동 변경했습니다.

자세한 내용은 조사 결과 안 보이게 하기 섹션을 참조하세요.

금지 규칙

조사 결과를 자동으로 보관(금지) 하기 위해 생성하여 저장하는 속성 기반 필터 기준 세트입니다. 억제 규칙은 일련의 결과를 검토한 후 다시 알림을 받고 싶지 않은 경우에 유용합니다.

금지 규칙을 사용하여 조사 결과를 숨기는 경우 Macie는 해당 규칙의 기준에 맞는 조사 결과를 계속 생성합니다. 하지만 Macie는 자동으로 조사 결과 상태를 보관됨으로 변경합니다. 즉, Amazon Macie 콘솔에는 기본적으로 조사 결과가 표시되지 않으며 Macie는 결과를 다른 AWS 서비스에 게시하지 않습니다.

자세한 내용은 조사 결과 안 보이게 하기 섹션을 참조하세요.

분류할 수 없는 바이트 또는 크기

Macie가 제공하는 S3 버킷 통계에서 S3 버킷에 있는 모든 분류할 수 없는 객체의 총 스토리지 크기입니다.

버킷에 대한 버전 관리가 활성화된 경우, 이 값은 버킷에 있는 각 분류할 수 없는 객체의 최신 버전의 스토리지 크기를 기준으로 합니다. 객체가 압축된 파일인 경우, 이 값은 파일 압축이 풀린 후의 파일 콘텐츠의 실제 크기를 반영하지 않습니다.

자세한 정보는 S3 버킷 인벤토리 검토 및 Amazon S3 보안 태세 액세스(을)를 참조하세요.

분류할 수 없는 객체

Macie가 민감한 데이터를 탐지하기 위해 분석할 수 없는 S3 객체입니다.

S3 버킷 통계를 계산할 때 Macie는 객체의 스토리지 클래스와 파일 이름 확장자을 기반으로 객체를 분류할 수 없다고 판단합니다. 지원되는 Amazon S3 스토리지 클래스를 사용하지 않거나, 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자가 없는 경우에는 객체를 분류할 수 없습니다.

자세한 정보는 S3 버킷 인벤토리 검토 및 Amazon S3 보안 태세 액세스(을)를 참조하세요.

민감한 데이터 검색의 경우 Macie는 객체의 스토리지 클래스, 파일 이름 확장자 및 콘텐츠를 기반으로 객체를 분류할 수 없다고 판단합니다. 지원되는 Amazon S3 스토리지 클래스를 사용하지 않거나, 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자가 없거나, Macie가 객체에서 데이터를 추출 및 분석할 수 없는 경우에는 객체를 분류할 수 없습니다. 예를 들어, 객체는 형식이 잘못된 파일입니다.

자세한 정보는 민감한 데이터 검색 및 비용 예측 및 모니터링(을)를 참조하세요.

Amazon Macie를 통한 데이터 보안 및 개인정보 보호 모니터링

Amazon Macie를 활성화하면 Macie는 현재 상태인 Amazon AWS 계정 Simple Storage Service (Amazon S3) 범용 버킷의 전체 인벤토리를 자동으로 생성하여 유지 관리하기 시작합니다. AWS 리전 Macie는 또한 보안 및 액세스 제어를 위한 버킷의 평가 및 모니터링도 시작합니다. Macie는 버킷의 보안 또는 개인 정보 보호를 저해하는 이벤트를 감지하면 사용자가 필요에 따라 검토하고 수정할 수 있도록 정책을 찾습니다.

또한 민감한 데이터가 있는지 S3 버킷을 평가하고 모니터링하기 위해 민감한 데이터 검색 작업을 생성하고 실행할 수 있습니다. 민감한 데이터 검색 작업은 매일, 매주 또는 매월 버킷 객체에 대한 증분 분석을 수행할 수 있습니다. Macie가 S3 객체에서 민감한 데이터를 감지하면 Macie는 민감한 데이터 검색 결과를 생성하여 발견한 민감한 데이터를 사용자에게 알립니다. 계정 설정에 따라 민감한 데이터 자동 검색을 수행하도록 Macie를 구성할 수도 있습니다. 자동화된 민감한 데이터 검색은 샘플링 기법을 사용하여 버킷의 대표 객체를 지속적으로 식별, 선택, 분석합니다. 두 옵션에 대한 자세한 내용은 을 참조하십시오민감한 데이터 검색.

또한 Macie는 Amazon S3 데이터의 보안 및 개인 정보 보호에 대한 지속적인 가시성을 제공합니다. 데이터의 보안 상태를 평가하고 조치를 취할 위치를 결정하려면 콘솔의 요약 대시보드를 사용하면 됩니다. 대시보드를 통해 Amazon S3 데이터에 대한 집계된 통계의 스냅샷을 확인할 수 있습니다. 통계에는 공개적으로 액세스할 수 있거나 다른 사람과 공유되는 범용 버킷의 수와 같은 주요 보안 지표에 대한 데이터가 포함됩니다. AWS 계정대시보드에는 지난 7일 동안 가장 많은 조사 결과가 있는 1~5개 버킷 이름 등 계정에 대해 집계된 조사 결과 데이터 그룹 또한 표시됩니다. 각 통계를 드릴다운하여 해당 통계의 근거 데이터를 검토할 수 있습니다. 프로그래밍 방식으로 통계를 쿼리하려면 Amazon GetBucketStatisticsMacie API의 작업을 사용하십시오.

더 심층적인 분석과 평가를 위해 Macie는 인벤토리의 개별 S3 버킷에 대한 자세한 정보와 통계를 제공합니다. 여기에는 각 버킷의 퍼블릭 액세스 및 암호화 설정에 대한 분석, 버킷의 민감한 데이터를 감지하기 위해 Macie가 분석할 수 있는 객체의 크기와 개수도 포함됩니다. 또한 인벤토리에는 민감한 데이터 검색 작업을 구성했는지 아니면 버킷의 객체를 분석하기 위한 자동화된 민감한 데이터 검색을 구성했는지도 표시됩니다. 있는 경우 해당 분석이 가장 최근에 이루어진 시기가 표시됩니다. Amazon Macie 콘솔 또는 Amazon Macie API의 DescribeBuckets작업을 사용하여 인벤토리를 탐색, 정렬 및 필터링할 수 있습니다.

조직의 Macie 관리자는 멤버 계정이 소유한 S3 버킷에 대한 통계 및 기타 데이터에 액세스할 수 있습니다. 또한 Macie가 버킷에 대해 생성한 정책 결과에 액세스하고 버킷에 민감한 데이터가 있는지 검사

할 수 있습니다. 즉, Macie를 사용하여 조직의 Amazon S3 데이터 자산의 전반적인 보안 상태를 평가하고 모니터링할 수 있습니다. 자세한 내용은 여러 계정 관리을(를) 참조하세요.

주제

- Amazon Macie가 Amazon S3 데이터 보안을 모니터링하는 방법
- Amazon Macie를 사용하여 Amazon S3 보안 태세 액세스
- Amazon Macie를 통한 Amazon S3 보안 태세 분석
- Amazon Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용

Amazon Macie가 Amazon S3 데이터 보안을 모니터링하는 방법

Amazon Macie를 활성화하면 Macie는 현재 계정에 AWS 계정대해 AWS Identity and Access Management (IAM) 서비스 연결 역할을 생성합니다. AWS 리전이 역할에 대한 권한 정책을 통해 Macie는 사용자를 대신하여 다른 사람에게 전화를 AWS 서비스 걸고 리소스를 모니터링할 수 있습니다. AWS 이 역할을 사용하여 Macie는 리전에서 Amazon Simple Storage Service (Amazon S3) 범용 버킷의 전체 인벤토리를 생성하고 유지 관리합니다. 또한 Macie는 보안 및 액세스 제어를 위해 버킷을 모니터링하고 평가합니다.

조직의 Macie 관리자인 경우 인벤토리에는 사용자 계정 및 조직 내 구성원 계정의 S3 버킷에 대한 통계 및 기타 데이터가 포함됩니다. 이 데이터를 통해 Macie를 사용하여 Amazon S3 데이터 자산 전반에 걸쳐 조직의 보안 상태를 모니터링하고 평가할 수 있습니다. 자세한 정보는 여러 계정 관리을 참조하세요.

주제

- 핵심 구성 요소
- 데이터 새로 고침
- 추가 고려 사항

핵심 구성 요소

Amazon Macie는 다양한 기능과 기술을 사용하여 S3 범용 버킷에 대한 인벤토리 데이터를 제공 및 유지하고 보안 및 액세스 제어를 위해 버킷을 모니터링 및 평가합니다.

메타데이터 수집 및 통계 계산

버킷 인벤토리에 대한 메타데이터와 통계를 생성하고 유지하기 위해 Macie는 Amazon S3에서 직접 버킷 및 객체 메타데이터를 검색합니다. 각 버킷의 메타데이터에는 다음이 포함됩니다.

- 버킷의 이름, Amazon Resource Name (ARN), 생성 날짜, 암호화 설정, 태그, 버킷을 소유한 계정 ID 등과 같은 버킷에 대한 일반 정보. AWS 계정
- 버킷에 적용되는 계정 수준의 권한 설정(예: 계정의 공개 액세스 차단 설정).
- 버킷에 대한 버킷 수준 권한 설정(예: 버킷에 대한 공개 액세스 차단 설정, 버킷 정책 또는 액세스 제어 목록(ACL)에서 파생되는 설정).
- 버킷에 대한 공유 액세스 및 복제 설정 (버킷 데이터를 조직에 속하지 AWS 계정 않은 사람과 복제할지 또는 공유할지 여부 포함)
- 버킷의 객체 수 및 설정(예: 버킷의 객체 수, 암호화 유형, 파일 유형, 스토리지 클래스별 객체 수 분류).

Macie는 이 정보를 사용자에게 직접 제공합니다. 또한 Macie는 이 정보를 사용하여 통계를 계산하고 전체 버킷 인벤토리와 인벤토리 내 개별 버킷의 보안 및 개인 정보 보호에 대한 평가를 제공합니다. 예를 들어, 인벤토리의 총 스토리지 크기 및 버킷 수, 총 스토리지 크기 및 해당 버킷의 객체 수, Macie가 버킷의 민감한 데이터를 탐지하기 위해 분석할 수 있는 총 스토리지 크기 및 객체 수 등을 확인할 수 있습니다.

기본적으로 메타데이터와 통계에는 불완전한 멀티파트 업로드로 인해 존재하는 모든 객체 부분에 대한 데이터가 포함됩니다. 특정 버킷의 객체 메타데이터를 수동으로 새로 고치는 경우 Macie는 버킷 및 전체 버킷 인벤토리에 대한 통계를 다시 계산하고 객체 부분에 대한 데이터는 재계산된 값에서 제외합니다. 다음에 Macie가 일일 새로 고침 주기의 일부로 Amazon S3에서 버킷 및 객체 메타데이터를 검색할 때 Macie는 인벤토리 데이터를 업데이트하고 객체 부분에 대한 데이터를 다시 포함합니다. Macie가 버킷 및 객체 메타데이터를 검색하는 시점에 대한 자세한 내용은 데이터 새로 고침을 참조하세요.

Macie가 민감한 데이터를 탐지하기 위해 분석할 수 없는 객체의 부분이라는 점에 유의하는 것이 중요합니다. Amazon S3는 먼저 Macie가 분석할 수 있도록 부품을 하나 이상의 객체로 조립하는 작업을 완료해야 합니다. 수명 주기 규칙에 따라 파트를 자동으로 삭제하는 방법을 비롯하여 멀티파트 업로드 및 객체 파트에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 멀티파트 업로드를 사용한 객체 업로드 및 복사를 참조하세요. Amazon S3 Storage Lens에서 불완전한 멀티파트 업로드 지표를 참조하여 객체 부분이 포함된 버킷을 식별할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 스토리지 활동 및 사용량 평가를 참조하세요.

버킷 보안 및 개인정보 보호 모니터링

인벤토리의 버킷 수준 데이터의 정확성을 보장하기 위해 Macie는 Amazon S3 데이터에 발생할 수 있는 특정 AWS CloudTrail 이벤트를 모니터링하고 분석합니다. 관련 이벤트가 발생하면 Macie는 적절한 인벤토리 데이터를 업데이트합니다.

예를 들어, 버킷의 공개 액세스 차단 설정을 활성화하면 Macie는 버킷의 공개 액세스 설정에 대한 모든 데이터를 업데이트합니다. 마찬가지로 버킷에 대한 버킷 정책을 추가하거나 업데이트하는 경우 Macie는 정책을 분석하고 인벤토리의 관련 데이터를 업데이트합니다.

Macie는 다음 이벤트에 대한 데이터를 모니터링하고 분석합니다. CloudTrail

- 계정 수준 이벤트 — 및 DeletePublicAccessBlock PutPublicAccessBlock
- 버킷 수준 이벤트 —CreateBucket,,, DeleteAccountPublicAccessBlock, DeleteBucket,DeleteBucketEncryption, DeleteBucketPolicy, DeleteBucketPublicAccessBlock,DeleteBucketReplication,, DeleteBucketTagging, PutAccountPublicAccessBlock,PutBucketAcl, PutBucketEncryption, PutBucketPolicy PutBucketPublicAccessBlock PutBucketReplication PutBucketTagging PutBucketVersioning

추가 CloudTrail 이벤트에 대한 모니터링을 활성화하거나 이전 이벤트에 대한 모니터링을 비활성화할 수 없습니다. 이전 이벤트의 해당 작업에 대한 자세한 내용은 Amazon Simple Storage Service API 참조를 참조하세요.

> **Tip**
>
> 객체 수준 이벤트를 모니터링하려면 Amazon의 Amazon S3 보호 기능을 사용하는 것이 좋습니다. GuardDuty 이 기능은 객체 수준의 Amazon S3 데이터 이벤트를 모니터링하고 악성 및 의심스러운 활동을 분석합니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 GuardDuty Amazon에서의 Amazon S3 보호를 참조하십시오.

버킷 보안 및 액세스 제어 평가

버킷 수준의 보안 및 액세스 제어를 평가하기 위해 Macie는 자동화된 로직 기반 추론을 사용하여 버킷에 적용되는 리소스 기반 정책을 분석합니다. 또한 Macie는 버킷에 적용되는 계정 및 버킷 수준의 권한 설정을 분석합니다. 이 분석에는 계정과 버킷에 대한 버킷 정책, 버킷 수준 ACL, 공개 액세스 차단 설정이 고려됩니다.

리소스 기반 정책의 경우 Macie는 Zelkova를 사용합니다. Zelkova는 AWS Identity and Access Management (IAM) 정책을 논리적 명령문으로 변환하고 의사 결정 문제에 대한 범용 및 특수 논리

해결사 모음 (만족도 모듈로 이론) 을 실행하는 자동화된 추론 엔진입니다. Macie는 정책이 허용하는 행동 수준을 특성화하기 위해 점점 더 구체적인 쿼리가 있는 정책에 Zelkova를 반복적으로 적용합니다. Zelkova가 사용하는 해석기의 특성에 대해 자세히 알아보려면 만족도 모듈로 이론을 참조하세요.

> **Important**
>
> 버킷에 대해 위의 작업을 수행하려면 해당 버킷이 S3 범용 버킷이어야 합니다. Macie는 S3 디렉터리 버킷을 모니터링하거나 분석하지 않습니다.
>
> 또한 Macie가 버킷에 액세스할 수 있어야 합니다. 버킷의 권한 설정으로 인해 Macie가 버킷 또는 버킷의 객체에 대한 메타데이터를 검색할 수 없는 경우, Macie는 버킷에 대한 일부 정보만 제공할 수 있습니다. 여기에는 버킷 이름과 생성한 날짜가 포함됩니다. Macie는 버킷에 대한 추가 작업을 수행할 수 없습니다. 자세한 내용은 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용 섹션을 참조하세요.

데이터 새로 고침

Amazon Macie를 활성화하면 Macie는 Amazon AWS 계정 S3에서 직접 S3 범용 버킷 및 객체에 대한 메타데이터를 검색합니다. 이후 Macie는 일일 새로 고침 주기의 일부로 Amazon S3에서 직접 버킷 및 객체 메타데이터를 매일 자동으로 검색합니다.

또한 Macie는 다음이 발생할 때 Amazon S3에서 직접 버킷 메타데이터를 검색합니다.

- Amazon Macie 콘솔에서 새로 고침 ()을 선택하여 인벤토리 데이터를 새로 고칩니다. 매 5분 빈도로 데이터를 새로 고칠 수 있습니다.
- Amazon Macie API에 프로그래밍 방식으로 DescribeBuckets요청을 제출했지만 지난 5분 동안 DescribeBuckets 요청을 제출하지 않았습니다.
- Macie는 관련 이벤트를 감지합니다. AWS CloudTrail

Macie는 데이터를 수동으로 새로 고치기로 선택한 경우 특정 버킷의 최신 객체 메타데이터를 검색할 수도 있습니다. 최근에 버킷을 만들었거나 지난 24시간 동안 버킷의 객체를 상당 부분 변경한 경우에 유용할 수 있습니다. 버킷의 객체 메타데이터를 수동으로 새로 고치려면 콘솔의 S3 버킷 페이지에 있는 버킷 세부 정보 패널의 객체 통계 섹션에서 새로 고침

( )
을 선택합니다. 이 기능은 30,000개 이하의 객체를 저장하는 버킷에 사용할 수 있습니다.

Macie가 버킷 또는 객체 메타데이터를 검색할 때마다 Macie는 인벤토리의 모든 관련 데이터를 자동으로 업데이트합니다. Macie는 버킷의 보안 또는 개인 정보 보호에 영향을 미치는 차이점을 탐지하면 즉시 변경 사항을 평가하고 분석하기 시작합니다. 분석이 완료되면 Macie는 인벤토리의 관련 데이터를 업데이트합니다. 버킷의 보안 또는 개인정보 보호를 약화시키는 차이점을 탐지하면 Macie는 사용자가 검토하고 필요에 따라 수정할 수 있도록 정책 조사 결과를 생성합니다.

Macie가 계정에 대한 버킷 또는 객체 메타데이터를 가장 최근에 검색한 시점을 확인하려면 콘솔의 최근 업데이트 필드를 참조하세요. 이 필드는 요약 대시보드, S3 버킷 페이지 및 S3 버킷 페이지의 버킷 세부 정보 패널에 표시됩니다. (Amazon Macie API를 사용하여 재고 데이터를 쿼리하는 경우 `lastUpdated` 필드에 이 정보가 제공됩니다.) 조직의 Macie 관리자인 경우 최근 업데이트 필드에는 Macie가 조직 계정의 데이터를 검색한 가장 최근 날짜와 시간이 표시됩니다.

드문 경우이긴 하지만, 특정 조건에서는 지연 시간 및 기타 문제로 인해 Macie가 버킷 및 객체 메타데이터를 검색하지 못할 수 있습니다. 또한 이로 인해 버킷 인벤토리 변경 사항이나 개별 버킷의 권한 설정 및 정책에 대한 Macie의 알림이 지연될 수도 있습니다. 예를 들어 CloudTrail 이벤트와 관련된 전송 문제로 인해 지연이 발생할 수 있습니다. 이 경우 Macie는 다음 번에 24시간 이내에 매일 새로 고침을 수행할 때 새 데이터와 업데이트된 데이터를 분석합니다.

추가 고려 사항

Amazon Macie를 사용하여 Amazon S3 데이터의 보안 태세를 모니터링하고 평가할 때는 다음 사항에 유의하세요.

- 인벤토리 데이터는 현재의 AWS 리전 S3 범용 버킷에만 적용됩니다. 추가 리전의 데이터에 액세스하려면 각 추가 리전에서 Macie를 활성화하고 사용하세요.
- 조직의 Macie 관리자인 경우 현재 리전에서 Macie가 해당 계정에 대해 활성화된 경우에만 멤버 계정의 인벤토리 데이터에 액세스할 수 있습니다.
- 버킷의 권한 설정으로 인해 Macie가 버킷 또는 버킷의 객체에 대한 정보를 검색할 수 없는 경우, Macie는 버킷 데이터의 보안 및 개인정보를 평가 및 모니터링하거나 버킷의 세부 정보를 제공할 수 없습니다.

  이러한 경우에 해당하는 버킷을 식별할 수 있도록 Macie는 다음과 같은 작업을 수행합니다.

  - 버킷 인벤토리에서 Macie는 해당 버킷에 대한 경고 아이콘
    ( )
    을 표시합니다. 버킷 세부 정보의 경우 Macie는 버킷을 소유한 계정 ID, 버킷 이름, Amazon

Resource Name (ARN), 생성 날짜, 지역, Macie가 가장 최근에 일일 새로 고침 주기의 일부로 버킷에 대한 버킷과 객체 메타데이터를 모두 검색한 날짜 및 시간 등 필드 및 데이터의 하위 집합만 표시합니다. AWS 계정 Amazon Macie API를 사용하여 인벤토리 데이터를 쿼리하는 경우 Macie는 버킷에 대한 오류 코드와 메시지를 제공하며 대부분의 버킷 속성 값은 null입니다.

- 요약 대시보드에서 버킷의 공개 액세스, 암호화 및 공유 통계 값은 알 수 없음으로 설정되어 있습니다. (Amazon Macie API를 사용하여 통계를 쿼리하는 경우, 버킷은 이 통계에 대해 unknown에 해당하는 값을 보유합니다.) 또한 Macie는 스토리지 및 객체 통계에 대한 데이터를 계산할 때 버킷을 제외합니다.

문제를 조사하려면 Amazon S3의 버킷 정책 및 권한 설정을 검토하십시오. 예를 들어 버킷에 제한적인 버킷 정책이 있을 수 있습니다. 자세한 내용은 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용 섹션을 참조하세요.

- 액세스 및 권한에 대한 데이터는 계정 및 버킷 수준 설정으로 제한됩니다. 버킷의 특정 객체에 대한 액세스를 결정하는 객체 수준 설정은 반영하지 않습니다. 예를 들어, 버킷의 특정 객체에 대해 공개 액세스가 활성화된 경우, Macie는 해당 버킷 또는 버킷의 객체에 공개적으로 액세스할 수 있다고 보고하지 않습니다.

  객체 수준 작업을 모니터링하고 잠재적인 보안 위험을 식별하려면 Amazon의 Amazon S3 보호 기능을 사용하는 것이 좋습니다. GuardDuty 이 기능은 객체 수준의 Amazon S3 데이터 이벤트를 모니터링하고 악성 및 의심스러운 활동을 분석합니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 GuardDuty Amazon에서의 Amazon S3 보호를 참조하십시오.

- 특정 버킷의 객체 메타데이터를 수동으로 새로 고침하면 Macie는 객체에 적용되는 암호화 통계를 일시적으로 알 수 없음으로 보고합니다. 다음에 Macie가 매일 데이터를 새로 고칠 때(24시간 이내) Macie는 객체의 암호화 메타데이터를 재평가하고 통계를 위해 정량적 데이터를 다시 보고합니다.
- 특정 버킷의 객체 메타데이터를 수동으로 새로 고치는 경우 Macie는 불완전한 멀티파트 업로드로 인해 버킷에 포함된 모든 객체 부분의 데이터를 일시적으로 제외합니다. 다음에 Macie가 매일 데이터 새로 고침을 수행하면(24시간 이내) Macie는 버킷 객체의 개수 및 스토리지 크기 값을 다시 계산하고 해당 계산에 해당 부분에 대한 데이터를 포함합니다.
- 드문 경우이긴 하지만, Macie는 버킷이 공개적으로 액세스 가능한지 또는 공유되는지 판단하지 못하거나 새 객체의 서버 측 암호화가 필요한지 확인하지 못할 수도 있습니다. 예를 들어, 일시적인 문제로 인해 Macie가 필요한 데이터를 검색하고 분석하지 못할 수 있습니다. 또는 Macie는 하나 이상의 정책 명령문이 외부 주체에 대한 액세스 권한을 부여하는지를 완전히 판단하지 못할 수도 있습니다. 이러한 경우 Macie는 인벤토리의 관련 통계 및 필드에 대해 알 수 없음을 보고합니다. 이러한 사례를 조사하려면 Amazon S3의 버킷 정책 및 권한 설정을 검토하세요.

또한 Macie는 계정에서 Macie를 활성화한 후 버킷의 보안 또는 개인 정보 보호가 저하되는 경우에만 정책 조사 결과를 생성한다는 점에 유의하세요. 예를 들어 Macie를 활성화한 후 버킷에 대한 공개 액세스 차단 설정을 비활성화하면 Macie는 해당 버킷에 대해 정책:IAmuser/S3 찾기 기능을 생성합니다. BlockPublicAccessDisabled 하지만 Macie를 활성화했을 때 버킷에 대한 공개 액세스 차단 설정이 비활성화되었는데도 계속 비활성화되어 있는 경우 Macie는 해당 버킷에 대해 정책:IAmuser/S3 찾기 기능을 생성하지 않습니다. BlockPublicAccessDisabled

또한 Macie는 버킷의 보안 및 개인 정보를 평가할 때 액세스 로그를 검사하거나 사용자, 역할 및 계정에 대한 기타 관련 구성을 분석하지 않습니다. 대신 Macie는 잠재적 보안 위험을 나타내는 주요 설정에 대한 데이터를 분석하고 보고합니다. 예를 들어, 정책 조사 결과에 따르면 버킷에 공개적으로 액세스할 수 있는 것으로 나타났다고 해서 반드시 외부 주체가 버킷에 액세스했다는 의미는 아닙니다. 마찬가지로, 정책 결과에 따르면 버킷이 조직 AWS 계정 외부와 공유되는 것으로 나타나는 경우 Macie는 이러한 액세스가 의도되고 안전한지 여부를 확인하려고 하지 않습니다. 대신 이러한 조사 결과는 외부 주체가 잠재적으로 버킷 데이터에 액세스할 수 있다는 것을 나타내며, 이는 의도하지 않은 보안 위험일 수 있습니다.

Amazon Macie를 사용하여 Amazon S3 보안 태세 액세스

Amazon Macie 콘솔의 요약 대시보드를 사용하여 Amazon Simple Storage Service(S3) 데이터의 전반적 보안 태세를 평가하고 조치를 취할 위치를 결정할 수 있습니다.

요약 대시보드는 현재 AWS 리전의 Amazon S3 데이터에 대한 집계된 통계의 스냅샷을 제공합니다. 통계에는 공개적으로 액세스할 수 있거나 다른 AWS 계정사람과 공유되는 범용 버킷의 수와 같은 주요 보안 지표에 대한 데이터가 포함됩니다. 또한 대시보드에는 계정에 대해 집계된 조사 결과 데이터 그룹(예: 지난 7일 동안 가장 많이 발생한 조사 결과 유형)이 표시됩니다. 조직의 Macie 관리자인 경우, 대시보드는 조직 내 모든 계정에 대한 집계된 통계 및 데이터를 제공합니다. 필요에 따라 계정별로 데이터를 필터링할 수 있습니다.

더 심층적인 분석을 수행하려면 대시보드에서 개별 항목에 대한 지원 데이터를 드릴다운하고 검토할 수 있습니다. Amazon Macie 콘솔을 사용하여 S3 버킷 인벤토리를 검토 및 분석하거나 Amazon Macie API의 DescribeBuckets작업을 사용하여 프로그래밍 방식으로 인벤토리 데이터를 쿼리 및 분석할 수도 있습니다.

주제

- 요약 대시보드 표시
- 요약 대시보드의 구성 요소 이해
- 요약 대시보드의 데이터 보안 통계 이해

요약 대시보드 표시

Amazon Macie 콘솔에서, 요약 대시보드는 현재 AWS 리전의 Amazon S3 데이터에 대한 집계된 통계 및 조사 결과 데이터의 스냅샷을 제공합니다. 프로그래밍 방식으로 통계를 쿼리하려는 경우 Amazon Macie API의 GetBucketStatistics작업을 사용할 수 있습니다.

요약 대시보드를 표시하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다. Macie는 요약 대시보드를 표시합니다.
3. Macie가 사용자 계정의 Amazon S3에서 가장 최근에 버킷 또는 객체 메타데이터를 검색한 시점을 확인하려면 대시보드 상단의 마지막 업데이트 필드를 참조하세요. 자세한 내용은 데이터 새로 고침 섹션을 참조하세요.
4. 대시보드의 항목에 대한 지원 데이터를 자세히 살펴보고 검토하려면 해당 항목을 선택합니다.

조직의 Macie 관리자인 경우, 대시보드는 사용자의 계정 및 조직의 멤버 계정에 대한 집계된 통계 및 데이터를 표시합니다. 대시보드를 필터링하고 특정 계정에 대한 데이터만 표시하려면 계정 상자에 계정 ID를 입력합니다.

요약 대시보드의 구성 요소 이해

요약 대시보드에는 통계 및 데이터가 여러 섹션으로 구성되어 있습니다. 대시보드 상단에는 Amazon S3에 저장하는 데이터의 양과 Amazon Macie가 민감한 데이터를 탐지하기 위해 분석할 수 있는 데이터의 양을 나타내는 집계된 통계가 있습니다. 또한 마지막 업데이트 필드를 참조하여 Macie가 사용자 계정의 Amazon S3에서 가장 최근에 버킷 또는 객체 메타데이터를 검색한 시점을 확인할 수 있습니다. 추가 섹션에서는 현재 AWS 리전의 Amazon S3 데이터의 보안, 개인정보 보호 및 민감도를 평가하는 데 도움이 되는 통계 및 최근 조사 결과 데이터를 제공합니다.

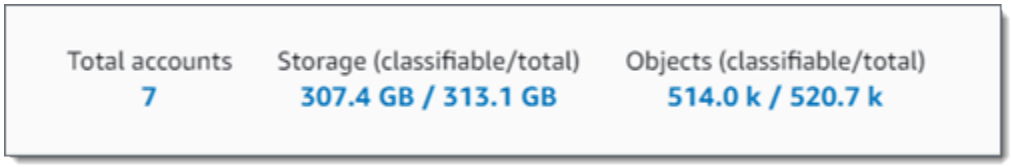
통계 및 데이터는 다음 섹션으로 구성되어 있습니다.

스토리지 및 민감한 데이터 검색 | 자동 검색 및 범위 문제 | 데이터 보안 | 상위 S3 버킷 | 주요 조사 결과 유형 | 정책 조사 결과

각 섹션을 검토할 때는 선택적으로 드릴다운할 항목을 선택하여 지원 데이터를 검토할 수 있습니다. 또한 대시보드에는 S3 디렉터리 버킷에 대한 데이터가 포함되지 않고 범용 버킷에 대한 데이터만 포함됩니다. Macie는 디렉터리 버킷을 모니터링하거나 분석하지 않습니다.

스토리지 및 민감한 데이터 검색

대시보드 상단의 통계는 Amazon S3에 저장하는 데이터의 양과 Macie가 민감한 데이터를 탐지하기 위해 분석할 수 있는 데이터의 양을 나타냅니다. 예:



이 섹션:

- 총 계정 - 조직의 Macie 관리자거나 독립형 Macie 계정이 있는 경우 이 필드가 표시됩니다. 버킷 인벤토리에 AWS 계정 있는 해당 버킷의 총 개수를 나타냅니다. 귀하가 Macie 관리자인 경우, 이는 조직을 위해 귀하가 관리하는 Macie 계정의 총 수입니다. 독립형 Macie 계정이 있는 경우, 이 값은 1입니다.

  총 S3 버킷 - 이 필드는 Macie 계정이 조직의 멤버인 경우 나타납니다. 객체를 저장하지 않는 버킷을 포함하여 인벤토리에 있는 범용 버킷의 총 개수를 나타냅니다.
- 스토리지 - 이 지표는 버킷 인벤토리에 있는 객체의 스토리지 크기에 대한 정보를 제공합니다.
  - 분류 가능 - Macie가 버킷에서 분석할 수 있는 모든 객체의 총 스토리지 크기입니다.
  - 합계 - Macie가 분석할 수 없는 객체를 포함하여 버킷에 있는 모든 객체의 총 스토리지 크기입니다.

  객체가 압축된 파일인 경우, 이러한 값은 압축을 푼 후의 해당 파일의 실제 크기를 반영하지 않습니다. 모든 버킷에 버전 관리가 활성화된 경우, 이 값은 해당 버킷에 있는 각 객체의 최신 버전 스토리지 크기를 기반으로 합니다.
- 객체- 이 지표는 버킷 인벤토리의 객체 수에 대한 정보를 제공합니다.
  - 분류 가능 - Macie가 버킷에서 분석할 수 있는 총 객체 수입니다.
  - 합계 - Macie가 분석할 수 없는 객체를 포함하여 버킷에 있는 총 객체 수입니다.

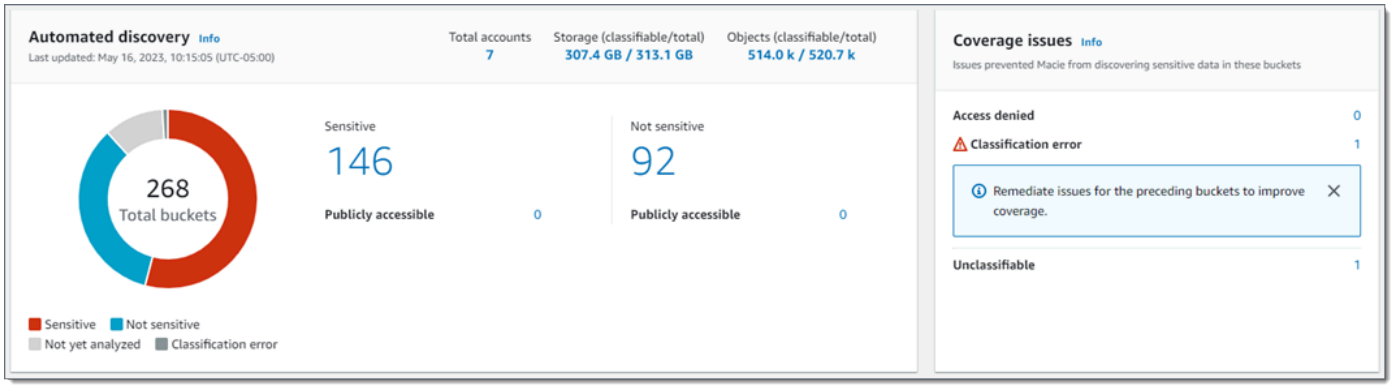
위 통계에서 데이터와 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자가 있는 경우, 분류 가능합니다. Macie를 사용하여 객체에서 민감한 데이터를 탐지할 수 있습니다. 자세한 내용은 지원하는 스토리지 클래스 및 형식 섹션을 참조하세요.

참고로 스토리지 및 객체 통계에는 Macie가 액세스할 수 없는 버킷의 객체에 대한 데이터는 포함되지 않습니다. 제한적인 버킷 정책이 적용되는 버킷의 객체를 예로 들 수 있습니다. 해당하는 버킷을 식별하려면, S3 버킷 테이블

을 사용하여 버킷 인벤토리를 검토할 수 있습니다. 버킷 이름 옆에 경고 아이콘 (⚠) 이 표시되면 Macie는 해당 버킷에 액세스할 수 없습니다.

자동 검색 및 범위 문제

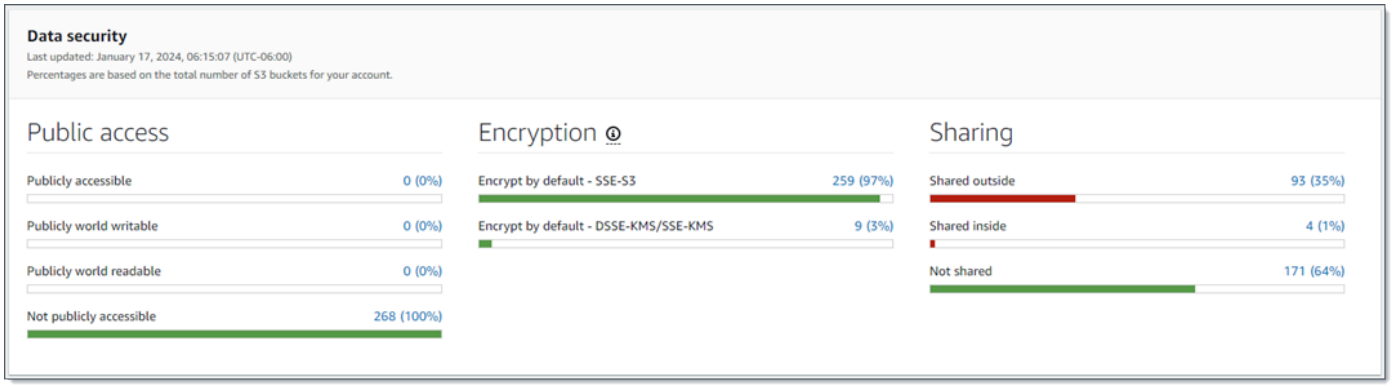
민감한 데이터 자동 검색이 활성화된 경우 이러한 섹션이 대시보드에 표시됩니다. 이 섹션의 통계는 Macie가 Amazon S3 데이터에 대해 지금까지 수행한 민감한 데이터 자동 검색 활동의 상태 및 결과를 수집합니다. 예:



통계에 대한 자세한 내용은 요약 대시보드에서 집계된 데이터 민감도 통계 검토(을)를 참조하세요.

데이터 보안

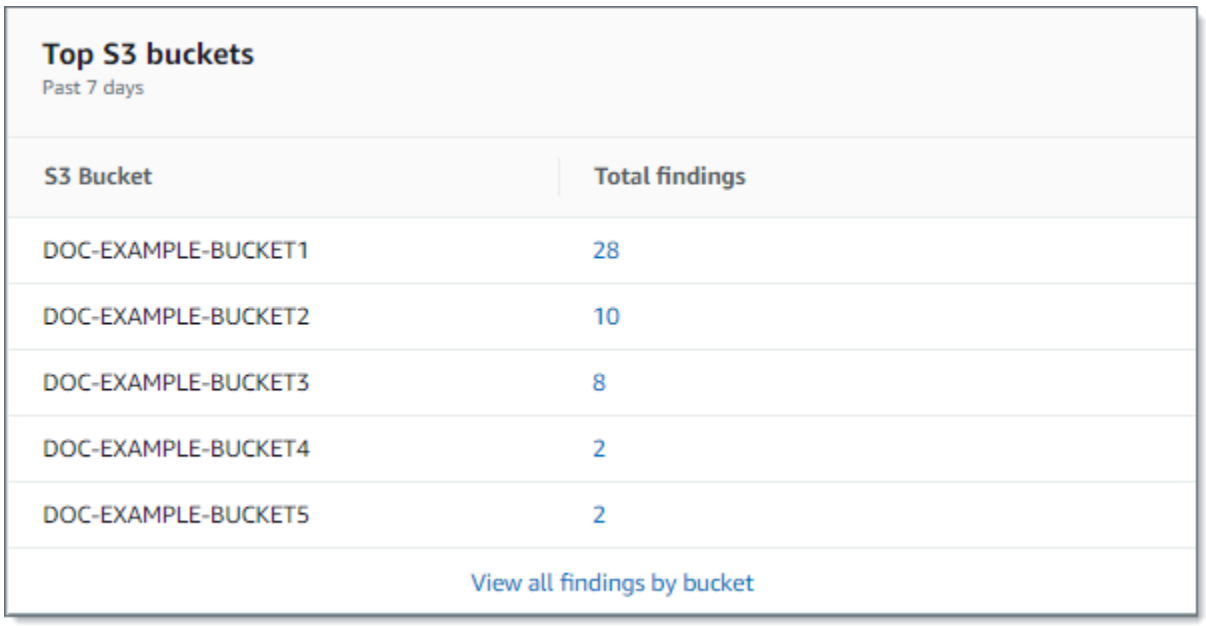
이 섹션에서는 Amazon S3 데이터에 대한 잠재적 보안 및 개인 정보 보호 위험을 나타내는 통계를 제공합니다. 예:



통계에 대한 자세한 내용은 요약 대시보드의 데이터 보안 통계 이해(을)를 참조하세요.

상위 S3 버킷

이 섹션에는 지난 7일 동안 최대 5개 버킷에 대해 모든 유형의 조사 결과를 가장 많이 생성한 S3 버킷이 나열되어 있습니다. 또한 Macie가 각 버킷에 대해 생성한 조사 결과의 수를 나타냅니다. 예:

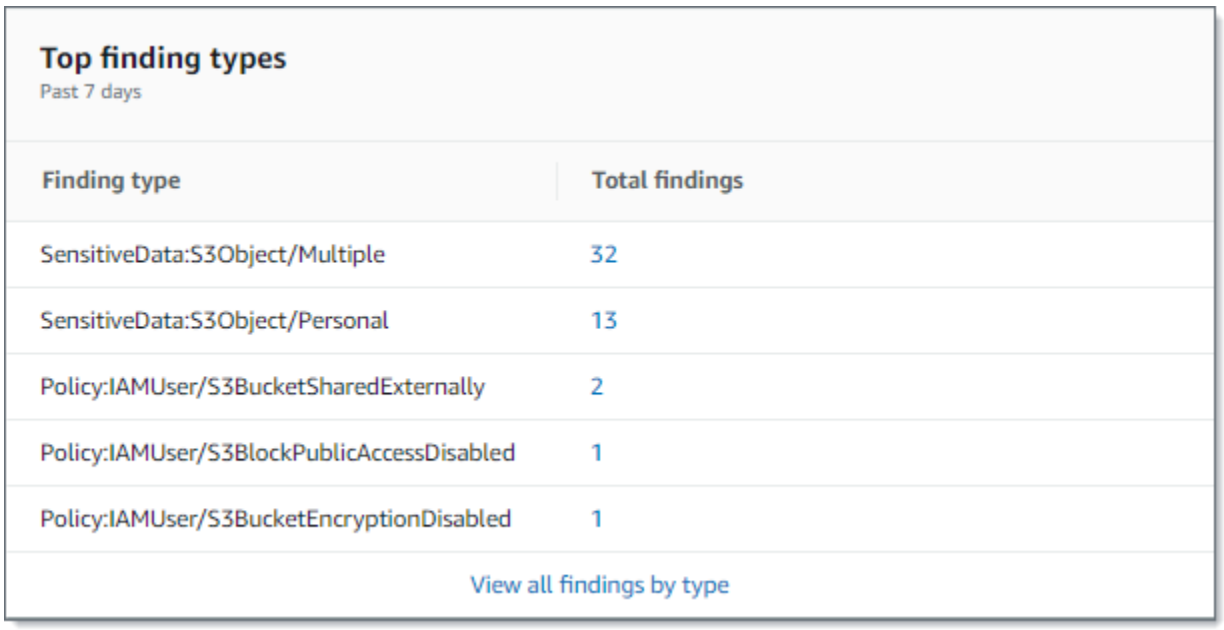


지난 7일 동안의 버킷에 대한 모든 조사 결과를 표시하고 선택적으로 드릴다운하려면 전체 조사 결과 필드에서 값을 선택합니다. 모든 버킷에 대한 모든 현재 조사 결과를 버킷별로 그룹화하여 표시하려면 버킷별로 모든 조사 결과 보기를 선택합니다.

Macie가 지난 7일 동안 조사 결과를 생성하지 않은 경우 이 섹션은 비어 있습니다. 또는 지난 7일 동안 생성된 모든 조사 결과는 금지 규칙에 의해 숨겨집니다.

상위 조사 결과 유형

이 섹션에는 지난 7일 동안 가장 많이 발생한 조사 결과 유형(최대 5개 유형)이 나열되어 있습니다. 또한 Macie가 각 유형에 대해 생성한 조사 결과의 수를 나타냅니다. 예:



지난 7일 동안의 특정 유형의 모든 조사 결과를 표시하고 선택적으로 드릴다운하려면 전체 조사 결과 필드에서 값을 선택합니다. 모든 현재 조사 결과를 조사 결과 유형별로 그룹화하여 표시하려면 유형별로 모든 조사 결과 보기를 선택합니다.

Macie가 지난 7일 동안 조사 결과를 생성하지 않은 경우 이 섹션은 비어 있습니다. 또는 지난 7일 동안 생성된 모든 조사 결과는 금지 규칙에 의해 숨겨집니다.

정책 조사 결과

이 섹션에는 Macie가 가장 최근에 생성하거나 업데이트한 정책 조사 결과(최대 10개의 조사 결과)가 나열되어 있습니다. 예:

특정 조사 결과의 세부 정보를 표시하려면 조사 결과를 선택합니다.

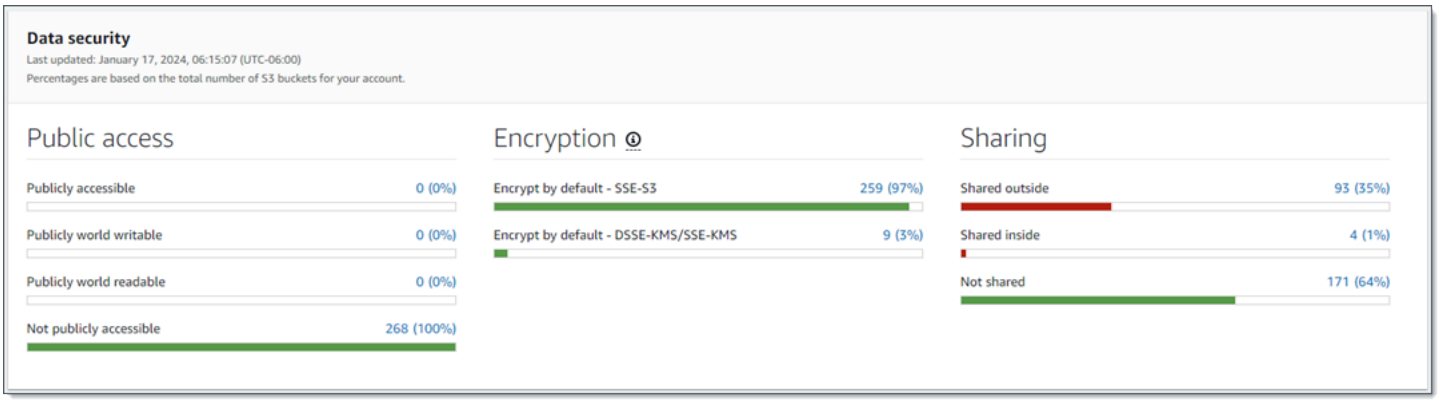
Macie가 지난 7일 동안 정책 조사 결과를 생성하거나 업데이트하지 않은 경우 이 섹션은 비어 있습니다. 또는 지난 7일 동안 생성되거나 업데이트된 모든 정책 조사 결과는 금지 규칙에 의해 숨겨집니다.

요약 대시보드의 데이터 보안 통계 이해

요약 대시보드의 데이터 보안 섹션은 현재 AWS 리전의 Amazon S3 데이터에 대한 잠재적 보안 및 개인정보 보호 위험을 식별하고 조사하는 데 도움이 되는 통계를 제공합니다. 예를 들어 이 데이터를 사용하여 공개적으로 액세스할 수 있거나 다른 AWS 계정사람과 공유하는 범용 버킷을 식별할 수 있습니다.

Macie 계정이 조직의 멤버인 경우 이 섹션 상단의 스토리지 및 민감한 데이터 검색 통계에 Amazon S3에 저장하는 데이터의 양과 Macie가 민감한 데이터를 탐지하기 위해 분석할 수 있는 데이터의 양이 나와 있습니다.

모든 유형의 Macie 계정에 대해, 다음 이미지와 같이 추가 통계가 세 가지 영역으로 구성되어 있습니다.



각 영역을 검토하면서 필요에 따라 드릴다운할 항목을 선택하여 지원 데이터를 검토할 수 있습니다. 또한 통계에는 S3 디렉터리 버킷에 대한 데이터는 포함되지 않고 범용 버킷에 대한 데이터만 포함됩니다. Macie는 디렉터리 버킷을 모니터링하거나 분석하지 않습니다.

각 영역의 개별 통계는 다음과 같습니다.

공개 액세스(Public access)

이 통계는 공개적으로 액세스할 수 있거나 액세스할 수 없는 S3 버킷 수를 나타냅니다.

- 공개적으로 액세스 가능 - 일반 대중이 버킷에 대한 읽기 또는 쓰기 액세스 권한을 가질 수 있는 버킷의 총 수 및 백분율입니다.
- 공개적으로 전체 쓰기 가능 - 일반 대중이 버킷에 대한 쓰기 액세스 권한을 가질 수 있는 버킷의 총 수입니다.
- 공개적으로 전체 읽기 가능 - 일반 대중이 버킷에 대한 읽기 액세스 권한을 가질 수 있는 버킷의 총 수입니다.

- 공개적으로 액세스할 수 없음 - 일반 대중이 버킷에 대한 읽기 또는 쓰기 액세스 권한을 가질 수 없는 버킷의 총 수입니다.

각 백분율을 계산하기 위해 Macie는 해당 버킷 수를 버킷 인벤토리의 총 버킷 수로 나눕니다.

이 섹션에서 값을 결정하기 위해 Macie는 계정의 공개 액세스 차단 설정, 버킷의 공개 액세스 차단 설정, 버킷의 버킷 정책, 버킷의 액세스 제어 목록(ACL) 등 각 버킷에 대한 계정 및 버킷 수준 설정의 조합을 분석합니다. 이러한 설정에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3의 ID 및 액세스 관리 및 Amazon S3 스토리지에 대한 공개 액세스 차단을 참조하세요.

경우에 따라 공개 액세스 섹션에 알 수 없음에 대한 값도 표시됩니다. 이러한 값이 나타나면, Macie는 지정된 버킷 수 및 백분율에 대한 공개 액세스 설정을 평가할 수 없었습니다. 예를 들어, 일시적인 문제나 버킷의 권한 설정으로 인해 Macie는 필요한 데이터를 검색하지 못했습니다. 또는 Macie는 하나 이상의 정책 문이 외부 주체의 버킷 액세스를 허용하는지를 완전히 판단할 수 없었습니다.

암호화(Encryption)

이 통계는 버킷에 추가된 객체에 특정 유형의 서버 측 암호화를 적용하도록 구성된 S3 버킷 수를 나타냅니다.

- 기본적으로 암호화 - SSE-S3 - Amazon S3 관리 키를 사용하여 새 객체를 암호화하도록 기본 암호화 설정이 구성된 버킷 수와 백분율입니다. 이 버킷의 경우 새 객체는 SSE-S3 암호화를 사용하여 자동으로 암호화됩니다.
- 기본 암호화 — DSSE-KMS/SSE-KMS — 기본 암호화 설정이 A 또는 고객 관리 키를 사용하여 새 객체를 암호화하도록 구성된 버킷의 수와 비율입니다. AWS KMS key AWS 관리형 키 이러한 버킷의 경우 새 객체는 DSSE-KMS 또는 SSE-KMS 암호화를 사용하여 자동으로 암호화됩니다.

각 백분율을 계산하기 위해 Macie는 해당 버킷 수를 버킷 인벤토리의 총 버킷 수로 나눕니다.

이 섹션의 값을 결정하기 위해 Macie는 각 버킷의 기본 암호화 설정을 분석합니다. 2023년 1월 5일부터 Amazon S3가 Amazon S3 관리형 키를 사용한 서버 측 암호화 (SSE-S3) 를 버킷에 추가되는 객체의 암호화의 기본 수준으로 자동 적용합니다. 선택적으로 키를 사용한 서버 측 암호화 (SSE-KMS) 또는 AWS KMS 키를 사용한 이중 레이어 서버 측 암호화 (DSSE-KMS) 를 대신 사용하도록 버킷의 기본 암호화 설정을 구성할 수 있습니다. AWS KMS 기본 암호화 설정 및 옵션에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 S3 버킷의 기본 서버 측 암호화 동작 설정을 참조하세요.

경우에 따라 암호화 섹션에 알 수 없음에 대한 값도 표시됩니다. 이러한 값이 나타나면 Macie는 지정된 버킷 수 및 백분율에 대한 기본 암호화 설정을 평가할 수 없었습니다. 예를 들어, 일시적인 문제나 버킷의 권한 설정으로 인해 Macie는 필요한 데이터를 검색하지 못했습니다.

공유 중

이 통계는 다른 AWS 계정 Amazon CloudFront 원본 액세스 ID (OAI) 또는 CloudFront 원본 액세스 제어 (OAC) 와 공유되거나 공유되지 않는 S3 버킷의 수를 나타냅니다.

- 외부 공유 — CloudFront OAI, CloudFront OAC 또는 동일한 조직에 속하지 않는 계정 중 하나 이상 또는 이들의 조합과 공유된 버킷의 수와 비율입니다.
- 내부 공유됨 - 동일한 조직 내 하나 이상의 계정과 공유된 버킷 수 및 백분율입니다. 이러한 버킷은 OAI 또는 OAC와 CloudFront 공유되지 않습니다.
- 공유되지 않음 — 다른 계정, CloudFront OAI 또는 OAC와 공유되지 않은 버킷의 수와 비율입니다. CloudFront

각 백분율을 계산하기 위해 Macie는 해당 버킷 수를 버킷 인벤토리의 총 버킷 수로 나눕니다.

버킷을 다른 AWS 계정사람과 공유할지 여부를 확인하기 위해 Macie는 각 버킷의 버킷 정책과 ACL을 분석합니다. 또한 조직은 Macie 초대를 통해 또는 Macie 초대를 통해 AWS Organizations 관련 계정 그룹으로 중앙에서 관리되는 Macie 계정 집합으로 정의됩니다. 버킷 공유에 대한 Amazon S3 옵션에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3의 ID 및 액세스 관리를 참조하세요.

> **Note**
>
> 경우에 따라, Macie는 버킷이 같은 조직에 속하지 않은 AWS 계정 와(과) 공유된다고 잘못 보고할 수 있습니다. 이는 Macie가 버킷 정책의 `Principal` 요소와 정책의 `Condition` 요소의 특정 AWS 글로벌 조건 컨텍스트 키 또는 Amazon S3 조건 키 간의 관계를 완전히 평가할 수 없는 경우 발생할 수 있습니다. 적용 가능한 조건 키는`aws:PrincipalAccount`,,,,`aws:PrincipalArn`,`aws:PrincipalOrgID`,,`aws:PrincipalOr` `aws:SourceVpc` `aws:SourceVpceaws:userid`, `s3:DataAccessPointAccount` 등입니다. `s3:DataAccessPointArn`
> 개별 버킷에 해당하는지 확인하려면 대시보드에서 외부 공유됨 통계를 선택합니다. 표시되는 표에서 각 버킷의 이름을 기록해 둡니다. 그런 다음, Amazon S3를 사용하여 각 버킷의 정책을 검토하고 공유 액세스 설정이 의도된 내용이고 안전한지를 결정합니다.

Macie는 버킷을 CloudFront OAI 또는 OAC와 공유할지 여부를 결정하기 위해 각 버킷의 버킷 정책을 분석합니다. CloudFront OAI 또는 OAC를 사용하면 사용자가 하나 이상의 지정된 배포를 통해 버킷의 객체에 액세스할 수 있습니다. CloudFront CloudFront OAI 및 OAC에 대한 자세한 내용은 Amazon 개발자 안내서의 Amazon S3 오리진에 대한 액세스 제한을 참조하십시오. CloudFront

경우에 따라 공유 중 섹션에 알 수 없음에 대한 값도 표시됩니다. 이러한 값이 나타나면 Macie는 지정된 버킷 수 및 백분율이 다른 계정, OAI 또는 OAC와 공유되는지 여부를 확인할 수 없었습니다. CloudFront CloudFront 예를 들어, 일시적인 문제나 버킷의 권한 설정으로 인해 Macie는 필요한 데이터를 검색하지 못했습니다. 또는 Macie는 버킷의 정책 또는 ACL을 완전히 평가할 수 없었습니다.

Amazon Macie를 통한 Amazon S3 보안 태세 분석

Amazon Simple Storage Service (Amazon S3) 데이터의 심층 분석을 수행하고 보안 상태를 평가할 수 있도록 Amazon Macie는 Macie를 사용하는 각 위치에서 S3 범용 버킷의 전체 인벤토리를 유지 관리합니다. AWS 리전 Macie가 이 인벤토리를 대신 관리하는 방법을 알아보려면 Macie가 Amazon S3 데이터 보안을 모니터링하는 방법(을)를 참조하세요. 귀하가 조직의 Macie 관리자인 경우 인벤토리에는 멤버 계정에서 소유한 S3 버킷의 인벤토리 데이터가 포함됩니다.

이 인벤토리를 사용하면 Amazon S3 데이터 자산을 검토하고 개별 S3 버킷에 적용되는 주요 보안 설정 및 지표에 대한 세부 정보 및 통계를 검토할 수 있습니다. 예를 들어, 각 버킷의 공개 액세스 및 암호화 설정에 대한 분석, 각 버킷의 민감한 데이터를 탐지하기 위해 Macie가 분석할 수 있는 객체의 크기와 개수에 액세스할 수 있습니다. 또한 버킷의 객체를 분석하기 위해 민감한 데이터 검색 작업을 구성했는지 아니면 민감한 데이터 자동 검색을 구성했는지도 확인할 수 있습니다. 있다면 인벤토리 데이터에 해당 분석이 가장 최근에 이루어진 시기가 표시됩니다. 민감한 데이터 자동 검색이 활성화된 경우 인벤토리를 사용하여 Macie가 지금까지 Amazon S3 데이터에 대해 수행한 자동 민감한 데이터 검색 활동의 결과를 검토할 수도 있습니다. 자세한 정보는 민감한 데이터 검색을 참조하세요.

Amazon Macie 콘솔의 S3 버킷 페이지를 사용하여 인벤토리 데이터를 찾아보고 필터링할 수 있습니다. Amazon Macie API의 DescribeBuckets작업을 사용하여 프로그래밍 방식으로 재고 데이터에 액세스할 수도 있습니다.

주제

- Amazon Macie를 사용하여 S3 버킷 인벤토리 검토
- Amazon Macie를 사용하여 S3 버킷 인벤토리 필터링하기

Amazon Macie를 사용하여 S3 버킷 인벤토리 검토

Amazon Macie 콘솔의 S3 버킷 페이지는 현재 AWS 리전에 있는 Amazon Simple Storage Service(S3) 데이터의 보안 및 개인정보 보호에 대한 자세한 인사이트를 제공합니다. 이 페이지에서는 리전 내 S3 범용 버킷의 전체 인벤토리를 검토 및 분석하고 개별 버킷에 대한 세부 정보 및 통계를 검토할 수 있습니다. 조직의 Macie 관리자인 경우 인벤토리에는 구성원 계정이 소유한 S3 버킷에 대한 세부 정보 및 통계가 포함됩니다.

S3 버킷 페이지에는 Macie가 가장 최근에 언제 사용자 계정의 Amazon S3에서 버킷 또는 객체 메타데이터를 검색했는지도 표시됩니다. 이 정보는 페이지 상단의 마지막 업데이트 필드에서 확인할 수 있습니다. 조직의 Macie 관리자인 경우, 이 필드는 Macie가 조직 계정의 데이터를 검색한 가장 빠른 날짜와 시간을 나타냅니다. 자세한 정보는 데이터 새로 고침을 참조하세요.

참고로 인벤토리 데이터와 통계에는 S3 디렉터리 버킷에 대한 데이터가 포함되지 않고 범용 버킷만 포함됩니다. Macie는 디렉터리 버킷을 모니터링하거나 분석하지 않습니다. 또한 대부분의 인벤토리 데이터는 Macie가 사용자 계정에서 액세스할 수 있는 버킷으로 제한됩니다. 버킷의 권한 설정으로 인해 Macie가 버킷 또는 버킷의 객체에 대한 정보를 검색할 수 없는 경우, Macie는 버킷에 대한 일부 정보만 제공할 수 있습니다. 특정 버킷의 경우, Macie는 버킷 인벤토리에 해당 버킷에 대한 경고 아이콘 (⚠) 과 메시지를 표시합니다. 버킷 세부 정보의 경우, Macie는 버킷을 소유한 AWS 계정 의 계정 ID, 버킷 이름, Amazon 리소스 이름(ARN), 생성 날짜, 리전, 매일 새로 고침 주기의 일부로 Macie가 가장 최근에 버킷과 버킷의 개체 메타데이터를 모두 검색한 날짜 등 필드와 데이터의 하위 집합만 표시합니다. 문제를 조사하려면 Amazon S3의 버킷 정책 및 권한 설정을 검토하십시오. 예를 들어 버킷에 제한적인 버킷 정책이 있을 수 있습니다. 자세한 정보는 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을 참조하세요.

프로그래밍 방식으로 재고 데이터에 액세스하고 쿼리하려는 경우 Amazon Macie API DescribeBuckets작업을 사용할 수 있습니다.

주제

- S3 버킷 인벤토리 검토
- S3 버킷의 세부 정보 검토

S3 버킷 인벤토리 검토

Amazon Macie 콘솔의 S3 버킷 페이지는 현재의 S3 범용 버킷에 대한 정보를 제공합니다. AWS 리전 이 페이지에는 인벤토리의 각 버킷에 대한 요약 정보가 표로 표시됩니다. 표를 정렬하고 필터링하여 보기를 사용자 지정할 수 있습니다. 표에서 버킷을 선택하면 세부 정보 패널에 해당 버킷에 대한 추가 정보가 표시됩니다. 여기에는 설정 및 메트릭에 대한 세부 정보 및 통계가 포함되어 버킷 데이터의 보안 및 개인정보 보호에 대한 인사이트를 제공받을 수 있습니다. 선택적으로 테이블의 데이터를 쉼표로 구분된 값(CSV) 파일로 내보낼 수 있습니다.

민감한 데이터 자동 검색이 활성화된 경우 대화형 히트 맵을 사용하여 인벤토리를 검토할 수도 있습니다. 이 맵은 Amazon S3 데이터 자산 전반의 데이터 민감도를 시각적으로 보여줍니다. Macie가 지금까지 수행한 자동화된 민감한 데이터 검색 활동의 결과를 캡처합니다. 이 맵에 대해 자세히 알아보려면, S3 버킷 맵을 사용한 데이터 민감도 시각화을 참조하십시오.

S3 버킷 인벤토리를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 S3 버킷을 선택합니다. S3 버킷 페이지에는 버킷 인벤토리가 표시됩니다. 페이지에 인벤토리의 대화형 지도가 표시되면 페이지 상단의 표 ( ) 를 선택하십시오. 그러면 Macie는 인벤토리의 버킷 수와 버킷 표를 표시합니다.

   민감한 데이터 자동 검색이 활성화된 경우 현재 자동 검색에서 제외된 버킷의 데이터는 기본 보기에 표시되지 않습니다. 이 데이터를 표시하려면 필터 상자 아래에 있는 자동 검색으로 모니터링됨 필터 토큰에서 X를 선택합니다.
3. 필요에 따라 페이지 상단에서 새로 고침 ( ) 을 선택하여 Amazon S3에서 최신 버킷 메타데이터를 검색할 수 있습니다.

   버킷 이름 옆에 정보 아이콘 ( ) 이 표시되면 이렇게 하는 것이 좋습니다. 정보 아이콘은 지난 24시간 동안 버킷이 생성되었음을 의미합니다. 아마도 Macie가 일일 새로 고침 주기의 일부로 Amazon S3에서 버킷과 객체 메타데이터를 마지막으로 검색한 이후일 것입니다.
4. S3 버킷 페이지에서 표를 사용하여 인벤토리의 각 버킷에 대한 정보의 하위 집합을 검토하세요.

   - 민감도 - 버킷의 현재 민감도 점수. 이 열은 민감한 데이터 자동 검색이 활성화된 경우에만 나타납니다. Macie가 정의하는 민감도 점수 범위에 대한 자세한 내용은 S3 버킷의 민감도 점수 섹션을 참조하세요.
   - 버킷 - 버킷의 이름
   - 계정 – 버킷을 소유한 AWS 계정 의 계정 ID.
   - 분류 가능한 객체는 Macie가 버킷에서 민감한 데이터를 탐지하기 위해 분석할 수 있는 총 객체 수입니다.
   - 분류 가능한 크기는 Macie가 버킷에서 민감한 데이터를 탐지하기 위해 분석할 수 있는 모든 객체의 총 스토리지 크기입니다.

     이 값은 압축 해제된 후 압축된 객체의 실제 크기를 반영하지 않습니다. 버킷에 버전 관리가 활성화된 경우, 이 값은 버킷에 있는 각 객체의 최신 버전의 스토리지 크기를 기준으로 합니다.
   - 작업별 모니터링 - 민감한 데이터 검색 작업이 버킷의 객체를 일별, 주별 또는 월별로 주기적으로 분석하도록 구성되어 있는지 여부를 나타냅니다.

이 필드의 값이 예이면 해당 버킷이 명시적으로 정기적인 작업에 포함되어 있거나 버킷이 지난 24시간 이내에 정기적인 작업 기준과 일치한 경우입니다. 또한 이러한 작업 중 하나 이상의 상태는 취소되지 않습니다. Macie는 이 데이터를 매일 업데이트합니다.

- 최근 작업 실행 - 버킷의 객체를 분석하도록 일회성 또는 주기적 중요 데이터 검색 작업을 구성한 경우 이 필드는 해당 작업 중 하나가 실행되기 시작한 가장 최근 날짜 및 시간을 나타냅니다. 그렇지 않으면 이 필드에 대시 (-) 가 표시됩니다.

앞의 데이터에서, 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식의 파일 이름 확장자를 가진 경우 분류할 수 있습니다. Macie를 사용하여 객체에서 민감한 데이터를 탐지할 수 있습니다. 자세한 정보는 지원하는 스토리지 클래스 및 형식을 참조하세요.

5. 표를 사용하여 인벤토리를 분석하려면, 다음 작업 중 하나를 수행합니다.

   - 특정 필드를 기준으로 테이블을 정렬하려면 해당 필드의 열 제목을 선택합니다. 정렬 순서를 변경하려면 열 제목을 다시 선택합니다.
   - 테이블을 필터링하고 필드에 특정 값이 있는 버킷만 표시하려면 필터 상자에 커서를 놓고 필드에 필터 조건을 추가합니다. 결과를 더 세분화하려면 추가 필드에 필터 조건을 추가합니다. 자세한 정보는 S3 버킷 인벤토리 필터링을 참조하세요.

6. 특정 버킷에 대한 세부 정보 및 통계를 검토하려면 테이블에서 버킷 이름을 선택하고 세부 정보 패널을 참조하세요.

> **Tip**
>
> 패널의 버킷 세부 정보 패널에서 여러 필드를 피벗하고 드릴다운
> 할 수 있습니다. 필드 값이 동일한 버킷을 표시하려면 필드에서
> 
> 를
> 선택합니다. 필드에 다른 값이 있는 버킷을 표시하려면 필드에서
> 
> 를
> 선택합니다.

7. 테이블의 데이터를 CSV 파일로 내보내려면 내보내려는 각 행의 확인란을 선택하거나 선택 항목의 열 제목의 확인란을 선택하여 모든 행을 선택합니다. 그런 다음 페이지 상단에서 CSV로 내보내기를 선택합니다. 테이블에서 최대 50,000개의 행을 내보낼 수 있습니다.

S3 버킷의 세부 정보 검토

Amazon Macie 콘솔에서는 S3 버킷 페이지의 세부 정보 패널을 사용하여 S3 버킷 인벤토리의 각 범용 버킷에 대한 통계 및 기타 정보를 검토할 수 있습니다. 여기에는 설정 및 메트릭에 대한 세부 정보 및 통계가 포함되어 버킷 데이터의 보안 및 개인정보 보호에 대한 인사이트를 제공받을 수 있습니다.

예를 들어, S3 버킷의 퍼블릭 액세스 설정의 세부 분석을 검토하고, 버킷이 객체를 복제하도록 구성되어 있는지 또는 다른 AWS 계정과 공유되는지 여부를 확인할 수 있습니다. 또한 버킷에서 민감한 데이터를 검사하도록 민감한 데이터 검색 작업이 구성되어 있는지도 확인할 수 있습니다. 있는 경우 가장 최근에 실행된 작업에 대한 세부 정보에 액세스하고, 해당 작업에서 생성된 조사 결과를 선택적으로 표시할 수 있습니다.

민감한 데이터 자동 검색이 활성화된 경우 세부 정보 패널을 사용하여 민감한 데이터 검색 통계 및 개별 S3 버킷에 대한 기타 정보를 검토할 수도 있습니다. 이 패널은 Macie가 지금까지 버킷에 대해 수행한 민감한 자동 데이터 검색 활동의 결과를 캡처합니다. 이러한 세부 정보에 대해 자세히 알아보려면, 개별 S3 버킷의 데이터 민감도 세부 정보 검토을 참조하십시오.

S3 버킷의 세부 정보를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 S3 버킷을 선택합니다. S3 버킷 페이지에는 버킷 인벤토리가 표시됩니다.

   민감한 데이터 자동 검색이 활성화된 경우 현재 자동 검색에서 제외된 버킷의 데이터는 기본 보기에 표시되지 않습니다. 이 데이터를 표시하려면 필터 상자 아래에 있는 자동 검색으로 모니터링됨 필터 토큰에서 X를 선택합니다.
3. 필요에 따라 페이지 상단에서 새로 고침 () 을 선택하여 Amazon S3에서 최신 버킷 메타데이터를 검색할 수 있습니다.
4. 세부 정보를 검토하려는 버킷을 선택합니다. 세부 정보 패널에는 버킷에 대한 통계 및 기타 정보가 표시됩니다.

세부 정보 패널에서 통계 및 정보는 다음과 같은 기본 섹션으로 구성되어 있습니다.

개요 | 객체 통계 | 서버 측 암호화 | 민감한 데이터 검색 | 퍼블릭 액세스 | 복제| 태그

각 섹션의 정보를 검토하면서, 선택적으로 특정 필드를 피벗하고 드릴다운할 수 있습니다. 필드 값이 동일한 버킷을 표시하려면 필드에서 를

선택합니다. 필드에 다른 값이 있는 버킷을 표시하려면 필드에서

를 선택합니다.

개요

이 섹션에서는 버킷 이름, 버킷 생성 시기, 버킷을 소유한 계정 ID 등 버킷에 대한 일반 정보를 제공합니다. AWS 계정 특히 최종 업데이트 필드에는 Macie가 Amazon S3에서 가장 최근에 버킷 또는 버킷 객체에 대한 메타데이터를 검색한 시기가 표시됩니다.

공유 액세스 필드는 버킷을 다른 사람과 공유하는지 AWS 계정, Amazon CloudFront 원본 액세스 ID (OAI) 또는 CloudFront 원본 액세스 제어 (OAC) 와 공유하는지를 나타냅니다.

- 외부 — 버킷은 CloudFront OAI, CloudFront OAC 또는 조직 외부 (소속이 아닌) 계정 중 하나 이상 또는 이들의 조합과 공유됩니다.
- 내부 - 버킷은 조직 내부(일부)에 있는 하나 이상의 계정과 공유됩니다. CloudFront OAI 또는 OAC와는 공유되지 않습니다.
- 공유되지 않음 — 버킷은 다른 계정, CloudFront OAI 또는 OAC와 공유되지 않습니다. CloudFront
- 알 수 없음 - Macie가 버킷의 공유된 접속 설정을 평가할 수 없었습니다.

버킷을 다른 AWS 계정사람과 공유하는지 여부를 확인하기 위해 Macie는 버킷의 버킷 정책 및 ACL (액세스 제어 목록) 을 분석합니다. 분석은 버킷 수준 설정으로 제한됩니다. 버킷에서 특정 객체를 공유하기 위한 객체 수준 설정은 반영되지 않습니다. 또한 조직은 Macie 초대를 통해 AWS Organizations 또는 Macie 초대를 통해 관련 계정 그룹으로 중앙에서 관리되는 Macie 계정 집합으로 정의됩니다. 버킷 공유를 위한 Amazon S3 옵션에 대해 알아보려면, Amazon Simple Storage Service 사용 설명서에서 Amazon S3의 ID 및 액세스 관리를 참조하십시오.

> **Note**
>
> 경우에 따라 Macie에서 버킷이 조직 외부(조직의 일부가 아닌) AWS 계정 와 공유되고 있다고 잘못 표시될 수 있습니다. 이는 Macie가 버킷 정책의 `Principal` 요소와 정책의 `Condition` 요소의 특정 AWS 글로벌 조건 컨텍스트 키 또는 Amazon S3 조건 키 간의 관계를 완전히 평가할 수 없는 경우 발생할 수 있습니다. 적용 가능한 조건 키는`aws:PrincipalAccount`,,,`aws:PrincipalArn`,`aws:PrincipalOrgID`,,`aws:PrincipalOrgPa` `aws:SourceIp` `aws:SourceVpc` `aws:SourceVpceaws:userid`, `s3:DataAccessPointAccount` 및 입니다. `s3:DataAccessPointArn` 버킷 정책을 검토하여 이러한 액세스가 의도적이고 안전한지 판단하는 것이 좋습니다.

Macie는 버킷을 CloudFront OAI 또는 OAC와 공유할지 여부를 결정하기 위해 버킷의 버킷 정책을 분석합니다. CloudFront OAI 또는 OAC를 사용하면 사용자가 하나 이상의 지정된 배포를 통해 버킷의 객체에 액세스할 수 있습니다. CloudFront CloudFront OAI 및 OAC에 대해 자세히 알아보려면 Amazon 개발자 안내서의 Amazon S3 오리진에 대한 액세스 제한을 참조하십시오. CloudFront

개요 섹션에는 최신 자동 검색 실행 필드도 포함되어 있습니다. 이 필드는 Macie가 민감한 데이터 자동 검색을 수행하는 동안 가장 최근에 버킷의 객체를 분석한 시기를 나타냅니다. 이 분석이 수행되지 않은 경우 이 필드에 대시 (-) 가 표시됩니다.

객체 통계

이 섹션에서는 버킷에 있는 객체의 (총 개수), 모든 객체의 총 스토리지 크기(총 스토리지 크기), 압축 (.gz, .gzip 또는 .zip) 파일인 모든 객체의 총 스토리지 크기(총 압축 크기)를 비롯하여 버킷에 있는 객체에 대한 정보를 확인할 수 있습니다. 이 섹션의 추가 통계를 통해 Macie가 버킷에서 민감한 데이터를 감지하기 위해 분석할 수 있는 데이터의 양을 평가할 수 있습니다.

최근에 버킷을 생성했거나 지난 24시간 동안 버킷 객체를 크게 변경한 경우, 선택적으로 새로 고침 ( ) 을 선택하여 버킷 객체에 대한 최신 메타데이터를 검색할 수 있습니다. Macie는 정보 아이콘 ( ) 을 표시하여 해당 여부를 판단하는 데 도움을 줍니다. 버킷에 저장된 객체가 30,000개 이하인 경우 새로 고침 옵션을 사용할 수 있습니다.

이 섹션의 통계를 검토할 때 다음 사항에 유의하십시오.

- 버킷에 대해 버전 관리가 활성화된 경우, 크기 값은 해당 버킷에 있는 각 객체의 최신 버전 스토리지 크기를 기준으로 합니다.
- 버킷에 압축된 객체가 저장되어 있는 경우, 크기 값은 압축을 푼 후의 해당 객체의 실제 크기를 반영하지 않습니다.
- 버킷의 객체 메타데이터를 새로 고침하면, Macie는 객체에 적용되는 암호화 통계를 일시적으로 알 수 없음으로 보고합니다. Macie는 24시간 이내에 버킷 및 객체 메타데이터를 다음 일일 새로 고침을 수행할 때 이러한 통계에 대한 데이터를 재평가하고 업데이트합니다.
- 기본적으로 객체 수와 크기 값에는 불완전한 멀티파트 업로드로 인해 버킷에 포함된 모든 객체 파트에 대한 데이터가 포함됩니다. 버킷의 객체 메타데이터를 새로 고침하면, Macie는 다시 계산된 값에서 객체 파트에 대한 데이터를 제외합니다. Macie가 버킷 및 객체 메타데이터의 다음 일일 새로 고침을 수행할 때(24시간 이내), Macie는 이러한 통계의 값을 다시 계산하여 업데이트하고 객체 파트에 대한 데이터를 다시 값에 포함합니다.

Macie는 민감한 데이터를 감지하기 위해 객체 부분을 분석할 수 없습니다. Amazon S3는 먼저 Macie가 분석할 수 있도록 부품을 하나 이상의 객체로 조립하는 작업을 완료해야 합니다. 수명 주기 규칙에 따라 파트를 자동으로 삭제하는 방법을 비롯하여 멀티파트 업로드 및 객체 파트에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 멀티파트 업로드를 사용한 객체 업로드 및 복사를 참조하세요. Amazon S3 Storage Lens에서 불완전한 멀티파트 업로드 지표를 참조하여 객체 부분이 포함된 버킷을 식별할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 스토리지 활동 및 사용량 평가를 참조하세요.

객체 통계는 다음과 같이 구성됩니다.

분류 가능한 객체

이 섹션에는 Macie가 민감한 데이터를 감지하기 위해 분석할 수 있는 총 객체 수와 해당 객체의 총 스토리지 크기가 표시됩니다. 이러한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하며 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가집니다. Macie를 사용하여 객체에서 민감한 데이터를 탐지할 수 있습니다. 자세한 정보는 지원하는 스토리지 클래스 및 형식을 참조하세요.

분류할 수 없는 객체

이 섹션에는 Macie가 민감한 데이터를 감지하기 위해 분석할 수 없는 총 객체 수와 해당 객체의 총 스토리지 크기가 표시됩니다. 이러한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하지 않거나 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자가 없습니다.

분류할 수 없는 객체: 스토리지 클래스

이 섹션에서는 지원되는 Amazon S3 스토리지 클래스를 사용하지 않기 때문에 Macie에서 분석할 수 없는 객체의 수와 스토리지 크기에 대한 세부 분석을 제공합니다.

분류할 수 없는 객체: 파일 유형

이 섹션에서는 객체에 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장명이 없기 때문에 Macie가 분석할 수 없는 객체의 수와 스토리지 크기에 대한 세부 분석을 제공합니다.

암호화 유형별 객체

이 섹션에서는 Amazon S3가 지원하는 각 암호화 유형을 사용하는 객체 수를 분석합니다.

- 고객 제공 — 고객 제공 키로 암호화된 객체 수입니다. 이러한 객체는 SSE-C 암호화를 사용합니다.
- AWS KMS 관리형 — 고객 관리 키 AWS 관리형 키 또는 고객 관리 키로 암호화된 객체 수입니다. AWS KMS key이러한 객체는 DSSE-KMS 또는 SSE-KMS 암호화를 사용합니다.

- Amazon S3 관리 - Amazon S3 관리 키로 암호화된 객체 수입니다. 이러한 객체는 SSE-S3 암호화를 사용합니다.
- 암호화 안 함 - 암호화되지 않았거나 클라이언트 측 암호화를 사용하는 객체 수입니다. (객체가 클라이언트측 암호화를 사용하여 암호화된 경우 Macie는 해당 객체의 암호화 데이터에 액세스하여 이를 보고할 수 없습니다.)
- 알 수 없음 - Macie에 현재 암호화 메타데이터가 없는 객체 수입니다. 이는 일반적으로 최근에 버킷 객체의 메타데이터를 수동으로 새로 고침한 경우에 발생합니다. Macie는 24시간 이내에 버킷 및 객체 메타데이터의 다음 일일 새로 고침을 수행할 때 암호화 통계를 업데이트합니다.

지원되는 각 암호화 유형에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 암호화를 통한 데이터 보호를 참조하십시오.

서버 측 암호화

이 섹션에서는 버킷의 서버 측 암호화 설정에 대한 인사이트를 제공합니다.

버킷 정책에 필요한 암호화 필드에는 버킷에 객체를 추가할 때 버킷의 정책에서 객체의 서버 측 암호화를 요구하는지 여부가 표시됩니다.

- 아니요 - 버킷에 버킷 정책이 없거나 버킷 정책에 새 객체의 서버 측 암호화가 필요하지 않습니다. 버킷 정책이 있는 경우 PutObject요청에 유효한 서버 측 암호화 헤더를 포함할 필요가 없습니다.
- 예 - 버킷 정책에 따라 새 객체의 서버 측 암호화가 필요합니다. 버킷에 대한 PutObject 요청에는 유효한 서버 측 암호화 헤더가 포함되어야 합니다. 그렇지 않으면 Amazon S3은 요청을 거부합니다.
- 알 수 없음 - Macie에서 버킷 정책을 평가하여 새 객체의 서버 측 암호화가 필요한지 여부를 결정할 수 없습니다.

이 평가에서 유효한 서버 측 암호화 헤더는 다음과 같습니다: 값이 `AES256` 또는 `aws:kms`인 경우`x-amz-server-side-encryption`, 값이 `AES256`인 경우 `x-amz-server-side-encryption-customer-algorithm`입니다. 버킷 정책을 사용하여 새 객체의 서버 측 암호화를 요구하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 서버 측 암호화로 데이터 보호를 참조하십시오.

기본 암호화 필드는 버킷에 추가되는 객체에 기본적으로 적용하도록 버킷이 구성된 서버 측 암호화 알고리즘을 나타냅니다.

- AES256 - 버킷의 기본 암호화 설정은 Amazon S3 관리 키를 사용하여 새 객체를 암호화하도록 구성되어 있습니다. 새 객체는 SSE-S3 암호화를 사용하여 자동으로 암호화됩니다.

- aws:kms — 버킷의 기본 암호화 설정은 A 또는 고객 관리 키를 사용하여 새 객체를 암호화하도록 구성되어 있습니다. AWS KMS key AWS 관리형 키 새 객체는 SSE-KMS 암호화를 사용하여 자동으로 암호화됩니다. AWS KMS key필드에는 사용된 키의 Amazon 리소스 이름 (ARN) 또는 고유 식별자 (키 ID) 가 표시됩니다.
- aws:kms:dsse — 버킷의 기본 암호화 설정은 A 또는 고객 관리 키를 사용하여 새 객체를 암호화하도록 구성되어 있습니다. AWS KMS key AWS 관리형 키 새 객체는 DSSE-KMS 암호화를 사용하여 자동으로 암호화됩니다. AWS KMS key필드에는 사용된 키의 ARN 또는 키 ID가 표시됩니다.
- 없음 - 버킷의 기본 암호화 설정이 새 객체에 대한 서버 측 암호화 동작을 지정하지 않습니다.

2023년 1월 5일부터 Amazon S3가 Amazon S3 관리형 키를 사용한 서버 측 암호화 (SSE-S3) 를 버킷에 추가되는 객체의 암호화의 기본 수준으로 자동 적용합니다. 선택적으로 키를 사용한 서버 측 암호화 (SSE-KMS) 또는 AWS KMS 키를 사용한 이중 레이어 서버 측 암호화 (DSSE-KMS) 를 대신 사용하도록 버킷의 기본 암호화 설정을 구성할 수 있습니다. AWS KMS 기본 암호화 설정 및 옵션에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 S3 버킷의 기본 서버 측 암호화 동작 설정을 참조하세요.

민감한 데이터 검색

이 섹션은 민감한 데이터 검색 작업이 버킷의 객체를 매일, 매주 또는 매월 정기적으로 분석하도록 구성되어 있는지 여부를 나타냅니다. 작업별 활성 모니터링 필드 값이 예이면, 해당 버킷이 명시적으로 정기적인 작업에 포함되어 있거나 버킷이 지난 24시간 이내에 정기적인 작업 기준과 일치한 경우입니다. 또한 이러한 작업 중 하나 이상의 상태는 취소되지 않습니다. Macie는 이 데이터를 매일 업데이트합니다.

버킷을 검사하도록 모든 유형의 민감한 데이터 검색 작업(정기 작업 또는 일회성 작업)이 구성된 경우, 최신 작업 필드에는 가장 최근에 실행을 시작한 작업의 고유 식별자가 제공됩니다. 최근 작업 실행 필드에는 해당 작업이 실행되기 시작한 시간이 표시됩니다.

> **Tip**
>
> 작업에서 생성된 모든 민감한 데이터 결과를 표시하려면 최근 작업(Latest job) 필드에서 링크를 선택합니다. 작업 세부 정보 패널이 나타나면, 패널 상단에서 결과 표시를 선택한 다음 조사 결과 보기를 선택합니다.

공개 액세스(Public access)

이 섹션은 버킷에 퍼블릭 액세스가 가능한지를 나타냅니다. 또한 해당 여부를 결정하는 다양한 계정 및 버킷 수준 설정에 대한 분석도 제공합니다. 유효 권한 필드에는 이러한 설정의 누적 결과가 표시됩니다.

- 비공개 - 버킷에 공개적으로 액세스할 수 없습니다.
- 공개 - 버킷에 공개적으로 액세스할 수 있습니다.
- 알 수 없음 - Macie가 버킷의 퍼블릭 액세스 설정을 평가할 수 없었습니다.

참고로 이 데이터는 계정 및 버킷 수준 설정으로 제한됩니다. 버킷의 특정 객체에 대한 퍼블릭 액세스를 허용하는 객체 수준 설정은 반영되지 않습니다.

버킷 및 버킷 데이터에 대한 퍼블릭 액세스를 관리하기 위한 Amazon S3 설정에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서에서 Amazon S3의 ID 및 액세스 관리와 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단하기를 참조하십시오.

복제

이 섹션에서 복제됨 필드에는 버킷이 다른 버킷에 객체를 복제하도록 구성되어 있는지 여부가 표시됩니다. 이 필드의 값이 '예'이면, 버킷에 대해 하나 이상의 복제 규칙이 구성되고 활성화된 것입니다. 그런 다음 이 섹션에는 대상 버킷을 소유한 각 사용자의 계정 ID도 나열됩니다. AWS 계정

Replicated externally 필드는 조직 외부 (일부가 아닌) 의 버킷에 객체를 복제하도록 버킷을 구성했는지 여부를 나타냅니다. AWS 계정 조직은 Macie 초대를 통해 또는 Macie 초대를 통해 관련 계정 그룹으로 중앙에서 관리되는 Macie 계정 집합입니다. AWS Organizations 이 필드의 값이 Yes이면 해당 버킷에 대해 복제 규칙이 구성되고 활성화되며 외부 소유의 버킷에 객체를 복제하도록 규칙이 구성됩니다. AWS 계정

> **Note**
>
> 특정 상황에서 Macie는 버킷이 외부 소유의 버킷에 객체를 복제하도록 구성되어 있다고 잘못 표시할 수 있습니다. AWS 계정이는 Macie가 일일 새로 고침 주기의 일부로 Amazon S3에서 버킷 및 객체 메타데이터를 검색한 후 이전 24시간 동안 다른 AWS 리전 에서 대상 버킷을 생성한 경우 발생할 수 있습니다.
> Macie를 사용하여 문제를 조사하려면, 새로 고침
> ()
> 을 선택하여 Amazon S3에서 최신 버킷 메타데이터를 검색합니다. 그런 다음 이 섹션의 계정

ID 목록을 검토합니다. 더 심층적인 조사를 위해, Amazon S3를 사용하여 버킷의 복제 규칙을 검토합니다.

버킷 객체 복제를 위한 Amazon S3 옵션 및 설정에 대해 알아보려면, Amazon Simple Storage Service 사용 설명서에서 객체 복제하기를 참조하십시오.

Tags

태그가 버킷과 연결된 경우, 이 섹션이 패널에 표시되고 해당 태그가 나열됩니다. 태그는 S3 버킷을 비롯한 특정 유형의 AWS 리소스에 정의하여 할당할 수 있는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다.

버킷 태그 지정에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 비용 할당 S3 버킷 태그 사용을 참조하십시오.

Amazon Macie를 사용하여 S3 버킷 인벤토리 필터링하기

특정 특성을 가진 버킷을 식별하고 집중하기 위해 Amazon Macie 콘솔과 Amazon Macie API를 사용하여 프로그래밍 방식으로 제출하는 쿼리에서 S3 버킷 인벤토리를 필터링할 수 있습니다. 필터를 생성할 때는 특정 버킷 속성을 사용하여 보기 또는 쿼리 결과에서 버킷을 포함하거나 제외하는 기준을 정의합니다. 버킷 속성은 버킷의 특정 메타데이터를 저장하는 필드입니다.

Macie에서 필터는 하나 이상의 조건으로 구성됩니다. 기준이라고도 하는 각 조건은 다음과 같은 세 부분으로 구성됩니다.

- 버킷 이름, 태그 키 또는 작업에 정의됨과 같은 속성 기반 필드.
- equals 또는 not equals와 같은 연산자입니다.
- 하나 이상의 값입니다. 값의 유형과 개수는 선택한 필드와 연산자에 따라 달라집니다.

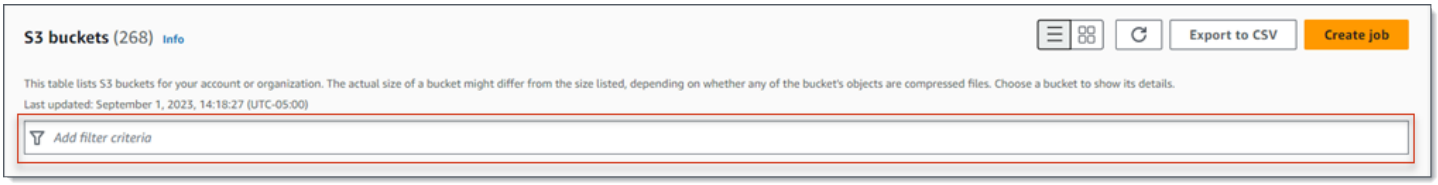
필터 조건을 정의하고 적용하는 방법은 Amazon Macie 콘솔을 사용하는지 아니면 Amazon Macie API를 사용하는지에 따라 다릅니다.

주제

- Amazon Macie 콘솔에서 인벤토리 필터링
- Amazon Macie API를 사용하여 프로그래밍 방식으로 인벤토리를 필터링합니다.

Amazon Macie 콘솔에서 인벤토리 필터링

Amazon Macie 콘솔을 사용하여 S3 버킷 인벤토리를 필터링하는 경우, Macie는 개별 조건에 대한 필드, 연산자, 값을 선택하는 데 도움이 되는 옵션을 제공합니다. 다음 이미지와 같이 S3 버킷 페이지의 필터 상자를 사용하여 이러한 옵션에 액세스할 수 있습니다.

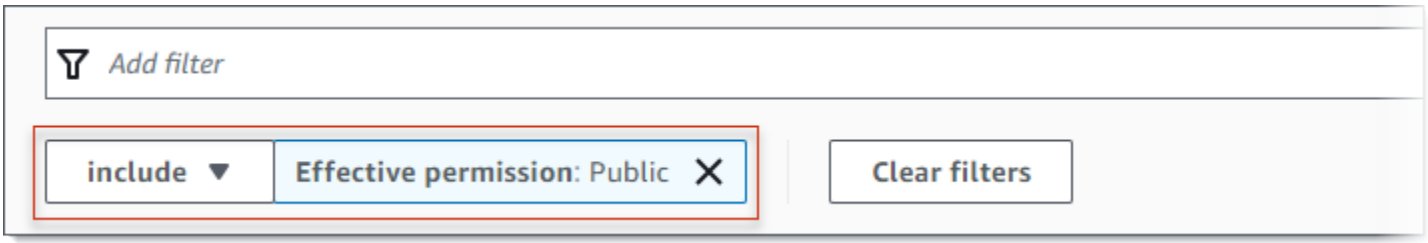


필터 상자에 커서를 놓으면 Macie는 필터 조건에서 사용할 수 있는 필드 목록을 표시합니다. 필드는 논리적 범주별로 구성되어 있습니다. 예를 들어, 일반 필드 카테고리에는 S3 버킷에 대한 일반 정보를 저장하는 필드가 포함됩니다. 퍼블릭 액세스 카테고리에는 버킷에 적용할 수 있는 다양한 유형의 퍼블릭 액세스 설정에 대한 데이터를 저장하는 필드가 있습니다. 필드는 각 범주 내에서 알파벳순으로 정렬됩니다.

조건을 추가하려면 먼저 목록에서 필드를 선택합니다. 필드를 찾으려면 전체 목록을 찾아보거나 필드 이름의 일부를 입력하여 필드 목록의 범위를 좁힙니다.

선택한 필드에 따라 Macie는 다른 옵션을 표시합니다. 옵션은 선택한 필드의 유형과 특성을 반영합니다. 예를 들어 공유 액세스 필드를 선택하면 Macie는 선택할 수 있는 값 목록을 표시합니다. 버킷 이름 필드를 선택하면 Macie는 S3 버킷의 이름을 입력할 수 있는 텍스트 상자를 표시합니다. 어떤 필드를 선택하든 Macie는 필드에 필요한 설정이 포함된 조건을 추가하는 단계를 안내합니다.

조건을 추가한 후 Macie는 조건에 대한 기준을 적용하고, 다음 이미지와 같이 필터 상자 아래에 있는 필터 토큰에 조건을 표시합니다.



이 예제에서는 공개적으로 액세스할 수 있는 모든 버킷을 포함하고 다른 모든 버킷은 제외하도록 조건을 구성합니다. 유효한 권한 필드의 값이 공개와 같은 버킷을 반환합니다.

조건을 추가하면 Macie는 조건을 적용하여 필터 상자 아래에 표시합니다. 여러 개의 조건을 추가하면 Macie는 AND 로직을 사용하여 조건을 결합하고 필터 기준을 평가합니다. 즉, S3 버킷은 필터의 모든 조건과 일치하는 경우에만 필터 기준과 일치합니다. 언제든지 필터 상자 아래 영역을 참조하여 어떤 기준을 적용했는지 확인할 수 있습니다.

콘솔을 사용하여 인벤토리 필터링하기

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 S3 버킷을 선택합니다. S3 버킷 페이지에는 버킷 인벤토리가 표시됩니다.

   민감한 데이터 자동 검색이 활성화된 경우 현재 자동 검색에서 제외된 버킷의 데이터는 기본 보기에 표시되지 않습니다. 조직의 Macie 관리자인 경우 현재 자동 검색이 비활성화된 계정의 데이터도 표시되지 않습니다. 이 데이터를 표시하려면 필터 상자 아래에 있는 자동 검색으로 모니터링됨 필터 토큰에서 X를 선택합니다.
3. 필요에 따라 페이지 상단에서 새로 고침
   ()
   을 선택하여 Amazon S3에서 최신 버킷 메타데이터를 검색할 수 있습니다.
4. 필터 상자에 커서를 놓고 조건에 사용할 필드를 선택합니다.
5. 다음 팁을 염두에 두고 필드에 적합한 유형의 값을 선택하거나 입력하세요.

   날짜, 시간, 시간 범위

   날짜 및 시간의 경우 시작 및 종료 상자를 사용하여 포함된 시간 범위를 정의합니다.

   - 고정된 시간 범위를 정의하려면, 시작 및 종료 상자를 사용하여 범위의 첫 번째 날짜 및 시간과 마지막 날짜 및 시간을 각각 지정합니다.
   - 특정 날짜와 시간에 시작하여 현재 시간에 끝나는 상대적인 시간 범위를 정의하려면, 시작 상자에 시작 날짜와 시간을 입력하고 종료 상자의 모든 텍스트를 삭제합니다.
   - 특정 날짜 및 시간에 종료되는 상대적 시간 범위를 정의하려면, 종료 상자에 종료 날짜 및 시간을 입력하고 시작 상자의 모든 텍스트를 삭제합니다.

   참고로 시간 값은 24시간 표기법을 사용합니다. 날짜 선택기를 사용하여 날짜를 선택하는 경우, 시작 및 종료 상자에 직접 텍스트를 입력하여 값을 조정할 수 있습니다.

   숫자 및 숫자 범위

   숫자 값의 경우 시작 및 종료 상자를 사용하여 포함된 숫자 범위를 정의하는 정수를 입력합니다.

   - 고정된 숫자 범위를 정의하려면 시작 및 종료 상자를 사용하여 범위의 가장 낮은 숫자와 가장 큰 숫자를 각각 지정합니다.

- 특정 값 하나로 제한되는 고정 숫자 범위를 정의하려면 시작 및 종료 상자 모두에 값을 입력합니다. 예를 들어 정확히 15개의 객체를 저장하는 S3 버킷만 포함하려면 From 및 To **15** 상자에 입력합니다.
- 특정 숫자에서 시작하는 상대적 숫자 범위를 정의하려면 시작 상자에 숫자를 입력하고 종료 상자에는 텍스트를 입력하지 마세요.
- 특정 숫자에서 끝나는 상대적 숫자 범위를 정의하려면 종료 상자에 숫자를 입력하고 시작 상자에는 텍스트를 입력하지 마세요.

텍스트(문자열) 값

이 유형의 값에는 필드에 대해 완전하고 유효한 값을 입력합니다. 값은 대소문자를 구분합니다.

이 유형의 값에는 부분 값이나 와일드카드 문자를 사용할 수 없다는 점에 유의하세요. 유일한 예외는 버킷 이름 필드입니다. 해당 필드에는 전체 버킷 이름 대신 접두사를 지정할 수 있습니다. 예를 들어 이름이 my-S3로 시작하는 모든 S3 버킷을 찾으려면 버킷 이름 필드에 필터 값으로 **`my-S3`**를 입력합니다. **`My-s3`** 또는 **`my*`**와 같은 다른 값을 입력하면 Macie는 버킷을 반환하지 않습니다.

6. 필드에 값을 모두 추가했으면 적용을 선택합니다. Macie는 필터 기준을 적용하고 필터 상자 아래의 필터 토큰에 조건을 표시합니다.
7. 추가할 각 추가 조건에 대해 4~6단계를 반복합니다.
8. 조건을 제거하려면 조건에 대한 필터 토큰에서 X를 선택합니다.
9. 조건을 변경하려면 조건에 대한 필터 토큰에서 X를 선택하여 조건을 제거합니다. 그런 다음 4~6단계를 반복하여 올바른 설정이 포함된 조건을 추가합니다.

Amazon Macie API를 사용하여 프로그래밍 방식으로 인벤토리를 필터링합니다.

프로그래밍 방식으로 S3 버킷 인벤토리를 필터링하려면 Amazon Macie API DescribeBuckets작업을 사용하여 제출하는 쿼리에 필터 기준을 지정하십시오. 이 작업은 객체의 배열을 반환합니다. 각 객체에는 필터 기준과 일치하는 버킷에 대한 통계 데이터 및 기타 정보가 들어 있습니다.

쿼리에서 필터 기준을 지정하려면 요청에 필터 조건 맵을 포함합니다. 각 조건에 대해 필드, 연산자, 하나 이상의 필드 값을 지정합니다. 값의 유형과 개수는 선택한 필드와 연산자에 따라 달라집니다. 조건에서 사용할 수 있는 필드, 연산자 및 값 유형에 대한 자세한 내용은 Amazon Macie API 참조의 Amazon S3 데이터 소스 섹션을 참조하세요.

다음 예제는 AWS Command Line Interface (AWS CLI)를 사용하여 제출하는 쿼리에 필터 기준을 지정하는 방법을 보여줍니다. 최신 버전의 다른 AWS 명령줄 도구 또는 AWS SDK를 사용하거나 HTTPS 요청을 Macie에 직접 전송하여 이 작업을 수행할 수도 있습니다. AWS 도구 및 SDK에 대한 자세한 내용은 빌드할 도구를 참조하십시오. AWS

예

- 예제 1: 버킷 이름으로 버킷 찾기
- 예 2: 공개적으로 액세스할 수 있는 버킷 찾기
- 예제 3: 암호화되지 않은 객체를 저장하는 버킷 찾기
- 예 4: 작업에서 모니터링되지 않는 버킷 찾기
- 예 5: 데이터를 외부 계정에 복제하는 버킷 찾기
- 예제 6: 여러 기준에 따라 버킷 찾기

이 예제에서는 describe-buckets 명령을 사용합니다. 예제가 성공적으로 실행되면 Macie는 `buckets` 배열을 반환합니다. 배열에는 현재 상태이고 필터 AWS 리전 기준과 일치하는 각 버킷의 객체가 포함됩니다. 이 출력의 예를 보려면 다음 섹션을 펼치세요.

`buckets` 배열의 예

이 예제에서 `buckets` 배열은 쿼리에 지정된 필터 기준과 일치하는 두 버킷에 대한 세부 정보를 제공합니다.

```
{
    "buckets": [
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "FALSE",
            "automatedDiscoveryMonitoringStatus": "MONITORED",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "bucketCreatedAt": "2020-05-18T19:54:00+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET1",
            "classifiableObjectCount": 13,
            "classifiableSizeInBytes": 1592088,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "TRUE",
                "lastJobId": "08c81dc4a2f3377fae45c9ddaexample",
                "lastJobRunTime": "2024-05-26T14:55:30.270000+00:00"
            },
```

```
            "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
            "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
            "objectCount": 13,
            "objectCountByEncryptionType": {
                "customerManaged": 0,
                "kmsManaged": 2,
                "s3Managed": 7,
                "unencrypted": 4,
                "unknown": 0
            },
            "publicAccess": {
                "effectivePermission": "NOT_PUBLIC",
                "permissionConfiguration": {
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        }
                    },
                    "bucketLevelPermissions": {
                        "accessControlList": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        },
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        },
                        "bucketPolicy": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        }
                    }
                }
            },
            "region": "us-east-1",
            "replicationDetails": {
                "replicated": false,
                "replicatedExternally": false,
                "replicationAccounts": []
```

```
            },
            "sensitivityScore": 78,
            "serverSideEncryption": {
                "kmsMasterKeyId": null,
                "type": "NONE"
            },
            "sharedAccess": "NOT_SHARED",
            "sizeInBytes": 4549746,
            "sizeInBytesCompressed": 0,
            "tags": [
                {
                    "key": "Division",
                    "value": "HR"
                },
                {
                    "key": "Team",
                    "value": "Recruiting"
                }
            ],
            "unclassifiableObjectCount": {
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "versioning": true
        },
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "TRUE",
            "automatedDiscoveryMonitoringStatus": "MONITORED",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
            "bucketCreatedAt": "2020-11-25T18:24:38+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET2",
            "classifiableObjectCount": 8,
            "classifiableSizeInBytes": 133810,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "FALSE",
                "lastJobId": "188d4f6044d621771ef7d65f2example",
```

```
            "lastJobRunTime": "2024-04-09T19:37:11.511000+00:00"
        },
        "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
        "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
        "objectCount": 8,
        "objectCountByEncryptionType": {
            "customerManaged": 0,
            "kmsManaged": 0,
            "s3Managed": 8,
            "unencrypted": 0,
            "unknown": 0
        },
        "publicAccess": {
            "effectivePermission": "NOT_PUBLIC",
            "permissionConfiguration": {
                "accountLevelPermissions": {
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    }
                },
                "bucketLevelPermissions": {
                    "accessControlList": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    }
                }
            }
        },
        "region": "us-east-1",
        "replicationDetails": {
            "replicated": false,
```

```
                "replicatedExternally": false,
                "replicationAccounts": []
            },
            "sensitivityScore": 95,
            "serverSideEncryption": {
                "kmsMasterKeyId": null,
                "type": "AES256"
            },
            "sharedAccess": "EXTERNAL",
            "sizeInBytes": 175978,
            "sizeInBytesCompressed": 0,
            "tags": [
                {
                    "key": "Division",
                    "value": "HR"
                },
                {
                    "key": "Team",
                    "value": "Recruiting"
                }
            ],
            "unclassifiableObjectCount": {
                "fileType": 3,
                "storageClass": 0,
                "total": 3
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 2999826,
                "storageClass": 0,
                "total": 2999826
            },
            "versioning": true
        }
    ]
}
```


필터 기준과 일치하는 버킷이 없는 경우 Macie는 빈 `buckets` 배열을 반환합니다.


```
{
    "buckets": []
}
```

예제 1: 버킷 이름으로 버킷 찾기

이 예제에서는 describe-buckets 명령을 사용하여 이름이 my-S3로 시작하고 현재 상태인 모든 버킷의 메타데이터를 쿼리합니다. AWS 리전

Linux, macOS, Unix의 경우:

```
$ aws macie2 describe-buckets --criteria '{"bucketName":{"prefix":"my-S3"}}'
```

Microsoft Windows의 경우:

```
C:\> aws macie2 describe-buckets --criteria={\"bucketName\":{\"prefix\":\"my-S3\"}}
```

위치:

- *bucketName*은 버킷 이름 필드의 JSON 이름을 지정합니다.
- *prefix*는 접두사 연산자를 지정합니다.
- *my-S3*는 버킷 이름 필드의 값입니다.

예 2: 공개적으로 액세스할 수 있는 버킷 찾기

이 예제에서는 describe-buckets 명령을 사용하여 현재 AWS 리전 상태이고 권한 설정의 조합에 따라 공개적으로 액세스할 수 있는 버킷의 메타데이터를 쿼리합니다.

Linux, macOS, Unix의 경우:

```
$ aws macie2 describe-buckets --criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]}}'
```

Microsoft Windows의 경우:

```
C:\> aws macie2 describe-buckets --criteria={\"publicAccess.effectivePermission\":
{\"eq\":[\"PUBLIC\"]}}
```

위치:

- *publicAccess.effectivePermission*은 유효한 권한 필드의 JSON 이름을 지정합니다.
- *eq*는 등호 연산자를 지정합니다.

- *PUBLIC*은 유효한 권한 필드의 열거형 값입니다.

예제 3: 암호화되지 않은 객체를 저장하는 버킷 찾기

이 예제에서는 describe-buckets 명령을 사용하여 현재 버킷에 있고 암호화되지 않은 객체를 저장하는 버킷의 메타데이터를 쿼리합니다. AWS 리전

Linux, macOS, Unix의 경우:

```
$ aws macie2 describe-buckets --criteria '{"objectCountByEncryptionType.unencrypted":
{"gte":1}}'
```

Microsoft Windows의 경우:

```
C:\> aws macie2 describe-buckets --
criteria={\"objectCountByEncryptionType.unencrypted\":{\"gte\":1}}
```

위치:

- *objectCountByEncryptionType.uncrypted# ### # # ### JSON* 이름을 지정합니다.
- *gte*는 크거나 같음 연산자를 지정합니다.
- *1*은 암호화 없음 필드의 포괄적이고 상대적 숫자 범위 중 가장 낮은 값입니다.

예 4: 작업에서 모니터링되지 않는 버킷 찾기

이 예제에서는 describe-buckets 명령을 사용하여 최신 상태이고 정기적인 민감한 데이터 검색 AWS 리전 작업과 연결되지 않은 버킷의 메타데이터를 쿼리합니다.

Linux, macOS, Unix의 경우:

```
$ aws macie2 describe-buckets --criteria '{"jobDetails.isMonitoredByJob":{"eq":
["FALSE"]}}'
```

Microsoft Windows의 경우:

```
C:\> aws macie2 describe-buckets --criteria={\"jobDetails.isMonitoredByJob\":{\"eq\":
[\"FALSE\"]}}
```

위치:

- *## ## ##. isMonitoredByJob#* 작업별 능동 모니터링 필드의 JSON 이름을 지정합니다.
- *eq*는 등호 연산자를 지정합니다.
- *FALSE*는 작업을 통해 적극적으로 모니터링된 필드의 열거형 값입니다.

예 5: 데이터를 외부 계정에 복제하는 버킷 찾기

이 예제에서는 describe-buckets 명령을 사용하여 현재 AWS 리전 상태에 있고 조직의 일부가 아닌 AWS 계정 곳으로 객체를 복제하도록 구성된 버킷의 메타데이터를 쿼리합니다.

Linux, macOS, Unix의 경우:

```
$ aws macie2 describe-buckets --criteria '{"replicationDetails.replicatedExternally":
{"eq":["true"]}}'
```

Microsoft Windows의 경우:

```
C:\> aws macie2 describe-buckets --
criteria={\"replicationDetails.replicatedExternally\":{\"eq\":[\"true\"]}}
```

위치:

- *replicationDetails.replicatedExternally*는 외부에서 복제 필드의 JSON 이름을 지정합니다.
- *eq*는 등호 연산자를 지정합니다.
- *true*는 외부에서 복제 필드의 부울 값을 지정합니다.

예제 6: 여러 기준에 따라 버킷 찾기

이 예제에서는 describe-buckets 명령을 사용하여 현재 상태이고 권한 설정 조합을 기반으로 공개적으로 액세스할 수 AWS 리전 있고, 암호화되지 않은 객체를 저장하고, 주기적인 민감한 데이터 검색 작업과 관련이 없는 버킷의 메타데이터를 쿼리합니다.

Linux, macOS 또는 Unix의 경우, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws macie2 describe-buckets \
```

```
--criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]},"objectCountByEncryptionType.unencrypted":
{"gte":1},"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

Microsoft Windows의 경우 캐럿(^) 줄 연속 문자를 사용하여 가독성을 개선합니다.

```
C:\> aws macie2 describe-buckets ^
--criteria={\"publicAccess.effectivePermission\":{\"eq\":
[\"PUBLIC\"]},\"objectCountByEncryptionType.unencrypted\":{\"gte\":1},
\"jobDetails.isMonitoredByJob\":{\"eq\":[\"FALSE\"]}}
```

위치:

- *publicAccess.effectivePermission*은 유효한 권한 필드의 JSON 이름을 지정합니다.
  - *eq*는 등호 연산자를 지정합니다.
  - *PUBLIC*은 유효한 권한 필드의 열거형 값입니다.
- *objectCountByEncryptionType.uncrypted# ### #* 함 필드의 JSON 이름을 지정하고 다음을 수행합니다.
  - *gte*는 크거나 같음 연산자를 지정합니다.
  - *1*은 암호화 없음 필드의 포괄적이고 상대적 숫자 범위 중 가장 낮은 값입니다.
- *## ## ##. isMonitoredByJob#* 작업별 능동적 모니터링 필드의 JSON 이름을 지정하고 다음을 수행합니다.
  - *eq*는 등호 연산자를 지정합니다.
  - *FALSE*는 작업을 통해 적극적으로 모니터링됨 필드의 열거형 값입니다.

Amazon Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용

Amazon Macie를 활성화하면 Macie는 사용자를 대신하여 AWS 계정 Amazon Simple Storage Service (Amazon S3) 및 기타 서비스를 호출하는 데 필요한 권한을 Macie에게 부여하는 서비스 연결 역할을 생성합니다. AWS 서비스 서비스 연결 역할을 사용하면 사용자 대신 작업을 완료하기 위해 서비스에 권한을 수동으로 추가할 필요가 AWS 서비스 없으므로 설정 프로세스가 간소화됩니다. 이러한 유형의 역할에 대해 자세히 알아보려면 AWS Identity and Access Management 사용 설명서의 서비스 연결 역할 사용을 참조하세요.

Macie 서비스 연결 역할(AWSServiceRoleForAmazonMacie)에 대한 권한 정책을 통해 Macie는 S3 버킷 및 객체에 대한 정보 검색, 버킷의 객체 검색 등의 작업을 수행할 수 있습니다. 조직의 Macie 관리

자인 경우, 정책에 따라 Macie가 조직 내 멤버 계정에 대해 사용자를 대신하여 이러한 작업을 수행할 수도 있습니다.

Macie는 이러한 권한을 사용하여 다음과 같은 태스크를 수행합니다.

- S3 범용 버킷의 인벤토리를 생성하고 유지 관리합니다.
- 버킷과 버킷의 객체에 대한 통계 및 기타 데이터를 제공합니다
- 보안 및 액세스 제어를 위한 버킷을 모니터링하고 평가합니다
- 버킷의 객체를 분석하여 민감한 데이터를 감지합니다

대부분의 경우, Macie는 이러한 태스크를 수행하는 데 필요한 권한을 가지고 있습니다. 그러나 S3 버킷에 제한적인 버킷 정책이 있는 경우, 정책으로 인해 Macie가 이러한 태스크의 일부 또는 전부를 수행하지 못할 수 있습니다.

버킷 정책은 보안 주체 AWS Identity and Access Management (사용자, 계정, 서비스 또는 기타 엔티티) 가 S3 버킷에서 수행할 수 있는 작업과 보안 주체가 해당 작업을 수행할 수 있는 조건을 지정하는 리소스 기반 (IAM) 정책입니다. 작업 및 조건은 버킷 수준 작업(예: 버킷 정보 검색)과 객체 수준 작업(예: 버킷에서 객체 검색)에 적용될 수 있습니다.

버킷 정책은 일반적으로 명시적 `Allow` 또는 `Deny` 명령문 및 조건을 사용하여 액세스를 허용하거나 제한합니다. 예를 들어 버킷에 액세스하는데 특정 소스 IP 주소, Amazon Virtual Private Cloud(VPC) 엔드포인트 또는 VPC를 사용하지 않는 한, 버킷 액세스를 거부하는 `Allow` 또는 `Deny` 명령문이 버킷 정책에 포함될 수 있습니다. Amazon S3의 버킷 정책에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 정책 및 사용자 정책 사용 및 Amazon S3가 요청을 승인하는 방법을 참조하십시오.

버킷 정책에서 명시적인 `Allow` 명령문을 사용하는 경우, 정책은 Macie가 버킷과 버킷의 객체에 대한 정보를 검색하거나 버킷에서 객체를 검색하는 것을 막지 않습니다. 이는 Macie 서비스 연결 역할에 대한 권한 정책의 `Allow` 명령문이 이러한 권한을 부여하기 때문입니다.

그러나 버킷 정책에서 하나 이상의 조건이 포함된 명시적 `Deny` 명령문을 사용하는 경우, Macie는 버킷 또는 버킷의 객체에 대한 정보를 검색하거나 버킷의 객체를 검색하지 못할 수 있습니다. 예를 들어 버킷 정책에서 특정 IP 주소를 제외한 모든 소스에서의 액세스를 명시적으로 거부하는 경우, 민감한 데이터 검색 작업을 실행할 때 Macie는 버킷의 객체를 분석할 수 없습니다. 이는 제한적 버킷 정책이 Macie 서비스 연결 역할에 대한 권한 정책의 `Allow` 명령문보다 우선하기 때문입니다.

Macie가 제한적인 버킷 정책이 있는 S3 버킷에 액세스할 수 있도록 하기 위해 Macie 서비스 연결 역할(`AWSServiceRoleForAmazonMacie`)에 대한 조건을 버킷 정책에 추가할 수 있습니다. 이 조

건은 Macie 서비스 연결 역할이 정책의 Deny 제한과 일치하지 않도록 제외할 수 있습니다. 이는 aws:PrincipalArn 전역 조건 키와 Macie 서비스 연결 역할의 Amazon 리소스 이름(ARN)을 사용하여 수행할 수 있습니다.

다음 절차는 이 프로세스를 안내하고 예제를 제공합니다.

Macie 서비스 연결 역할을 버킷 정책에 추가하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/s3/ 에서 Amazon S3 콘솔을 엽니다.
2. 탐색 창에서 버킷을 선택합니다.
3. Macie의 액세스를 허용할 S3 버킷을 선택합니다.
4. 권한(Permissions) 탭의 버킷 정책(Bucket policy)에서 편집(Edit)을 선택합니다.
5. 버킷 정책 편집기에서 액세스를 제한하고 Macie가 버킷 또는 버킷의 객체에 액세스하는 것을 막는 각 Deny 명령문을 식별합니다.
6. 각 Deny 명령문에 aws:PrincipalArn 전역 조건 컨텍스트 키를 사용하고 AWS 계정에 Macie 서비스 연결 역할의 ARN을 지정하는 조건을 추가합니다.

   조건 키의 값은 arn:aws:iam::*123456789012*:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie이어야 하며, 여기서 *123456789012*는 AWS 계정의 계정 ID입니다.

이를 버킷 정책에 추가하는 위치는 정책에 현재 포함되어 있는 구조, 요소 및 조건에 따라 달라집니다. 지원되는 구조 및 요소에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서의 Amazon S3의 정책 및 권한 섹션을 참조하세요.

다음은 명시적 Deny 명령문을 사용하여 DOC-EXAMPLE-BUCKET이라는 S3 버킷에 대한 액세스를 제한하는 버킷 정책의 예입니다. 현재 정책에서는 ID가 vpce-1a2b3c4d인 VPC 엔드포인트에서만 버킷에 액세스할 수 있습니다. 및 Macie에서의 액세스를 포함하여 다른 모든 VPC 엔드포인트에서의 액세스는 거부됩니다 AWS Management Console .

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115example",
   "Statement": [
      {
         "Sid": "Access from specific VPCE only",
         "Effect": "Deny",
```

```
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            }
         }
      }
   ]
}
```

이 정책을 변경하고 Macie가 S3 버킷과 버킷의 객체에 액세스할 수 있도록 하기 위해 `StringNotLike` 조건 연산자와 `aws:PrincipalArn` 전역 조건 컨텍스트 키를 사용하는 조건을 추가할 수 있습니다. 이 추가 조건은 Macie 서비스 연결 역할이 Deny 제한과 일치하지 않도록 제외합니다.

```
{
   "Version": "2012-10-17",
   "Id":" Policy1415115example ",
   "Statement": [
      {
         "Sid": "Access from specific VPCE and Macie only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            },
            "StringNotLike": {
               "aws:PrincipalArn": "arn:aws:iam::123456789012:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
            }
         }
      }
```

```
    ]
}
```

위 예제에서 `StringNotLike` 조건 연산자는 `aws:PrincipalArn` 조건 컨텍스트 키를 사용하여 Macie 서비스 연결 역할의 ARN을 지정합니다. 여기서,

- `123456789012`Macie를 사용하여 버킷과 버킷의 객체에 대한 정보를 검색하고 버킷에서 객체를 검색할 수 AWS 계정 있는 계정 ID입니다.
- `macie.amazonaws.com`은(는) Macie 서비스 주체의 식별자입니다.
- `AWSServiceRoleForAmazonMacie`은(는) Macie 서비스 연결 역할의 이름입니다.

정책에서 이미 `StringNotLike` 연산자를 사용하고 있기 때문에 `StringNotEquals` 연산자를 사용했습니다. 정책에서는 `StringNotEquals` 연산자를 한 번만 사용할 수 있습니다.

Amazon S3 리소스 액세스 관리에 대한 추가 정책 예시와 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3의 ID 및 액세스 관리를 참조하세요.

Amazon Macie를 통한 민감한 데이터 검색

Amazon Macie를 사용하면 Amazon Simple Storage Service(S3) 데이터 에스테이트에서 민감한 데이터의 검색, 로깅 및 보고를 자동화할 수 있습니다. 이 작업은 두 가지 방법으로 수행할 수 있습니다. 하나는 민감한 데이터 자동 검색을 수행하도록 Macie를 구성하는 것이고 다른 하나는 민감한 데이터 검색 작업을 만들고 실행하는 것입니다.

민감한 데이터 자동 검색

민감한 데이터 자동 검색을 통해 Amazon S3 데이터 자산에서 민감한 데이터가 어디에 있는지 폭넓게 파악할 수 있게 해줍니다. 이 옵션을 사용하여 Macie는 매일 S3 버킷 인벤토리를 평가하고 샘플링 기법을 사용하여 버킷의 대표적인 S3 객체를 식별하고 선택합니다. 그런 다음 Macie는 선택한 객체를 검색 및 분석하여 민감한 데이터가 있는지 검사합니다. 자세한 정보는 민감한 데이터 자동 검색 수행을 참조하세요.

민감한 데이터 검색 작업

민감한 데이터 검색 작업은 심층적이고 표적화된 분석을 제공합니다. 이 옵션을 사용하여 선택한 특정 S3 버킷 또는 특정 기준과 일치하는 버킷 등 분석의 범위와 깊이를 정의합니다. 또한 S3 객체의 속성에서 파생되는 사용자 지정 기준과 같은 옵션을 선택하여 분석 범위를 좁힐 수 있습니다. 또한 온디맨드 분석 및 평가의 경우 한 번만 실행하도록 작업을 구성하거나 정기적인 분석, 평가 및 모니터링의 경우 반복적으로 실행하도록 구성할 수 있습니다. 자세한 정보는 민감한 데이터 검색 작업 실행을 참조하세요.

민감한 데이터 자동 검색 또는 민감한 데이터 검색 작업 중 하나를 사용하면 Macie가 제공하는 관리형 데이터 식별자, 사용자가 정의한 사용자 지정 데이터 식별자 또는 이 둘의 조합을 사용하여 S3 객체를 분석할 수 있습니다. 허용 목록을 사용하여 분석을 세밀하게 조정할 수도 있습니다.

관리형 데이터 식별자

각 관리형 데이터 식별자는 신용카드 번호, AWS 비밀 액세스 키 또는 특정 국가 또는 리전의 여권 번호와 같은 특정 유형의 민감한 데이터를 탐지하도록 설계된 기본 기준 및 기술입니다. 이를 통해 여러 유형의 보안 인증 데이터, 금융 정보 및 개인 식별 정보(PII)를 포함하여 많은 국가 및 리전에 대해 증가하는 대규모 민감한 데이터 유형의 목록을 감지할 수 있습니다. 자세한 정보는 관리형 데이터 식별자 사용을 참조하세요.

사용자 지정 데이터 식별자

사용자 지정 데이터 식별자는 민감한 데이터를 감지하기 위해 사용자 지정 기준을 정의합니다. 각 사용자 지정 데이터 식별자는 일치시킬 텍스트 패턴을 정의하고 선택적으로 문자 시퀀스와 결과를

세분화하는 근접성 규칙을 정의하는 정규 표현식(regex)을 지정합니다. 특정 시나리오, 지적 재산 또는 독점 데이터(예: 직원 ID, 고객 계정 번호 또는 내부 데이터 분류)를 반영하는 민감한 데이터를 감지하는 데 사용할 수 있습니다. 자세한 정보는 사용자 지정 데이터 식별자 빌드을 참조하세요.

허용 목록

Macie에서 허용 목록은 S3 객체에서 무시할 텍스트 또는 텍스트 패턴을 지정합니다. 일반적으로 특정 시나리오나 환경에 대한 민감한 데이터(예: 조직의 공개 이름이나 전화 번호 또는 조직에서 테스트에 사용하는 샘플 데이터)는 예외입니다. Macie는 허용 목록에서 입력이나 패턴과 일치하는 텍스트를 찾으면 텍스트가 관리형 데이터 식별자 또는 사용자 지정 데이터 식별자의 기준과 일치하더라도 Macie는 해당 텍스트 발생을 보고하지 않습니다. 자세한 정보는 허용 목록을 사용하여 민감한 데이터 예외사항 정의을 참조하세요.

Macie가 S3 객체를 분석할 때, Macie는 Amazon S3에서 객체의 최신 버전을 검색한 다음 민감한 데이터에 대한 객체의 콘텐츠를 검사합니다. Macie는 다음이 참일 경우 객체를 분석할 수 있습니다.

- 객체는 지원되는 파일 또는 스토리지 형식을 사용하며 지원되는 스토리지 클래스를 사용하는 S3 범용 버킷에 저장됩니다. 자세한 정보는 지원하는 스토리지 클래스 및 형식을 참조하세요.
- 객체가 암호화된 경우 Macie에서 액세스할 수 있고 사용할 수 있는 키로 해당 암호화됩니다. 자세한 정보는 암호화된 S3 객체 분석을 참조하세요.
- 객체가 제한적인 버킷 정책이 적용되는 버킷에 저장되는 경우, 정책은 Macie가 버킷의 객체에 액세스할 수 있도록 허용합니다. 자세한 정보는 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을 참조하세요.

데이터 보안 및 개인 정보 보호 요구 사항을 충족하고 규정 준수를 유지할 수 있도록 Macie는 발견한 민감한 데이터와 수행하는 분석(민감한 데이터 조사 결과 및 민감한 데이터 검색 결과)의 기록을 생성합니다. 민감한 데이터 조사 결과는 Macie가 S3 객체에서 발견한 민감한 데이터에 대한 상세 보고서입니다. 민감한 데이터 검색 결과는 객체 분석에 대한 세부 정보를 기록하는 레코드입니다. 각 레코드 유형은 표준화된 스키마를 따르므로 필요에 따라 다른 애플리케이션, 서비스 및 시스템을 사용하여 쿼리, 모니터링 및 처리하는 데 도움이 됩니다.

> **Tip**
>
> Macie는 Amazon S3에 최적화되어 있지만, 이를 사용하여 현재 다른 곳에 저장하고 있는 리소스에서 민감한 데이터를 검색할 수 있습니다. 데이터를 Amazon S3로 임시 또는 영구적으로 이동하여 이 작업을 수행할 수 있습니다. 예를 들어 Amazon 관계형 데이터베이스 서비스 또는 Amazon Aurora 스냅샷을 Apache Parquet 형식으로 Amazon S3로 내보낼 수 있습니다. 또는

Amazon DynamoDB 표를 Amazon S3로 내보냅니다. 그런 다음 Amazon S3의 데이터를 분석하는 작업을 생성할 수 있습니다.

주제

Amazon Macie에서 관리형 데이터 식별자 사용

Amazon Macie는 기계 학습 및 패턴 일치를 비롯한 다양한 기준과 기술을 사용하여 Amazon Simple Storage Service (S3)의 중요한 데이터를 탐지합니다. 총칭하여 관리형 데이터 식별자라고 하는 이러한 기준 및 기술은 여러 유형의 보안 인증 정보 데이터, 금융 정보, 개인 건강 정보(PHI) 및 개인 식별 정보(PII)를 포함하여 점점 증가하는 중요한 데이터 유형 목록을 많은 국가 및 리전에서 탐지할 수 있습니다. 각 관리형 데이터 식별자는 신용카드 번호, AWS 비밀 액세스 키 또는 특정 국가 또는 리전의 여권 번호와 같은 특정 유형의 중요한 데이터를 탐지하도록 설계되었습니다.

Amazon SNS는 관리형 데이터 식별자를 사용하여 다음과 같은 중요한 데이터 범주를 탐지할 수 있습니다.

- 프라이빗 키 또는AWS 보안 액세스 키와 같은 보안 인증 정보입니다.
- 금융 정보: 신용 카드 번호, 은행 계좌 번호와 같은 금융 데이터
- 개인정보: 건강 보험 및 의료 식별 번호와 같은 PHI와 운전면허증 번호 및 여권 번호와 같은 PII

Macie는 각 범주 내에서 여러 유형의 중요한 데이터를 탐지할 수 있습니다. 이 섹션의 항목에서는 각 유형과 이를 탐지하기 위한 관련 요구 사항을 나열하고 설명합니다. 각 유형에 대해 데이터를 탐지하도록 설계된 관리되는 데이터 식별자의 고유 식별자(ID)도 나타냅니다. 민감한 데이터 검색 작업을 만들거나 민감한 데이터 자동 검색 설정을 구성할 때 이러한 ID를 사용하여 Macie가 S3 객체를 분석할 때 사용할 관리형 데이터 식별자를 지정할 수 있습니다.

작업에 권장하는 관리형 데이터 식별자 목록은 민감한 데이터 검색 작업에 권장되는 관리형 데이터 식별자을(를) 참조하세요. 민감한 데이터 자동 검색에 권장하는 기본적으로 사용되는 관리형 데이터 식별자 목록은 민감한 데이터 자동 검색을 위한 기본 설정을 참조하십시오.

주제

- Amazon Macie의 관리형 데이터 식별자에 대한 키워드 요구 사항
- 빠른 참조: Amazon Macie 관리형 데이터 식별자
- 상세 참조: Amazon Macie 관리형 데이터 식별자

Amazon Macie의 관리형 데이터 식별자에 대한 키워드 요구 사항

관리형 데이터 식별자를 사용하여 특정 유형의 민감한 데이터를 탐지하기 위해 Amazon Macie는 데이터 근처에 키워드가 있어야 합니다. 특정 유형의 데이터에 해당하는 경우 이 섹션의 후속 항목에서 해당 데이터에 대한 키워드 요구 사항을 나타냅니다.

키워드가 특정 유형의 데이터와 인접해야 하는 경우 키워드는 일반적으로 데이터로부터 30자 이내(포함) 이내여야 합니다. 추가 근접성 요구 사항은 Amazon Simple Storage Service(S3) 객체의 스토리지 형식에 따라 달라집니다.

정형 열 기반 데이터

열 기반 데이터의 경우 키워드는 동일한 값의 일부이거나 값을 저장하는 열 또는 필드의 이름에 포함되어야 합니다. Microsoft Excel 통합 문서, CSV 파일 및 TSV 파일의 경우에도 마찬가지입니다.

예를 들어 필드 값에 SSN과 미국 사회보장번호(SSN) 구문을 사용하는 9자리 숫자가 모두 포함된 경우 Macie는 필드에서 SSN을 감지할 수 있습니다. 마찬가지로 열 이름에 SSN이 포함된 경우 Macie는 열의 각 SSN을 감지할 수 있습니다. Macie는 해당 열의 값을 키워드 SSN과 가까운 위치에 있는 것으로 취급합니다.

정형 레코드 기반 데이터

레코드 기반 데이터의 경우 키워드는 값이 같거나 값을 저장하는 필드 또는 배열의 경로에 있는 요소 이름에 포함되거나 요소 이름에 포함되어야 합니다. 이는 Apache Avro 객체 컨테이너, Apache Parquet 파일, JSON 파일 및 JSON 행 파일에 해당합니다.

예를 들어 필드 값에 보안 인증 정보와 AWS 비밀 액세스 키 구문을 사용하는 문자 시퀀스가 모두 포함되어 있는 경우 Macie는 필드에서 키를 감지할 수 있습니다. 마찬가지로 필드 경로가 `$.credentials.aws.key`인 경우 Macie는 해당 필드에서 AWS 비밀 액세스 키를 탐지할 수 있습니다. Macie는 필드의 값을 키워드 보안 인증 정보과 가까운 위치에 있는 것으로 취급합니다.

비정형 데이터

CSV, JSON, JSON 라인 및 TSV 파일을 제외한 Adobe 휴대용 문서 형식 파일, Microsoft Word 문서, 이메일 메시지 및 바이너리가 아닌 텍스트 파일에 대한 추가 근접성 요구 사항은 없습니다. 키워드는 일반적으로 데이터에서 30자 이내(포함) 이내여야 합니다. 여기에는 이러한 유형의 파일에 있는 모든 정형 데이터(예: 표)가 포함됩니다.

키워드는 대/소문자를 구분하지 않습니다 또한 키워드에 공백이 포함된 경우 Macie는 공백을 포함하지 않거나 공백 대신 밑줄(_) 또는 하이픈(-)이 포함된 유사 키워드를 자동으로 찾습니다. 경우에 따라 Macie는 키워드의 일반적인 변형을 해결하기 위해 키워드를 확장하거나 축약하기도 합니다.

키워드가 어떻게 컨텍스트를 제공하고 Macie가 특정 유형의 민감한 데이터를 감지하는 데 도움이 되는지 알아보려면 다음 동영상을 시청하세요. Amazon Macie가 키워드를 사용하여 민감한 데이터를 검색하는 방법.

빠른 참조: Amazon Macie 관리형 데이터 식별자

Amazon Macie에서 관리형 데이터 식별자는 특정 유형의 민감한 데이터 (예: 특정 국가 또는 지역의 신용 카드 번호, AWS 보안 액세스 키 또는 여권 번호) 를 탐지하도록 설계된 기본 제공 기준 및 기술 세트입니다. 이 식별자를 통해 여러 유형의 보안 인증 데이터, 금융 정보, 개인 건강 정보(PHI), 개인 식별 정보(PII)를 포함하여 많은 국가 및 리전에 대해 증가하는 대규모 민감한 데이터 유형의 목록을 감지할 수 있습니다.

다음 테이블에는 현재 Macie가 제공하는 모든 관리형 데이터 식별자가 민감한 데이터 유형별로 정리되어 있습니다. 각 유형에 대한 다음 정보를 제공합니다.

- 민감한 데이터 범주 - 다음을 포함하는 민감한 데이터의 일반 범주를 지정합니다. 여기에는 프라이빗 키와 같은 보안 인증 정보 데이터의 경우 보안 인증 정보, 신용 카드 번호 및 은행 계좌 번호와 같은 금융 데이터의 경우 금융 정보, 건강 보험 및 의료 식별 번호와 같은 개인 의료 정보의 경우 개인 정보: PHI, 운전면허증과 여권 번호와 같은 개인 식별 정보의 경우 개인 정보: PII입니다.
- 관리형 데이터 식별자 ID - 데이터를 감지하도록 설계된 하나 이상의 관리형 데이터 식별자의 고유 식별자(ID)를 지정합니다. 민감한 데이터 검색 작업을 만들거나 민감한 데이터 자동 검색 설정을 구성할 때 이러한 ID를 사용하여 Macie가 데이터를 분석할 때 사용할 관리형 데이터 식별자를 지정할 수 있습니다. 작업에 권장하는 관리형 데이터 식별자 목록은 민감한 데이터 검색 작업에 권장되는 관리형 데이터 식별자을(를) 참조하세요. 민감한 데이터 자동 검색에 권장하는 관리형 데이터 식별자 목록은 민감한 데이터 자동 검색을 위한 기본 설정을(를) 참조하세요.

- 키워드 필수 - 감지를 위해 데이터에 근접한 키워드가 필요한지 여부를 지정합니다. Macie가 데이터를 분석할 때 키워드를 사용하는 방법에 대한 자세한 내용은 키워드 요구 사항을(를) 참조하세요.
- 국가 및 리전 - 해당 관리형 데이터 식별자가 어느 국가 또는 리전을 대상으로 설계되었는지 지정합니다. 관리형 데이터 식별자가 특정 국가 또는 리전을 대상으로 설계되지 않은 경우 이 값은 모두 선택입니다.

특정 유형의 민감한 데이터에 대한 관리형 데이터 식별자에 대한 추가 세부 정보를 검토하려면 유형을 선택하세요.

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
AWS 비밀 액세스 키	보안 인증 정보	AWS_CREDENTIALS	예	모두
은행 계좌 번호	금융 정보	BANK_ACCOUNT_NUMBER(캐나다와 미국 모두)	예	캐나다, 미국
기본 은행 계좌 번호 (BBAN)	금융 정보	국가 또는 리전에 따라 다름: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	예	프랑스, 독일, 이탈리아, 스페인, 영국
생년월일	개인 정보: PII	DATE_OF_BIRTH	예	모두
신용 카드 유효 기간	금융 정보	CREDIT_CARD_EXPIRATION	예	모두
신용 카드 마그네틱 스트립 데이터	금융 정보	CREDIT_CARD_MAGNETIC_STRIPE	예	모두

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
신용 카드 번호	금융 정보	CREDIT_CARD_NUMBER(키워드에 근접한 신용 카드 번호의 경우), CREDIT_CARD_NUMBER_(NO_KEYWORD)(키워드에 근접하지 않은 신용 카드 번호의 경우)	다양	모두
신용 카드 인증 코드	금융 정보	CREDIT_CARD_SECURITY_CODE	예	모두

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
운전면허증 식별 번호	개인 정보: PII	국가 또는 리전에 따라 다름: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	예	호주, 오스트리아, 벨기에, 불가리아, 캐나다, 크로아티아, 사이프러스, 체코 공화국, 덴마크, 에스토니아, 핀란드, 프랑스, 독일, 그리스, 헝가리, 인도, 아일랜드, 이탈리아, 라트비아, 리투아니아, 룩셈부르크, 몰타, 네덜란드, 폴란드, 포르투갈, 루마니아, 슬로바키아, 슬로베니아, 스페인, 스웨덴, 영국, 미국

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		
마약단속국(DEA) 등록 번호	개인 정보: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	예	미국
선거인단 번호	개인 정보: PII	UK_ELECTORAL_ROLL_NUMBER	예	영국
전체 이름	개인 정보: PII	NAME	아니요	임의(이름에 라틴 문자 집합이 사용된 경우)
위성 항법 시스템(GPS) 좌표	개인 정보: PII	LATITUDE_LONGITUDE	예	임의, 좌표가 영어 키워드와 가까운 경우
Google Cloud API 키	보안 인증 정보	GCP_API_KEY	예	모두
건강 보험 청구 번호(HICN)	개인 정보: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	예	미국

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
건강 보험 또는 의료 식별 번호	개인 정보: PHI	국가 또는 리전에 따라 다름: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	예	캐나다, EU, 핀란드, 프랑스, 영국, 미국
Healthcare Common Procedure Coding System(HCPCS) 코드	개인 정보: PHI	USA_HEALTHCARE_PROCEDURE_CODE	예	미국
HTTP Basic Authorization 헤더	보안 인증 정보	HTTP_BASIC_AUTH_HEADER	아니요	모두
HTTP 쿠키	개인 정보: PII	HTTP_COOKIE	아니요	모두

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
국제 은행 계좌 번호 (IBAN)	금융 정보	국가 또는 리전에 따라 다름: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER,	아니요	알바니아, 안도라, 보스니아 헤르체고비나, 브라질, 불가리아, 코스타리카, 크로아티아, 키프로스, 체코, 덴마크, 도미니카공화국, 이집트, 에스토니아, 페로 제도, 핀란드, 프랑스, 조지아, 독일, 그리스, 그린란드, 헝가리, 아이슬란드, 아일랜드, 이탈리아, 요르단, 코소보, 리히텐슈타인, 리투아니아, 몰타, 모리타니, 모리셔스, 모나코, 몬테네그로, 네덜

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
		JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRAT		란드, 북마케도니아, 폴란드, 포르투갈, 산마리노, 세네갈, 세르비아, 슬로바키아, 슬로베니아, 스페인, 스웨덴, 스위스, 동티모르, 튀니지, 튀르키예, 영국, 우크라이나, 아랍에미리트, 버진아일랜드(영국령)

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
		ES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER(영국령 버진 아일랜드의 경우)		
JSON Web Token(JWT)	보안 인증 정보	JSON_WEB_TOKEN	아니요	모두
우편 주소	개인 정보: PII	ADDRESS, BRAZIL_CEP_CODE(브라질 우편 번호용)	다양	호주, 브라질, 캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국
국가 의약품 코드(NDC)	개인 정보: PHI	USA_NATIONAL_DRUG_CODE	예	미국
국적 식별 번호	개인 정보: PII	국가 또는 리전에 따라 다름: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	예	브라질, 프랑스, 독일, 인도, 이탈리아, 스페인
National Insurance Number(NINO)	개인 정보: PII	UK_NATIONAL_INSURANCE_NUMBER	예	영국

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
국가 공급자 식별자(NPI)	개인 정보: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	예	미국
OpenSSH 프라이빗 키	보안 인증 정보	OPENSSH_PRIVATE_KEY	아니요	모두
여권 번호	개인 정보: PII	국가 또는 리전에 따라 다름: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	예	캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국
영주권 번호	개인 정보: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	예	캐나다
PGP 프라이빗 키	보안 인증 정보	PGP_PRIVATE_KEY	아니요	모두
전화번호	개인 정보: PII	국가 또는 리전에 따라 다름: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	다양	브라질, 캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
퍼블릭 키 암호화 표준(PKCS) 프라이빗 키	보안 인증 정보	PKCS	아니요	모두
PuTTY 프라이빗 키	보안 인증 정보	PUTTY_PRIVATE_KEY	아니요	모두
Social Insurance Number(SIN)	개인 정보: PII	CANADA_SOCIAL_INSURANCE_NUMBER	예	캐나다
사회 보장 번호(SSN)	개인 정보: PII	국가 또는 리전에 따라 다름: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	예	스페인, 미국
the section called “Stripe API 키”	보안 인증 정보	STRIPE_CREDENTIALS	아니요	모두

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
납세자 식별 번호 또는 참조 번호	개인 정보: PII	국가 또는 리전에 따라 다름: AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	예	호주, 브라질, 프랑스, 독일, 인도, 이탈리아, 스페인, 영국, 미국
고유 디바이스 식별자(UDI)	개인 정보: PHI	MEDICAL_DEVICE_UDI	예	미국
차량 식별 번호(VIN)	개인 정보: PII	VEHICLE_IDENTIFICATION_NUMBER	예	모두 선택, VIN이 영어, 프랑스어, 독일어, 리투아니아어, 폴란드어, 포르투갈어, 루마니아어 또는 스페인어 중 하나의 키워드에 근접한 경우

상세 참조: Amazon Macie 관리형 데이터 식별자

Amazon Macie의 관리형 데이터 식별자는 특정 유형의 민감한 데이터를 감지하도록 설계된 기본 제공 기준 및 기술입니다. 이 기술은 보안 인증 정보 데이터, 금융 데이터, 개인 식별 정보 및 보호 대상 건강 정보를 포함하여 많은 국가 및 리전에 대한 대규모 중요한 데이터 유형 목록을 감지할 수 있습니다. 각 관리형 데이터 식별자는 신용카드 번호, AWS 비밀 액세스 키 또는 특정 국가 또는 리전의 여권 번호와 같은 특정 유형의 중요한 데이터를 탐지하도록 설계되었습니다.

Macie는 관리형 데이터 식별자를 사용하여 여러 범주의 민감한 데이터를 감지할 수 있습니다. Macie는 각 범주 내에서 여러 유형의 중요한 데이터를 탐지할 수 있습니다. 이 섹션의 주제에서는 각 유형과 이를 탐지하기 위한 관련 요구 사항을 나열하고 설명합니다. 특정 유형의 민감한 데이터에 대한 관리형 데이터 식별자에 대한 자세한 내용은 범주별로 주제를 찾아볼 수 있습니다.

- 자격 증명 - 개인 키 및 AWS 비밀 액세스 키와 같은 자격 증명 데이터용.
- 금융 정보 - 신용 카드 번호, 은행 계좌 번호와 같은 금융 데이터
- 개인 정보: PHI - 건강 보험 및 의료 식별 번호와 같은 개인 건강 정보(PHI)
- 개인 정보: PII - 운전면허증 번호 및 여권 번호와 같은 개인 식별 정보(PII)

또는 다음 표에서 특정 유형의 민감한 데이터를 선택할 수 있습니다. 이 표에는 현재 Macie가 제공하는 모든 관리형 데이터 식별자가 민감한 데이터 유형별로 정리되어 있습니다. 이 표에는 각 유형을 감지하기 위한 관련 요구 사항도 요약되어 있습니다.

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
AWS 비밀 액세스 키	보안 인증 정보	AWS_CREDENTIALS	예	모두
은행 계좌 번호	금융 정보	BANK_ACCOUNT_NUMBER(캐나다와 미국 모두)	예	캐나다, 미국
기본 은행 계좌 번호 (BBAN)	금융 정보	국가 또는 리전에 따라 다름: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BAN	예	프랑스, 독일, 이탈리아, 스페인, 영국

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
		K_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER		
생년월일	개인 정보: PII	DATE_OF_BIRTH	예	모두
신용 카드 유효 기간	금융 정보	CREDIT_CARD_EXPIRATION	예	모두
신용 카드 마그네틱 스트립 데이터	금융 정보	CREDIT_CARD_MAGNETIC_STRIPE	예	모두
신용 카드 번호	금융 정보	CREDIT_CARD_NUMBER(키워드에 근접한 신용 카드 번호의 경우), CREDIT_CARD_NUMBER_(NO_KEYWORD)(키워드에 근접하지 않은 신용 카드 번호의 경우)	다양	모두
신용 카드 인증 코드	금융 정보	CREDIT_CARD_SECURITY_CODE	예	모두

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
운전면허증 식별 번호	개인 정보: PII	국가 또는 리전에 따라 다름: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	예	호주, 오스트리아, 벨기에, 불가리아, 캐나다, 크로아티아, 사이프러스, 체코 공화국, 덴마크, 에스토니아, 핀란드, 프랑스, 독일, 그리스, 헝가리, 인도, 아일랜드, 이탈리아, 라트비아, 리투아니아, 룩셈부르크, 몰타, 네덜란드, 폴란드, 포르투갈, 루마니아, 슬로바키아, 슬로베니아, 스페인, 스웨덴, 영국, 미국

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		
마약단속국(DEA) 등록 번호	개인 정보: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	예	미국
선거인단 번호	개인 정보: PII	UK_ELECTORAL_ROLL_NUMBER	예	영국
전체 이름	개인 정보: PII	NAME	아니요	임의(이름에 라틴 문자 집합이 사용된 경우)
위성 항법 시스템(GPS) 좌표	개인 정보: PII	LATITUDE_LONGITUDE	예	임의, 좌표가 영어 키워드와 가까운 경우
Google Cloud API 키	보안 인증 정보	GCP_API_KEY	예	모두
건강 보험 청구 번호(HICN)	개인 정보: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	예	미국

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
건강 보험 또는 의료 식별 번호	개인 정보: PHI	국가 또는 리전에 따라 다름: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	예	캐나다, EU, 핀란드, 프랑스, 영국, 미국
Healthcare Common Procedure Coding System(HCPCS) 코드	개인 정보: PHI	USA_HEALTHCARE_PROCEDURE_CODE	예	미국
HTTP Basic Authorization 헤더	보안 인증 정보	HTTP_BASIC_AUTH_HEADER	아니요	모두
HTTP 쿠키	개인 정보: PII	HTTP_COOKIE	아니요	모두

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
국제 은행 계좌 번호 (IBAN)	금융 정보	국가 또는 리전에 따라 다름: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER,	아니요	알바니아, 안도라, 보스니아 헤르체고비나, 브라질, 불가리아, 코스타리카, 크로아티아, 키프로스, 체코, 덴마크, 도미니카공화국, 이집트, 에스토니아, 페로 제도, 핀란드, 프랑스, 조지아, 독일, 그리스, 그린란드, 헝가리, 아이슬란드, 아일랜드, 이탈리아, 요르단, 코소보, 리히텐슈타인, 리투아니아, 몰타, 모리타니, 모리셔스, 모나코, 몬테네그로, 네덜

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
		JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRAT		란드, 북마케도니아, 폴란드, 포르투갈, 산마리노, 세네갈, 세르비아, 슬로바키아, 슬로베니아, 스페인, 스웨덴, 스위스, 동티모르, 튀니지, 튀르키예, 영국, 우크라이나, 아랍에미리트, 버진아일랜드(영국령)

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
		ES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER(영국령 버진 아일랜드의 경우)		
JSON Web Token(JWT)	보안 인증 정보	JSON_WEB_TOKEN	아니요	모두
우편 주소	개인 정보: PII	ADDRESS, BRAZIL_CEP_CODE(브라질 우편 번호용)	다양	호주, 브라질, 캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국
국가 의약품 코드(NDC)	개인 정보: PHI	USA_NATIONAL_DRUG_CODE	예	미국
국적 식별 번호	개인 정보: PII	국가 또는 리전에 따라 다름: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	예	브라질, 프랑스, 독일, 인도, 이탈리아, 스페인
National Insurance Number(NINO)	개인 정보: PII	UK_NATIONAL_INSURANCE_NUMBER	예	영국

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
국가 공급자 식별자 (NPI)	개인 정보: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	예	미국
OpenSSH 프라이빗 키	보안 인증 정보	OPENSSH_PRIVATE_KEY	아니요	모두
여권 번호	개인 정보: PII	국가 또는 리전에 따라 다름: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	예	캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국
영주권 번호	개인 정보: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	예	캐나다
PGP 프라이빗 키	보안 인증 정보	PGP_PRIVATE_KEY	아니요	모두
전화번호	개인 정보: PII	국가 또는 리전에 따라 다름: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	다양	브라질, 캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
퍼블릭 키 암호화 표준(PKCS) 프라이빗 키	보안 인증 정보	PKCS	아니요	모두
PuTTY 프라이빗 키	보안 인증 정보	PUTTY_PRIVATE_KEY	아니요	모두
Social Insurance Number(SIN)	개인 정보: PII	CANADA_SOCIAL_INSURANCE_NUMBER	예	캐나다
사회 보장 번호(SSN)	개인 정보: PII	국가 또는 리전에 따라 다름: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	예	스페인, 미국
the section called “Stripe API 키”	보안 인증 정보	STRIPE_CREDENTIALS	아니요	모두

민감한 데이터 유형	민감한 데이터 범주	관리형 데이터 식별자 ID	필수 키워드	국가 및 리전
납세자 식별 번호 또는 참조 번호	개인 정보: PII	국가 또는 리전에 따라 다름: AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	예	호주, 브라질, 프랑스, 독일, 인도, 이탈리아, 스페인, 영국, 미국
고유 디바이스 식별자(UDI)	개인 정보: PHI	MEDICAL_DEVICE_UDI	예	미국
차량 식별 번호(VIN)	개인 정보: PII	VEHICLE_IDENTIFICATION_NUMBER	예	모두 선택, VIN이 영어, 프랑스어, 독일어, 리투아니아어, 폴란드어, 포르투갈어, 루마니아어 또는 스페인어 중 하나의 키워드에 근접한 경우

보안 인증 정보 데이터를 위한 관리형 데이터 식별자

Amazon Macie는 관리형 데이터 식별자를 사용하여 여러 유형의 민감한 보안 인증 정보 데이터를 탐지할 수 있습니다. 이 페이지의 항목에서는 각 유형을 지정하고 데이터를 탐지하도록 설계된 관리형 데이터 식별자에 대한 정보를 제공합니다. 각 주제는 다음 정보를 제공합니다.

- 관리형 데이터 식별자 ID – 데이터를 탐지하도록 설계된 관리형 데이터 식별자의 고유 식별자(ID)를 지정합니다. 민감한 데이터 검색 작업을 생성하거나 민감한 데이터 자동 검색 설정을 구성할 때 이 ID를 사용하여 Macie가 데이터를 분석할 때 관리형 데이터 식별자를 사용할지 여부를 지정할 수 있습니다.
- 지원되는 국가 및 리전 - 해당 관리 데이터 식별자가 어느 국가 또는 리전을 대상으로 설계되었는지를 나타냅니다. 관리 데이터 식별자가 특정 국가 또는 리전에 맞게 설계되지 않은 경우 이 값은 모두 선택 입니다.
- 키워드 필수 - 감지를 위해 데이터에 근접한 키워드가 필요한지 여부를 지정합니다. 키워드가 필요한 경우 해당 주제에서는 필수 키워드의 예시도 제공합니다. Macie가 데이터를 분석할 때 키워드를 사용하는 방법에 대한 자세한 내용은 키워드 요구 사항을(를) 참조하세요.
- 의견 - 관리형 데이터 식별자의 선택 또는 보고된 민감한 데이터 발생 현황에 대한 조사에 영향을 미칠 수 있는 관련 세부 정보를 제공합니다. 세부 정보에는 지원되는 표준, 구문 요구 사항 및 예외와 같은 정보가 포함됩니다.

주제는 민감한 데이터 유형의 알파벳 순서로 제시됩니다.

중요한 데이터 유형

- AWS 비밀 액세스 키
- Google Cloud API 키
- HTTP Basic Authorization 헤더
- JSON Web Token(JWT)
- OpenSSH 프라이빗 키
- PGP 프라이빗 키
- 퍼블릭 키 암호화 표준(PKCS) 프라이빗 키
- PuTTY 프라이빗 키
- Stripe API 키

AWS 비밀 액세스 키

관리형 데이터 식별자 ID: AWS_CREDENTIALS

지원되는 국가 및 리전: 모두 선택

필수 키워드: 예 키워드 예: aws_secret_access_key, credentials, secret access key, secret key, set-awscredential

코멘트: Macie는 일반적으로 가상의 예로 사용되는 `je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY` 및 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`와 같은 문자 시퀀스의 발생을 보고하지 않습니다.

Google Cloud API 키

관리형 데이터 식별자 ID: GCP_API_KEY

지원되는 국가 및 리전: 모두 선택

필수 키워드: 예 키워드 예: G_PLACES_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-key

코멘트: Macie는 Google Cloud API 키의 문자열(`keyString`) 구성 요소만 감지할 수 있습니다. Google Cloud API 키의 ID 또는 표시 이름 구성 요소 감지는 지원에 포함되지 않습니다.

HTTP Basic Authorization 헤더

관리형 데이터 식별자 ID: HTTP_BASIC_AUTH_HEADER

지원되는 국가 및 리전: 모두 선택

필수 키워드: 없음

코멘트: 탐지를 위해서는 RFC 7617에서 지정한 필드 이름 및 인증 체계 지시문을 포함한 전체 헤더가 필요합니다. 예를 들면 `Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==` 및 `Proxy-Authorization: Basic dGVzdDoxMjPCow==` 등입니다.

JSON Web Token(JWT)

관리형 데이터 식별자 ID: JSON_WEB_TOKEN

지원되는 국가 및 리전: 모두 선택

필수 키워드: 없음

코멘트: Macie는 JSON 웹 서명(JWS) 구조에 대한 RFC 7519에 지정된 요구 사항을 준수하는 JSON 웹 토큰(JWT)을 탐지할 수 있습니다. 토큰은 서명되거나 서명되지 않을 수 있습니다.

OpenSSH 프라이빗 키

관리형 데이터 식별자 ID: OPENSSH_PRIVATE_KEY

지원되는 국가 및 리전: 모두 선택

필수 키워드: 없음

코멘트: 없음

PGP 프라이빗 키

관리형 데이터 식별자 ID: PGP_PRIVATE_KEY

지원되는 국가 및 리전: 모두 선택

필수 키워드: 없음

코멘트: 없음

퍼블릭 키 암호화 표준(PKCS) 프라이빗 키

관리형 데이터 식별자 ID: PKCS

지원되는 국가 및 리전: 모두 선택

필수 키워드: 없음

코멘트: 없음

PuTTY 프라이빗 키

관리형 데이터 식별자 ID: PUTTY_PRIVATE_KEY

지원되는 국가 및 리전: 모두 선택

필수 키워드: 없음

설명: Macie는`Encryption`,,, `Comment`Public-Lines, `Private-Lines` 및 같은 표준 헤더 및 헤더 시퀀스를 사용하는 PuTTY 개인 키를 감지할 수 있습니다`PuTTY-User-Key-File`. `Private-MAC` 헤

더 값에는 영숫자, 하이픈 (-) 및 개행 문자 (또는) 가 포함될 수 있습니다. \n \r Public-Lines또한 Private-Lines 값에는 슬래시 (/), 더하기 기호 () 및 등호 () 가 포함될 수 있습니다. + = Private-MAC값에는 더하기 기호 () + 도 포함될 수 있습니다. 헤더 값에 공백이나 밑줄 (_) 같은 다른 문자가 포함된 개인 키의 감지는 Support에 포함되지 않습니다. 또한 사용자 지정 헤더가 포함된 개인 키의 탐지도 Support에 포함되지 않습니다.

Stripe API 키

관리형 데이터 식별자 ID: STRIPE_CREDENTIALS

지원되는 국가 및 리전: 모두 선택

필수 키워드: 없음

코멘트: Macie는 일반적으로 Stripe 코드 예로 사용되는 sk_test_4eC39HqLyjWDarjtT1zdp7dc 및 pk_test_TYooMQauvdEDq54NiTphI7jx와 같은 문자 시퀀스의 발생을 보고하지 않습니다.

금융 정보를 위한 관리형 데이터 식별자

Amazon Macie가 관리형 데이터 식별자를 사용하여 탐지할 수 있는 금융 정보 유형에 대해 알아보세요. 이 페이지의 주제는 각 유형을 제시하고 데이터를 감지하도록 설계된 관리형 데이터 식별자에 대한 정보를 제공합니다. 각 주제는 다음 정보를 제공합니다.

- 관리형 데이터 식별자 ID - 데이터를 감지하도록 설계된 하나 이상의 관리형 데이터 식별자의 고유 식별자(ID)를 지정합니다. 민감한 데이터 검색 작업을 만들거나 민감한 데이터 자동 검색 설정을 구성할 때 이러한 ID를 사용하여 Macie가 데이터를 분석할 때 사용할 관리형 데이터 식별자를 지정할 수 있습니다.
- 지원되는 국가 및 지역 - 해당 관리형 데이터 식별자가 어느 국가 또는 지역을 대상으로 설계되었는지 나타냅니다. 관리형 데이터 식별자가 특정 국가 또는 리전을 대상으로 설계되지 않은 경우 이 값은 모두 선택입니다.
- 키워드 필수 - 감지를 위해 데이터에 근접한 키워드가 필요한지 여부를 지정합니다. 키워드가 필요한 경우 해당 주제에서는 필수 키워드의 예시도 제공합니다. Macie가 데이터를 분석할 때 키워드를 사용하는 방법에 대한 자세한 내용은 키워드 요구 사항을(를) 참조하세요.
- 의견 - 관리형 데이터 식별자의 선택 또는 보고된 민감한 데이터 발생 현황에 대한 조사에 영향을 미칠 수 있는 관련 세부 정보를 제공합니다. 세부 정보에는 지원되는 표준, 구문 요구 사항 및 예외와 같은 정보가 포함됩니다.

주제는 민감한 데이터 유형의 알파벳 순서로 제시됩니다.

중요한 데이터 유형

- 은행 계좌 번호
- 기본 은행 계좌 번호(BBAN)
- 신용 카드 유효 기간
- 신용 카드 마그네틱 스트립 데이터
- 신용 카드 번호
- 신용 카드 인증 코드
- 국제 은행 계좌 번호(IBAN)

은행 계좌 번호

Macie는 9~17자리 시퀀스로 구성되고 공백이 없는 캐나다 및 미국 은행 계좌 번호를 감지할 수 있습니다.

관리형 데이터 식별자 ID: BANK_ACCOUNT_NUMBER

지원되는 국가 및 리전: 캐나다, 미국

필수 키워드: 예. 키워드 예: bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct

의견: 이 관리형 데이터 식별자는 캐나다와 미국의 은행 계좌 번호를 감지하도록 명시적으로 설계되었습니다. 이러한 국가는 ISO 13616에 명시된 은행 계좌 번호 지정에 대한 ISO 국제 표준에 정의된 BBAN(기본 은행 계좌 번호)또는 IBAN(국제 은행 계좌 번호)형식을 사용하지 않습니다. 다른 국가 및 지역의 은행 계좌 번호를 검색하려면 해당 형식에 맞게 설계된 관리형 데이터 식별자를 사용하세요. 자세한 내용은 기본 은행 계좌 번호(BBAN) 및 국제 은행 계좌 번호(IBAN) 섹션을 참조하세요.

기본 은행 계좌 번호(BBAN)

Macie는 ISO 13616에 명시된 은행 계좌 번호 지정에 대한 ISO 국제 표준에 정의된 BBAN 구조를 준수하는 기본 은행 계좌 번호(BBAN)를 탐지할 수 있습니다. 여기에는 공백이 없거나 공백이나 `NWBK60161331926819`, `NWBK 6016 1331 9268 19`, `NWBK-6016-1331-9268-19`와 같은 하이픈 구분자를 사용하는 BBAN도 포함됩니다.

관리형 데이터 식별자 ID: 국가 또는 지역에 따라, FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER

지원되는 국가 및 리전: 프랑스, 독일, 이탈리아, 스페인, 영국

필수 키워드: 예. 다음 표에는 특정 국가 및 리전에서 Amazon Macie가 인식하는 키워드가 나와 있습니다.

국가 또는 리전	키워드
프랑스	account code, account number, accountno#, accountnumber#, bban, code bancaire, compte bancaire, customer account id, customer account number, customer bank account id, iban, numéro de compte
독일	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzahl, iban, kartennummer, kontonummer, kreditkartennummer, sepa
이탈리아	account code, account number, accountno #, accountnumber#, bban, codice bancario, conto bancario, customer account id, customer account number, customer bank account id, iban, numero di conto
스페인	account code, account number, accountno #, accountnumber#, bban, código cuenta, código cuenta bancaria, cuenta cliente id, customer account ID, customer account number, customer bank account id, iban, número cuenta bancaria cliente, número cuenta cliente
uk	account code, account number, accountno #, accountnumber#, bban, customer account id, customer account number, customer bank account id, iban, sepa

의견: 이러한 관리형 데이터 식별자는 ISO 13616 표준을 준수하는 국제 은행 계좌 번호(IBAN)도 탐지할 수 있습니다. 자세한 정보는 국제 은행 계좌 번호(IBAN)을 참조하세요. 영국의 관리형 데이터 식별자(UK_BANK_ACCOUNT_NUMBER)는 영국의 국내 은행 계좌 번호도 감지할 수 있습니다(예:`60-16-13 31926819`).

신용 카드 유효 기간

관리형 데이터 식별자 ID: CREDIT_CARD_EXPIRATION

지원되는 국가 및 리전: 모두 선택

필수 키워드: 예. 키워드 예: exp d, exp m, exp y, expiration, expiry

의견: 지원에는 모든 숫자, 숫자 및 월 이름의 조합과 같은 대부분의 날짜 형식이 포함됩니다. 날짜 구성 요소는 공백, 슬래시(/) 또는 하이픈(-)으로 구분할 수 있습니다. 예를 들어 Macie는 `02/26`, `02/2026`, `Feb 2026`, `26-Feb`, `expY=2026, expM=02` 등의 날짜를 감지할 수 있습니다.

신용 카드 마그네틱 스트립 데이터

관리형 데이터 식별자 ID: CREDIT_CARD_MAGNETIC_STRIPE

지원되는 국가 및 리전: 모두 선택

필수 키워드: 예. 키워드 예: card data, iso7813, mag, magstripe, stripe, swipe

의견: 지원에는 1 및 2 트랙이 포함됩니다.

신용 카드 번호

관리형 데이터 식별자 ID: 키워드 근처에 있는 신용 카드 번호는 CREDIT_CARD_NUMBER_(NO_KEYWORD), 키워드와 인접하지 않은 신용 카드 번호는 CREDIT_CARD_NUMBER

지원되는 국가 및 리전: 모두 선택

필수 키워드: 다양. CREDIT_CARD_NUMBER관리 데이터 식별자에는 키워드가 필요합니다. 키워드 예: account number, american express, amex, bank card, c card, card, cc #, ccn, check card, cred card, credit, credit card, credit cards, credit no, credit num, dankort, debit, debit card, debit no, debit num, diners club, discover, electron, japanese card bureau, jcb, mastercard, mc, pan, payment account number, payment card number, pcn, pmnt #, pmnt card, pmnt no, pmnt number, union pay,

visa CREDIT_CARD_NUMBER_(NO_KEYWORD)관리 데이터 식별자에는 키워드가 필요하지 않습니다.

의견: 탐지를 위해서는 데이터가 Luhn check 공식을 준수하고 아메리칸 익스프레스, 단코트, 다이너스 클럽, 디스커버, 일렉트론, 일본 카드 뷰로 (JCB), 마스터카드, 비자 등의 신용 카드 유형에 표준 카드 번호 접두사를 사용하는 13~19자리 시퀀스여야 합니다. UnionPay

Macie는 신용 카드 발급 기관이 공개 테스트를 위해 예약한 다음 시퀀스가 발생하는 경우는 보고하지 않습니다. 122000000000003, 2222405343248877, 2222990905257051, 2223007648726984, 2223577120017656, 30569309025904, 34343434343434, 3528000700000000, 3530111333300000, 3566002020360505, 36148900647913, 36700102000000, 371449635398431, 378282246310005, 378734493671000, 38520000023237, 4012888888881881, 4111111111111111, 4222222222222, 4444333322221111, 4462030000000000, 4484070000000000, 4911830000000, 4917300800000000, 4917610000000000, 49176100000000000003, 5019717010103742, 5105105105105100, 5111010030175156, 5185540810000019, 5200828282828210, 5204230080000017, 5204740009900014, 5420923878724339, 5454545454545454, 5455330760000018, 5506900490000436, 5506900490000444, 5506900510000234, 5506920809243667, 5506922400634930, 5506927427317625, 5553042241984105, 5555553753048194, 5555555555554444, 5610591081018250, 6011000990139424, 6011000400000000, 6011111111111117, 63049001774029244l, 6304950600000000000, 6331101999990016, 6759649826438453, 6799990100000000019, 76009244561.

신용 카드 인증 코드

관리형 데이터 식별자 ID: CREDIT_CARD_SECURITY_CODE

지원되는 국가 및 리전: 모두 선택

필수 키워드: 예. 키워드 예: card id, card identification code, card identification number, card security code, card validation code, card validation number, card verification data, card verification value, cvc, cvc2, cvv, cvv2, elo verification code

코멘트: 없음

국제 은행 계좌 번호(IBAN)

Macie는 국가 코드와 같은 요소를 포함하여 최대 34개의 영숫자로 구성된 국제 은행 계좌 번호(IBAN)를 탐지할 수 있습니다. 구체적으로, Macie는 ISO 13616에서 명시한 은행 계좌 번호 지정에 대한 ISO 국제 표준을 준수하는 IBAN을 탐지할 수 있습니다. 여기에는 공백이 없

거나 공백이나 GB29NWBK60161331926819, GB29 NWBK 6016 1331 9268 19, GB29-NWBK-6016-1331-9268-19와 같은 하이픈 구분자를 사용하는 IBAN도 포함됩니다. 감지에는 Modulus 97 체계를 기반으로 한 검증 검사가 포함됩니다.

관리형 데이터 식별자 ID: 국가 또는 지역에 따라, ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER(영국령 버진 아일랜드의 경우)

지원 국가 및 지역: 알바니아, 안도라, 보스니아 헤르체고비나, 브라질, 불가리아, 코스타리카, 크로아티아, 키프로스, 체코, 덴마크, 도미니카공화국, 이집트, 에스토니아, 페로 제도, 핀란드, 프랑스, 조지아, 독일, 그리스, 그린란드, 헝가리, 아이슬란드, 아일랜드, 이탈리아, 요르단, 리투아니아, 몰타, 모리타니

아, 몰타, 모리타니아, 모리셔스, 모나코, 몬테네그로, 네덜란드, 북마케도니아, 폴란드, 포르투갈, 산마리노, 세네갈, 세르비아, 슬로바키아, 슬로베니아, 스페인, 스웨덴, 스위스, 동티모르, 튀니지, 터키, 영국, 우크라이나, 아랍에미레이트, 버진 아일랜드(영국령)

필수 키워드: 없음.

의견: 프랑스, 독일, 이탈리아, 스페인, 영국의 관리형 데이터 식별자는 문자 순서가 키워드와 비슷한 경우, ISO 13616 표준에 정의된 BBAN 구조를 준수하는 기본 은행 계좌 번호(BBAN)도 탐지할 수 있습니다. 자세한 내용은 기본 은행 계좌 번호(BBAN)을(를) 참조하세요.

개인 건강 정보(PHI) 관리형 데이터 식별자

Amazon Macie는 관리형 데이터 식별자를 사용하여 여러 유형의 민감한 개인 건강 정보(PHI) 유형을 탐지할 수 있습니다. 이 페이지의 항목에서는 각 유형을 지정하고 데이터를 탐지하도록 설계된 관리형 데이터 식별자에 대한 정보를 제공합니다. 각 주제는 다음 정보를 제공합니다.

- 관리형 데이터 식별자 ID – 데이터를 탐지하도록 설계된 관리형 데이터 식별자의 고유 식별자(ID)를 지정합니다. 민감한 데이터 검색 작업을 생성하거나 민감한 데이터 자동 검색 설정을 구성할 때 이 ID를 사용하여 Macie가 데이터를 분석할 때 관리형 데이터 식별자를 사용할지 여부를 지정할 수 있습니다.
- 지원되는 국가 및 리전 - 해당 관리 데이터 식별자가 어느 국가 또는 리전을 대상으로 설계되었는지를 나타냅니다. 관리 데이터 식별자가 특정 국가 또는 리전에 맞게 설계되지 않은 경우 이 값은 모두 선택 입니다.
- 키워드 필수 - 감지를 위해 데이터에 근접한 키워드가 필요한지 여부를 지정합니다. 키워드가 필요한 경우 해당 주제에서는 필수 키워드의 예시도 제공합니다. Macie가 데이터를 분석할 때 키워드를 사용하는 방법에 대한 자세한 내용은 키워드 요구 사항을(를) 참조하세요.
- 의견 - 관리형 데이터 식별자의 선택 또는 보고된 민감한 데이터 발생 현황에 대한 조사에 영향을 미칠 수 있는 관련 세부 정보를 제공합니다. 세부 정보에는 지원되는 표준, 구문 요구 사항 및 예외와 같은 정보가 포함됩니다.

주제는 민감한 데이터 유형의 알파벳 순서로 제시됩니다.

중요한 데이터 유형

- 마약단속국(DEA) 등록 번호
- 건강 보험 청구 번호(HICN)
- 건강 보험 또는 의료 식별 번호
- Healthcare Common Procedure Coding System(HCPCS) 코드

- 국가 의약품 코드(NDC)
- 국가 공급자 식별자(NPI)
- 고유 디바이스 식별자(UDI)

마약단속국(DEA) 등록 번호

관리형 데이터 식별자 ID: US_DRUG_ENFORCEMENT_AGENCY_NUMBER

지원되는 국가 및 리전: 미국

필수 키워드: 예 키워드 예: dea number, dea registration

코멘트: 없음

건강 보험 청구 번호(HICN)

관리형 데이터 식별자 ID: USA_HEALTH_INSURANCE_CLAIM_NUMBER

지원되는 국가 및 리전: 미국

필수 키워드: 예 키워드 예: health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hicno#

코멘트: 없음

건강 보험 또는 의료 식별 번호

지원에는 EU 및 핀란드의 경우 유럽 건강 보험 카드 번호, 프랑스의 건강 보험 번호, 미국의 경우 메디케어 수혜자 식별자 식별자, 영국의 NHS 번호 및 캐나다의 개인 건강 번호가 포함됩니다.

관리형 데이터 식별자 ID: 국가 또는 지역에 따라, CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

지원되는 국가 및 리전: 캐나다, EU, 핀란드, 프랑스, 영국, 미국

필수 키워드: 예 다음 표에는 특정 국가 및 리전에서 Amazon Macie가 인식하는 키워드가 나와 있습니다.

국가 또는 리전	Keywords
캐나다	canada healthcare number, msp number, personal healthcare number, phn, soins de santé
EU	assicurazione sanitaria numero, carta assicurazione numero, carte d’assurance maladie, carte européenne d'assurance maladie, ceam, ehic, ehic#, finlandehicnumber#, gesundheitskarte, hälsokort, health card, health card number, health insurance card, health insurance number, insurance card number, krankenversicherungskarte, krankenversicherungsnummer, medical account number, numero conto medico, numéro d’assurance maladie, numéro de carte d’assurance, numéro de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausvakuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicherungsnummer
핀란드	ehic, ehic#, finland health insurance card, finlandehicnumber#, finska sjukförsäkringskort, hälsokort, health card, health card number, health insurance card, health insurance number, sairaanhoitokortin, sairaanhoitokortin, sairausvakuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomen sairausvakuutuskortti, suomi ehic-numero, terveyskortti

국가 또는 리전	Keywords
프랑스	carte d'assuré social, carte vitale, insurance card
영국	national health service, NHS
미국	mbi, medicare beneficiary

코멘트: 없음

Healthcare Common Procedure Coding System(HCPCS) 코드

관리형 데이터 식별자 ID: USA_HEALTHCARE_PROCEDURE_CODE

지원되는 국가 및 리전: 미국

필수 키워드: 예 키워드 예: current procedural terminology, hcpcs, healthcare common procedure coding system

코멘트: 없음

국가 의약품 코드(NDC)

관리형 데이터 식별자 ID: USA_NATIONAL_DRUG_CODE

지원되는 국가 및 리전: 미국

필수 키워드: 예 키워드 예: national drug code, ndc

코멘트: 없음

국가 공급자 식별자(NPI)

관리형 데이터 식별자 ID: USA_NATIONAL_PROVIDER_IDENTIFIER

지원되는 국가 및 리전: 미국

필수 키워드: 예 키워드 예: hipaa, n.p.i, national provider, npi

코멘트: 없음

고유 디바이스 식별자(UDI)

관리형 데이터 식별자 ID: MEDICAL_DEVICE_UDI

지원되는 국가 및 리전: 미국

필수 키워드: 예 키워드 예: blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifier

코멘트: Macie는 미국 식품의약청에서 승인한 형식을 준수하는 고유 디바이스 식별자(UDI)를 탐지할 수 있습니다. 여기에는 GS1, HIBCC 및 ICCBBA에서 정의한 표준 형식이 포함됩니다. ICCBA 지원은 ISBT 표준에 대한 것입니다.

개인 식별 정보(PII)용 관리 데이터 식별자

Amazon Macie가 관리형 데이터 식별자를 사용하여 탐지할 수 있는 개인 식별 정보(PII) 데이터 유형에 대해 알아보세요. 이 페이지의 주제는 각 유형을 제시하고 데이터를 감지하도록 설계된 관리형 데이터 식별자에 대한 정보를 제공합니다. 각 주제는 다음 정보를 제공합니다.

- 관리형 데이터 식별자 ID - 데이터를 감지하도록 설계된 하나 이상의 관리형 데이터 식별자의 고유 식별자(ID)를 지정합니다. 민감한 데이터 검색 작업을 만들거나 민감한 데이터 자동 검색 설정을 구성할 때 이러한 ID를 사용하여 Macie가 데이터를 분석할 때 사용할 관리형 데이터 식별자를 지정할 수 있습니다.
- 지원되는 국가 및 지역 - 해당 관리형 데이터 식별자가 어느 국가 또는 지역을 대상으로 설계되었는지 나타냅니다. 관리형 데이터 식별자가 특정 국가 또는 리전을 대상으로 설계되지 않은 경우 이 값은 모두 선택입니다.
- 키워드 필수 - 감지를 위해 데이터에 근접한 키워드가 필요한지 여부를 지정합니다. 키워드가 필요한 경우 해당 주제에서는 필수 키워드의 예시도 제공합니다. Macie가 데이터를 분석할 때 키워드를 사용하는 방법에 대한 자세한 내용은 키워드 요구 사항을(를) 참조하세요.
- 의견 - 관리형 데이터 식별자의 선택 또는 보고된 민감한 데이터 발생 현황에 대한 조사에 영향을 미칠 수 있는 관련 세부 정보를 제공합니다. 세부 정보에는 지원되는 표준, 구문 요구 사항 및 예외와 같은 정보가 포함됩니다.

주제는 민감한 데이터 유형의 알파벳 순서로 제시됩니다.

중요한 데이터 유형

- 생년월일
- 운전면허증 식별 번호

- 선거인단 번호
- 전체 이름
- 위성 항법 시스템(GPS) 좌표
- HTTP 쿠키
- 우편 주소
- 국적 식별 번호
- National Insurance Number(NINO)
- 여권 번호
- 영주권 번호
- 전화번호
- Social Insurance Number(SIN)
- 사회 보장 번호(SSN)
- 납세자 식별 번호 또는 참조 번호
- 차량 식별 번호(VIN)

생년월일

관리형 데이터 식별자 ID: DATE_OF_BIRTH

지원되는 국가 및 리전: 모두 선택

필수 키워드: 예. 키워드 예: bday, b-day, birth date, birthday, date of birth, dob

의견: 지원에는 모든 숫자, 숫자 및 월 이름의 조합과 같은 대부분의 날짜 형식이 포함됩니다. 날짜 구성 요소는 공백, 슬래시(/) 또는 하이픈(-)으로 구분할 수 있습니다.

운전면허증 식별 번호

관리형 데이터 식별자 ID: 국가 또는 지역에 따라, AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE,

LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE

지원되는 국가 및 리전: 호주, 오스트리아, 벨기에, 불가리아, 캐나다, 크로아티아, 사이프러스, 체코 공화국, 덴마크, 에스토니아, 핀란드, 프랑스, 독일, 그리스, 헝가리, 아일랜드, 이탈리아, 라트비아, 리투아니아, 룩셈부르크, 몰타, 네덜란드, 폴란드, 포르투갈, 루마니아, 슬로바키아, 슬로베니아, 스페인, 스웨덴, 영국, 미국

필수 키워드: 예. 다음 표에는 특정 국가 및 리전에서 Amazon Macie가 인식하는 키워드가 나와 있습니다.

국가 또는 리전	키워드
호주	dl#, dl:, dlno#, driver licence, driver license, driver permit, drivers lic., drivers licence, driver's licence, drivers license, driver's license, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
오스트리아	führerschein, fuhrerschein, führerschein republik österreich, fuhrerschein republik osterreich
벨기에	fuehrerschein, fuehrerschein- nr, fuehrerschheinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrerscheinnummer, führerscheinnummer, numéro permis conduire, permis de conduire, rijbewijs, rijbewijsnummer
불가리아	превозно средство, свидетелство за управление на моторно, свидетелство за управление на мпс, сумпс, шофьорска книжка

국가 또는 리전	키워드
캐나다	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit, permis de conduire
크로아티아	vozačka dozvola
사이프러스	άδεια οδήγησης
체코 공화국	číslo licence, číslo licence řidiče, číslo řidičskéh o průkazu, ovladače lic., povolení k jízdě, povolení řidiče, řidiči povolení, řidičský prúkaz, řidičský průkaz
덴마크	kørekort, kørekortnummer
에스토니아	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
핀란드	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire
프랑스	permis de conduire
독일	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer
그리스	δεια οδήγησης, adeia odigisis

국가 또는 리전	키워드
헝가리	illesztőprogramok lic, jogosítvány, jogsi, licencszám, vezető engedély, vezetői engedély
인도	driver licence, driver licences, driver license, driver licenses, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, driving licence, driving license
아일랜드	ceadúnas tiomána
이탈리아	patente di guida, patente di guida numero, patente guida, patente guida numero
라트비아	autovadītāja apliecība, licences numurs, vadītāja apliecība, vadītāja apliecības numurs, vadītāja atļauja, vadītāja licences numurs, vadītāji lic.
리투아니아	vairuotojo pažymėjimas
룩셈부르크	fahrerlaubnis, führerschäin
몰타	liċenzja tas-sewqan
네덜란드	permis de conduire, rijbewijs, rijbewijsnummer
폴란드	numer licencyjny, prawo jazdy, zezwolenie na prowadzenie
포르투갈	carta de condução, carteira de habilitação, carteira de motorist, carteira habilitação, carteira motorist, licença condução, licença de condução, número de licença, número licença, permissão condução, permissão de condução

국가 또는 리전	키워드
루마니아	numărul permisului de conducere, permis de conducere
슬로바키아	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
슬로베니아	vozniško dovoljenje
스페인	carnet conducer, el carnet de conducer, licencia conducer, licencia de manejo, número carnet conducer, número de carnet de conducer, número de permiso conducer, número de permiso de conducer, número licencia conducer, número permiso conducer, permiso conducción, permiso conducer, permiso de conducción
스웨덴	ajokortin numero, dlno# ajokortti, drivere lic., förare lic., körkort, körkort nummer, körkortsn ummer, kuljettajat lic.
영국	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

국가 또는 리전	키워드
미국	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

코멘트: 없음

선거인단 번호

관리형 데이터 식별자 ID: UK_ELECTORAL_ROLL_NUMBER

지원되는 국가 및 리전: 영국

필수 키워드: 예. 키워드 예: electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollno

코멘트: 없음

전체 이름

관리형 데이터 식별자 ID: NAME

지원되는 국가 및 리전: 모두 선택

필수 키워드: 없음.

의견: Macie는 전체 이름만 감지할 수 있습니다. 라틴 문자 집합만 지원합니다.

위성 항법 시스템(GPS) 좌표

관리형 데이터 식별자 ID: LATITUDE_LONGITUDE

지원되는 국가 및 지역: Any, 좌표가 영어 키워드에 근접한 경우

필수 키워드: 예. 키워드 예: coordinate, coordinates, lat long, latitude longitude, position

코멘트: Macie는 위도 및 경도 좌표가 한 쌍으로 저장되고 십진수(DD) 형식인 경우에서 GPS 좌표를 탐지할 수 있습니다, 예를 들어 `41.948614,-87.655311` 10진수 도(DDM) 형식(예: `41°56.9168'N 87°39.3187'W`) 또는 도, 분 초(DMS) 형식(예: `41°56'55.0104"N 87°39'19.1196"W`)의 좌표 감지는 지원되지 않습니다.

HTTP 쿠키

관리형 데이터 식별자 ID: HTTP_COOKIE

지원되는 국가 및 리전: 모두 선택

필수 키워드: 없음.

의견: 감지를 위해서는 전체 `Cookie` 또는 `Set-Cookie` 헤더가 필요합니다. 헤더에는 하나 이상의 이름-값 쌍이 포함될 수 있습니다(예: `Set-Cookie: id=TWlrZQ` 및 `Cookie: session=3948; lang=en`).

우편 주소

관리 데이터 식별자 ID: ADDRESS (호주, 캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국의 경우), BRAZIL_CEP_CODE (브라질 우편 번호의 경우)

지원되는 국가 및 지역: 호주, 브라질, 캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국

필수 키워드: 다양. 관리 데이터 식별자에는 키워드가 필요하지 않습니다. ADDRESS BRAZIL_CEP_CODE관리 데이터 식별자에는 키워드가 필요합니다. 키워드 예: cep, código de endereçamento postal, codigo de endereçamento postal, código postal, codigo postal

댓글: ADDRESS 관리 데이터 식별자에는 키워드가 필요하지 않지만 검색하려면 도시 또는 장소의 이름을 포함하는 주소와 지원되는 국가 또는 지역의 해당 우편번호 또는 우편번호가 필요합니다. BRAZIL_CEP_CODE관리형 데이터 식별자는 주소의 CEP (우편 번호) 부분만 탐지할 수 있습니다.

국적 식별 번호

지원에는 Documento Nacional de Identidad(DNI) 식별자(스페인), 프랑스 국립 통계 및 경제 연구소(INSEE) 코드, 독일 신분증 번호 및 Registro Geral(RG) 번호(브라질)이 포함됩니다.

관리형 데이터 식별자 ID: 국가 또는 지역에 따라, BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER,

GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

지원되는 국가 및 지역: 브라질, 프랑스, 독일, 인도, 이탈리아, 스페인

필수 키워드: 예. 다음 표에는 특정 국가 및 리전에서 Amazon Macie가 인식하는 키워드가 나와 있습니다.

국가 또는 리전	키워드
브라질	registro geral, rg
프랑스	assurance sociale, carte nationale d’identité, cni, code sécurité sociale, French social security number, fssn#, insee, insurance number, national id number, nationalid#, numéro d'assurance, sécurité sociale, sécurité sociale non., sécurité sociale numéro, social, social security, social security number, socialsecuritynumber, ss#, ssn, ssn#
독일	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
인도	aadhaar, aadhar, adhaar, uidai
이탈리아	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
스페인	dni, dni#, dninúmero#, documento nacional de identidad, identidad único, identidadúnico#, insurance number, national identification number, national identity, nationalid#, nationalidno#, número nacional identidad, personal identification number, personal identity no, unique identity number, uniqueid#

코멘트: 없음

National Insurance Number(NINO)

관리형 데이터 식별자 ID: UK_NATIONAL_INSURANCE_NUMBER

지원되는 국가 및 리전: 영국

필수 키워드: 예. 키워드 예: insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

코멘트: 없음

여권 번호

관리형 데이터 식별자 ID: 국가 또는 지역에 따라, CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER

지원되는 국가 및 지역: 캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국

필수 키워드: 예. 다음 표에는 특정 국가 및 리전에서 Amazon Macie가 인식하는 키워드가 나와 있습니다.

국가 또는 리전	키워드
캐나다	passeport, passeport#, passport, passport#, passportno, passportno#
프랑스	numéro de passeport, passeport, passeport #, passeport n °, passeport non
독일	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reisepass, reisepass–nr, reisepassnummer
이탈리아	italian passport number, numéro passeport, numéro passeport italien, passaporto, passaporto italiana, passaporto numero,

국가 또는 리전	키워드
	passport number, repubblica italiana passaport o
스페인	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport
영국	passeport #, passeport n °, passeport non, passeportn °, passport #, passport no, passport number, passport#, passportid
미국	passport, travel document

코멘트: 없음

영주권 번호

관리형 데이터 식별자 ID: CANADA_NATIONAL_IDENTIFICATION_NUMBER

지원되는 국가 및 리전: 캐나다

필수 키워드: 예. 키워드 예: carte résident permanent, numéro carte résident permanent, numéro résident permanent, permanent resident card, permanent resident card number, permanent resident no, permanent resident no., permanent resident number, pr no, pr no., pr non, pr number, résident permanent no., résident permanent non

코멘트: 없음

전화번호

관리형 데이터 식별자 ID: 국가 또는 지역에 따라, BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER

지원되는 국가 및 지역: 브라질, 캐나다, 프랑스, 독일, 이탈리아, 스페인, 영국, 미국

필수 키워드: 다양. 키워드가 데이터에 근접한 경우 번호에 국가 코드를 포함할 필요가 없습니다. 키워드 예: cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone number

브라질의 경우 키워드에 다음을 포함합니다. cel, celular, fone, móvel, número residencial, numero residencial, telefone. 키워드가 데이터에 근접하지 않은 경우 숫자에 국가 코드가 포함되지 않아도 됩니다.

의견: 미국의 경우 수신자 부담 전화 번호가 지원됩니다.

Social Insurance Number(SIN)

관리형 데이터 식별자 ID: CANADA_SOCIAL_INSURANCE_NUMBER

지원되는 국가 및 리전: 캐나다

필수 키워드: 예. 키워드 예: canadian id, numéro d'assurance sociale, sin, social insurance number

코멘트: 없음

사회 보장 번호(SSN)

관리형 데이터 식별자 ID: 국가 또는 지역에 따라, SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

지원되는 국가 및 리전: 스페인, 미국

필수 키워드: 예. 스페인의 경우 키워드는 número de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#와 같습니다. 미국의 경우 키워드는 다음과 같습니다 social security, ss#, ssn.

코멘트: 없음

납세자 식별 번호 또는 참조 번호

지원 대상: 스페인의 경우 CIF, NIE 및 NIF 번호, 브라질의 경우 CNPJ 및 CPF 번호, 이탈리아의 경우 Codice Fisscale 번호, 미국의 경우 ITIN, 인도의 경우 PAN, 독일의 경우 SteueridentificationsNumer 번호, 호주의 경우 TFN, 프랑스의 경우 TIN, 영국의 경우 TRN 및 UTR 번호.

관리형 데이터 식별자 ID: 국가 또는 지역에 따라, AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

지원되는 국가 및 지역: 호주, 브라질, 프랑스, 독일, 인도, 이탈리아, 스페인, 영국, 미국

필수 키워드: 예. 다음 표에는 특정 국가 및 리전에서 Amazon Macie가 인식하는 키워드가 나와 있습니다.

국가 또는 리전	키워드
호주	tax file number, tfn
브라질	cadastro de pessoa física, cadastro de pessoa fisica, cadastro de pessoas físicas, cadastro de pessoas fisicas, cadastro nacional da pessoa jurídica, cadastro nacional da pessoa juridica, cnpj, cpf
프랑스	numéro d'identification fiscal, tax id, tax identification number, tax number, tin, tin#
독일	identifikationsnummer, steuer id, steueridentifikationsnummer, steuernummer, tax id, tax identification number, tax number
인도	e-pan, pan card, pan number, permanent account number
이탈리아	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
스페인	cif, cif número, cifnúmero#, nie, nif, número de contribuyente, número de identidad de extranjero, número de identificación fiscal, número de impuesto corporativo, personal tax number, tax id, tax identification number, tax number, tin, tin#
영국	paye, tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax number, tax reference, tax#, taxid#, temporary

국가 또는 리전	키워드
	reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
미국	개인 납세자 식별 번호(itin, i.t.i.n.)

코멘트: 없음

차량 식별 번호(VIN)

관리형 데이터 식별자 ID: VEHICLE_IDENTIFICATION_NUMBER

지원되는 국가 및 지역: 모두 선택, VIN이 영어, 프랑스어, 독일어, 리투아니아어, 폴란드어, 포르투갈어, 루마니아어 또는 스페인어 중 하나의 키워드에 근접한 경우

필수 키워드: 예. 키워드 예: Fahrgestellnummer, niv, numarul de identificare, numarul seriei de sasiu, numer VIN, Número de Identificação do Veículo, Número de Identificación de Automóviles, numéro d'identification du véhicule, vehicle identification number, vin, VIN numeris

코멘트: Macie는 17자 시퀀스로 구성되고 ISO 3779 및 3780 표준을 준수하는 VIN을 탐지할 수 있습니다. 이 표준은 전 세계에서 사용할 수 있도록 설계되었습니다.

Amazon Macie에서 사용자 지정 데이터 식별자 빌드

사용자 지정 데이터 식별자는 Amazon Simple Storage Service(S3) 객체의 민감한 데이터를 감지하기 위해 정의하는 기준 집합입니다. 기준은 일치시킬 텍스트 패턴을 정의하고 선택적으로 문자 시퀀스와 결과를 세분화하는 근접성 규칙을 정의하는 정규 표현식(regex)으로 구성됩니다.

사용자 지정 데이터 식별자를 사용하면 조직의 특정 시나리오, 지적 재산 또는 독점 데이터(예: 직원 ID, 고객 계정 번호 또는 내부 데이터 분류)를 반영하는 탐지 기준을 정의할 수 있습니다. 이러한 식별자를 사용하도록 민감한 데이터 검색 작업 또는 민감한 데이터 자동 검색을 구성하면 Amazon Macie가 제공하는 관리형 데이터 식별자를 보완하는 방식으로 S3 객체를 분석할 수 있습니다.

탐지 기준 외에도, 사용자 지정 데이터 식별자가 생성하는 민감한 데이터 조사 결과에 대한 사용자 지정 심각도 설정을 정의할 수 있습니다. 기본적으로 Macie는 사용자 지정 데이터 식별자가 생성하는 모든 결과에 중간 심각도를 할당합니다. 즉, 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 텍스트의 발생 횟수에 따라 심각도가 변경되지 않습니다. 사용자 지정 심각도 설정을 정의하여 기준과 일치하는 텍스트 발생 횟수에 따라 할당할 심각도를 지정할 수 있습니다.

주제

사용자 지정 데이터 식별자의 탐지 기준 정의

사용자 지정 데이터 식별자를 생성할 때 S3 객체에서 일치시킬 텍스트 패턴을 정의하는 정규 표현식(정규식)을 지정합니다. Macie는 펄 호환 정규 표현식(PCRE) 라이브러리에서 제공하는 정규식 패턴 구문의 하위 집합을 지원합니다. 자세한 내용은 이 정규식 지원 단원의 뒷부분을 참조하세요.

또한 단어 및 구문과 같은 문자 시퀀스와 근접 규칙을 지정하여 결과를 세분화할 수 있습니다.

키워드

이는는 정규식 패턴과 일치하는 텍스트와 근접해야 하는 특정 문자 시퀀스입니다. 근접성 요구 사항은 S3 객체의 스토리지 형식 또는 파일 유형에 따라 달라집니다.

- 컬럼 형식의 정형 데이터의 경우, Macie는 텍스트가 정규식 패턴과 일치하고 키워드가 텍스트를 저장하는 필드 또는 열의 이름에 포함되거나, 텍스트 앞에 동일한 필드 또는 셀 값에서 키워드의 최대 일치 거리 이내에 있는 경우, 결과를 포함합니다. Microsoft Excel 통합 문서, CSV 파일 및 TSV 파일의 경우에도 마찬가지입니다.
- 레코드 기반의 정형 데이터의 경우, Macie는 텍스트가 정규식 패턴과 일치하고 텍스트가 키워드의 최대 일치 거리 내에 있는 경우, 결과를 포함합니다. 키워드는 텍스트를 저장하는 필드 또는 배열의 경로에 있는 요소 이름에 포함되거나 텍스트를 저장하는 필드 또는 배열에서 동일한 값의 앞에 올 수도 있고 그 값의 일부일 수도 있습니다. 이는 Apache Avro 객체 컨테이너, Apache Parquet 파일, JSON 파일 및 JSON 행 파일에 해당합니다.
- 비정형 데이터의 경우, Macie는 텍스트가 정규식 패턴과 일치하고 텍스트 앞에 키워드의 최대 일치 거리 이내에 있거나 키워드의 최대 일치 거리 내에 있는 경우, 결과를 포함합니다. CSV, JSON, JSON Lines 및 TSV 파일을 제외한 Adobe Portable Document Format 형식 파일, Microsoft Word 문서, 이메일 메시지 및 바이너리가 아닌 텍스트 파일의 경우에도 마찬가지입니다. 여기에는 이러한 유형의 파일에 있는 모든 정형 데이터(예: 표)가 포함됩니다.

최대 50개의 키워드를 지정할 수 있습니다. 각 키워드는 3~90개의 UTF-8 문자를 포함할 수 있습니다. 키워드는 대/소문자를 구분하지 않습니다

최대 일치 거리

키워드에 대한 문자 기반 근접성 규칙입니다. Macie는 이 설정을 사용하여 정규식 패턴과 일치하는 텍스트에 대한 키워드가 앞에 있는지 확인합니다. 설정은 전체 키워드의 끝과 정규식 패턴과 일치하는 텍스트의 끝 사이에 존재할 수 있는 최대 문자 수를 정의합니다. 텍스트가 정규식 패턴과 일치하고 하나 이상의 완전한 키워드 뒤에 나타나며 키워드로부터 지정된 거리 내에 있는 경우, Macie는 해당 텍스트를 결과에 포함합니다. 그렇지 않으면 Macie는 해당 결과를 결과에서 제외합니다.

1~300자의 거리를 지정할 수 있습니다. 기본 거리는 50자입니다. 최상의 결과를 얻으려면 이 거리가 정규식이 감지하도록 설계된 텍스트의 최소 문자 수보다 커야 합니다. 텍스트의 일부만 키워드의 최대 일치 거리 내에 있는 경우, Macie는 해당 텍스트를 결과에 포함하지 않습니다.

단어 무시

이는 결과에서 제외할 특정 문자 시퀀스입니다. 텍스트가 정규식 패턴과 일치하지만 단어 무시를 포함하면 Macie는 결과에 이를 포함시키지 않습니다.

최대 10개의 단어 무시를 지정할 수 있습니다. 각 단어 무시는 4~90개의 UTF-8 문자를 포함할 수 있습니다. 단어 무시는 대/소문자를 구분합니다.

예를 들어, 많은 회사에서는 직원 ID에 대한 특정 구문을 사용합니다. 이러한 구문 중 하나는 직원이 상근직(F) 직원인지 비상근직(P) 직원인지를 나타내는 대문자, 하이픈 (-), 직원을 식별하는 8자리 시퀀스가 그 뒤에 오는 것입니다. 예: 상근직 직원의 경우, F-12345678, 비상근직 직원의 경우, P-87654321 등이 있습니다.

사용자 지정 데이터 식별자를 생성하여 이 구문을 사용하는 직원 ID를 탐지하는 경우, 다음 `[A-Z]-\d{8}` 정규식을 사용할 수 있습니다. 분석을 세분화하고 오탐을 방지하기 위해 직원 및 직원 ID 키워드를 사용하고 최대 20자의 일치 거리를 사용하도록 사용자 지정 데이터 식별자를 구성할 수도 있습니다. 이러한 기준을 사용하면 텍스트가 직원 또는 직원 ID 키워드 뒤에 나오고 모든 텍스트가 해당 키워드 중 하나의 20자 이내인 경우에만 정규식과 일치하는 텍스트가 결과에 포함됩니다.

키워드를 사용하여 민감한 데이터를 찾고 오탐을 방지하는 방법에 대한 데모를 보려면 다음 동영상을 시청하십시오. Amazon Macie가 키워드를 사용하여 민감한 데이터를 검색하는 방법.

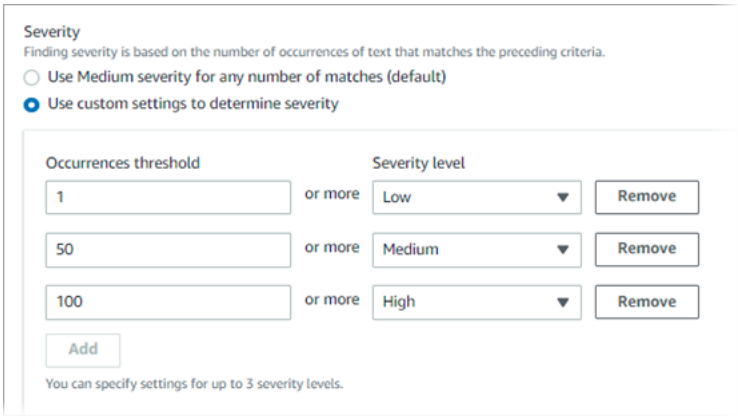
사용자 지정 데이터 식별자의 조사 결과 심각도 설정 정의

사용자 지정 데이터 식별자를 생성할 때 식별자가 생성하는 민감한 데이터 조사 결과에 대한 사용자 지정 심각도 설정을 정의할 수도 있습니다. 기본적으로 Macie는 사용자 지정 데이터 식별자가 생성하는

모든 조사 결과에 중간 심각도를 할당합니다. 즉, S3 객체에 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 텍스트가 하나 이상 포함되어 있는 경우, Macie는 결과적인 조사 결과에 중간 심각도를 자동으로 할당합니다.

사용자 지정 심각도 설정을 사용하면 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 텍스트 발생 횟수를 기반으로 할당할 심각도를 지정할 수 있습니다. 이를 위해 심각도 수준 낮음(가장 낮음), 중간, 높음(가장 심각) 의 최대 세 가지 심각도 수준에 대한 발생 임계값을 정의합니다. 발생 임계값은 지정된 심각도의 조사 결과를 생성하기 위해 S3 객체에 존재해야 하는 최소 일치 항목 수입니다. 임계값을 두 개 이상 지정하는 경우, 임계값은 심각도에 따라 오름차순으로 낮음에서 높음으로 이동해야 합니다.

예를 들어, 다음 이미지는 Macie가 지원하는 심각도 수준별로 하나씩 총 세 개의 발생 임계값을 지정하는 사용자 지정 데이터 식별자의 심각도 설정을 보여줍니다.



다음 표는 사용자 지정 데이터 식별자가 생성하는 조사 결과의 심각도를 나타냅니다.

발생 임계값	심각도 수준	결과
1	낮음	S3 객체에 탐지 기준과 일치하는 1~49개의 텍스트가 포함된 경우, 결과적인 조사 결과의 심각도는 낮음입니다.
50	중간	S3 객체에 탐지 기준과 일치하는 텍스트가 50~99개 포함되어 있는 경우, 결과적인 조사 결과의 심각도는 중간입니다.
100	높음	S3 객체에 탐지 기준과 일치하는 텍스트가 100개 이상 포함

발생 임계값	심각도 수준	결과
		된 경우, 결과적인 조사 결과의 심각도는 높음입니다.

또한 심각도 설정을 사용하여 조사 결과를 생성할지 여부를 지정할 수 있습니다. S3 객체의 발생 횟수가 최저 발생 임계값보다 적은 경우, Macie는 조사 결과를 생성하지 않습니다.

사용자 지정 데이터 식별자 생성

다음 단계에 따라 Amazon Macie 콘솔을 사용하여 사용자 지정 데이터 식별자를 생성합니다. 프로그래밍 방식으로 사용자 지정 데이터 식별자를 생성하려면 Amazon Macie API의 CreateCustomDataIdentifier 작업을 사용하십시오.

사용자 지정 데이터 식별자를 생성하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창의 설정에서 사용자 지정 데이터 식별자를 선택합니다.
3. 생성을 선택합니다.
4. 이름에서 사용자 지정 데이터 식별자의 이름을 입력합니다. 이름은 최대 128자까지 포함할 수 있습니다.

   이름에 민감한 데이터를 포함하지 마세요. Macie에서 수행할 수 있는 작업에 따라 계정의 기타 사용자가 이름을 볼 수 있습니다.
5. (선택 사항) 설명에 사용자 지정 데이터 식별자에 대한 간략한 설명을 입력합니다. 설명은 512자까지 포함할 수 있습니다.

   설명에 민감한 데이터를 포함하지 마세요. Macie에서 수행할 수 있는 작업에 따라 계정의 기타 사용자가 설명을 볼 수 있습니다.
6. 정규 표현식의 경우, 일치시킬 텍스트 패턴을 정의하는 정규 표현식(정규식)을 입력합니다. 이름은 최대 512자까지 포함할 수 있습니다. 지원되는 구문 및 제약조건에 대해 알아보려면 이 섹션 정규식 지원 뒷부분을 참조하세요.
7. (선택 사항) 키워드의 경우, 최대 50개의 문자 시퀀스 (쉼표로 구분) 를 입력하여 정규식 패턴과 일치하는 텍스트 근처에 있어야 하는 특정 텍스트를 정의합니다. 각 키워드는 3~90개의 UTF-8 문자를 포함할 수 있습니다. 키워드는 대/소문자를 구분하지 않습니다

Macie는 이전 항목에서 설명한 것처럼 텍스트가 정규식 패턴과 일치하고 텍스트가 이러한 키워드 중 하나와 일치하는 최대 일치 거리 내에 있는 경우에만 결과에 해당 항목을 포함합니다.

8. (선택 사항) 단어 무시 의 경우, 결과에서 제외할 특정 텍스트를 정의하는 최대 10개의 문자 시퀀스(쉼표로 구분) 를 입력합니다. 각 단어 무시는 4~90개의 UTF-8 문자를 포함할 수 있습니다. 단어 무시는 대/소문자를 구분합니다.

   Macie는 텍스트가 정규식 패턴과 일치하지만 이러한 단어 무시 중 하나를 포함하는 경우, 해당 항목을 결과에서 제외합니다.

9. (선택 사항) 최대 일치 거리의 경우, 키워드의 끝 및 정규식 패턴과 일치하는 텍스트 끝 사이에 존재할 수 있는 최대 문자 수를 입력합니다. 거리는 1~300자일 수 있습니다. 기본 거리는 50자입니다.

   Macie는 이전 항목에서 설명한 것처럼 텍스트가 정규식 패턴과 일치하고 텍스트가 전체 키워드로부터 이 거리 내에 있는 경우에만 결과에 일치 항목을 포함합니다.

10. 심각도에서는 Macie에서 사용자 지정 데이터 식별자가 생성하는 민감한 데이터 조사 결과에 심각도를 할당하는 방식을 선택합니다.

    - 모든 조사 결과에 중간 심각도를 자동으로 할당하려면 일치하는 개수에 대해 중간 심각도 사용(기본값) 을 선택합니다. 이 옵션을 사용하면 Macie는 영향을 받는 S3 객체에 탐지 기준과 일치하는 텍스트가 한 번 이상 포함되어 있는지 여부에 대해 조사 결과에 중간 심각도를 자동으로 할당합니다.
    - 지정한 발생 횟수 임계값을 기반으로 심각도를 할당하려면 사용자 지정 설정을 사용하여 심각도 확인을 선택합니다. 그런 다음 발생 임계값 및 심각도 수준 옵션을 사용하여 선택한 심각도의 조사 결과를 생성하기 위해 S3 객체에 존재해야 하는 최소 일치 개수를 지정합니다.

      예를 들어 탐지 기준과 일치하는 텍스트를 100회 이상 보고하는 조사 결과에 높음 심각도를 할당하려면 발생 임계값란의 **100**에 입력한 다음 심각도 수준 목록에서 높음을 선택합니다.

      가 지원하는 심각도 수준별로 낮음(가장 심각하지 않은 경우), 중간 또는 높음(가장 심각한 경우)의 발생 임계값을 3개까지 지정할 수 있습니다. 두 개 이상 지정하는 경우, 임계값은 심각도에 따라 오름차순으로 낮음에서 높음으로 이동해야 합니다. S3 객체의 발생 횟수가 최저 지정된 임계값보다 적은 경우, Macie는 조사 결과를 생성하지 않습니다.

11. (선택 사항) 태그 에서 태그 추가를 선택한 다음 사용자 지정 데이터 식별자에 할당할 태그를 50개까지 입력합니다.

    태그는 사용자가 정의하여 특정 유형의 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과

같은 다양한 방법으로 리소스를 식별, 분류, 관리하는 데 도움이 됩니다. 자세한 내용은 Amazon Macie에 리소스 태그 지정(을)를 참조하세요.

12. (선택 사항) 평가의 경우, 샘플 데이터란에 최대 1,000자를 입력한 다음 테스트를 선택하여 탐지 기준을 테스트합니다. Macie는 샘플 데이터를 평가하여 기준과 일치하는 텍스트의 발생 횟수를 보고합니다. 이 단계를 원하는 만큼 반복하여 기준을 세분화하고 최적화할 수 있습니다.

> **Note**
>
> 사용자 지정 데이터 식별자를 저장하기 전에 감지 기준을 테스트하고 수정하는 것이 좋습니다. 사용자 지정 데이터 식별자는 민감한 데이터 검색 작업에 사용되므로 사용자 지정 데이터 식별자를 저장한 후에는 편집할 수 없습니다. 이를 통해 수행하는 데이터 프라이버시 및 보호 감사 또는 조사에 대한 민감한 데이터 조사 결과 및 검색 결과에 대한 변경 불가능한 기록이 있는지 확인할 수 있습니다.

13. 마쳤으면 Submit(제출)을 선택합니다.

Macie는 설정을 테스트하여 정규식을 컴파일할 수 있는지 확인합니다. 설정이나 정규식에 문제가 있는 경우, 오류가 발생하여 문제의 본질을 알 수 있습니다. 문제를 해결한 후 사용자 지정 데이터 식별자를 저장할 수 있습니다.

사용자 지정 데이터 식별자의 정규식 지원

Macie는 펄 호환 정규 표현식(PCRE) 라이브러리에서 제공하는 정규식 패턴 구문의 하위 집합을 지원합니다. PCRE 라이브러리에서 제공하는 구문 중에서 Macie는 다음 패턴 요소를 지원하지 않습니다.

- 역참조
- 캡처 그룹
- 조건 패턴
- 임베디드 코드
- 글로벌 패턴 플래그(예: `/i`, `/m` 및 `/x`)
- 재귀 패턴
- 포지티브 및 네가티브 후방탐색 및 전방탐색 제로 폭 어설션(예: `?=`, `?!`, `?<=` 및 `?<!`)

사용자 지정 데이터 식별자를 위한 효과적인 정규식 패턴을 만들려면 다음 팁과 권장 사항도 참고하세요.

- 앵커 – 패턴이 줄의 시작이나 끝이 아닌 파일의 시작이나 끝에 나타날 것으로 예상되는 경우에만 앵커 (^ 또는 $) 를 사용하십시오.
- 제한된 반복 – 성능상의 이유로 Macie는 제한된 반복 그룹의 크기를 제한합니다. 예를 들어, Macie에서는 `\d{100,1000}` 컴파일되지 않습니다. 다음과 같은 서술형 반복을 사용하면 이 함수의 근사치를 계산할 수 있습니다(예: `\d{100,}`).
- 대소문자 구분 안 함 – 패턴의 일부를 대소문자를 구분하지 않도록 하려면 `/i` 플래그 대신 `(?i)` 구성을 사용할 수 있습니다.
- 성능 – 접두사나 대체를 수동으로 최적화할 필요가 없습니다. 예를 들어 `/h(?:ello|i|ey)/`를 `/hello|hi|hey/`로 변경해도 성능이 향상되지 않습니다.
- 와일드카드 – 성능상의 이유로 Macie는 반복되는 와일드카드 수를 제한합니다. 예를 들어, Macie에서는 `a*b*a*` 컴파일되지 않습니다.

형식이 잘못되었거나 오래 실행되는 식을 방지하기 위해 Macie는 샘플 텍스트 모음을 기준으로 정규식 패턴을 자동으로 테스트합니다.

Amazon Macie 허용 목록을 사용하여 민감한 데이터 예외사항 정의

Amazon Macie의 허용 목록에서, 특정 텍스트 또는 텍스트 패턴을 정의하여 Macie가 Amazon Simple Storage Service(S3) 객체에서 민감한 데이터를 검사할 때 무시하도록 할 수 있습니다. 이는 일반적으로 특정 시나리오나 환경에 대한 민감한 데이터 예외사항입니다. 데이터가 허용 목록의 텍스트 또는 텍스트 패턴과 일치하는 경우 Macie는 데이터가 관리형 데이터 식별자 또는 사용자 정의 데이터 식별자의 기준과 일치하더라도 데이터를 보고하지 않습니다. 허용 목록을 사용하면 Amazon S3 데이터 분석을 세분화하고 노이즈를 줄일 수 있습니다.

Macie에서 두 가지 유형의 허용 목록을 만들고 사용할 수 있습니다.

- 사전 정의된 텍스트 - 이 유형의 목록에서는 조직의 공공 담당자 이름, 특정 전화번호 또는 조직에서 테스트에 사용하는 특정 샘플 데이터 등 무시할 특정 문자 시퀀스를 지정합니다. 이 유형의 목록을 사용하면 Macie는 목록의 항목과 정확히 일치하는 텍스트를 무시합니다.

  이 유형의 허용 목록에는 일반적으로 단어, 구문 및 민감하지 않고 변경되지 않을 뿐 아니라 반드시 일반 패턴을 따르지 않는 기타 유형의 문자 시퀀스를 지정하고 싶지 않을 때 유용합니다.
- 정규 표현식 - 이 유형의 목록에는 무시할 텍스트 패턴을 정의하는 정규 표현식(regex)을 지정합니다. 예를 들어, 조직의 공용 전화번호, 조직 도메인의 이메일 주소, 조직에서 테스트에 사용하는 패턴화된 샘플 데이터 등이 있습니다. 이 유형의 목록을 사용하는 경우 Macie는 목록에서 정의하는 패턴과 완전히 일치하는 텍스트를 무시합니다.

이 유형의 허용 목록은 민감하지는 않지만 다르거나 공통 패턴을 준수하면서 변경될 가능성이 있는 텍스트를 지정하려는 경우에 유용합니다.

허용 목록을 생성한 후, 목록을 사용하도록 민감한 데이터 검색 작업을 만들고 구성하거나 계정의 민감한 데이터 자동 검색 설정에 목록을 추가할 수 있습니다. 그런 다음, Macie는 데이터를 분석할 때 해당 목록을 사용합니다. Macie는 허용 목록의 항목 또는 패턴과 일치하는 텍스트를 발견한 경우 민감한 데이터 조사 결과, 통계 및 기타 유형의 결과에서 해당 텍스트가 발생했다고 보고하지 않습니다.

아시아 태평양(오사카) 리전을 제외하고 Macie를 현재 이용할 수 있는 모든 AWS 리전에서 허용 목록을 생성하고 사용할 수 있습니다.

주제

Amazon Macie의 허용 목록 옵션 및 요구 사항

Amazon Macie에서 허용 목록을 사용하여 Macie가 Amazon Simple Storage Service(S3) 객체의 민감한 데이터를 검사할 때 무시할 텍스트 또는 텍스트 패턴을 지정할 수 있습니다. Macie는 사전 정의된 텍스트와 정규 표현식이라는 두 가지 유형의 허용 목록에 대한 옵션을 제공합니다.

사전 정의된 텍스트 목록은 Macie가 민감할 것으로 간주되지 않는 특정 단어, 구 및 기타 유형의 문자 시퀀스를 무시하도록 하는 경우에 유용합니다. 가령, 조직의 공식 담당자 이름, 특정 전화번호 또는 조직에서 테스트에 사용하는 특정 샘플 데이터 등이 있습니다. Macie가 관리 데이터 식별자 또는 사용자 지정 데이터 식별자의 기준과 일치하는 텍스트를 찾았으며 해당 텍스트가 허용 목록의 항목과도 일치하는 경우 Macie는 민감한 데이터 결과, 통계 및 기타 유형의 결과에서 해당 텍스트가 발생했다고 보고하지 않습니다.

정규 표현식(정규식)은 Macie가 다르거나 변경될 가능성이 있는 텍스트를 무시하고 공통 패턴을 준수하도록 하려는 경우에 유용합니다. 정규식은 무시할 텍스트 패턴을 지정합니다. 가령, 조직의 공용 전화번호, 조직 도메인의 이메일 주소 또는 조직에서 테스트할 때 사용하는 패턴화된 샘플 데이터 등이 있습니다. Macie가 관리 데이터 식별자 또는 사용자 지정 데이터 식별자의 기준과 일치하는 텍스트를 발견하고 해당 텍스트가 허용 목록의 정규식 패턴과도 일치하는 경우 Macie는 민감한 데이터 결과, 통계 및 기타 유형의 결과에서 해당 텍스트가 발생했다고 보고하지 않습니다.

아시아 태평양 (오사카) 지역을 제외하고 현재 Macie를 사용할 수 AWS 리전 있는 모든 지역에서 두 가지 유형의 허용 목록을 생성하여 사용할 수 있습니다. 허용 목록을 생성하고 관리할 때는 다음 옵션과 요구 사항을 염두에 두세요. 또한 우편 주소의 허용 목록 항목 및 정규식 패턴은 지원되지 않습니다.

주제

사전 정의된 텍스트 목록의 옵션 및 요구 사항

이 유형의 허용 목록의 경우, 무시할 특정 문자 시퀀스가 나열된 행으로 구분된 일반 텍스트 파일을 제공합니다. 목록 항목은 일반적으로 단어, 구문 및 민감하다고 생각하지 않고 변경될 가능성이 없을 뿐 아니라 반드시 일반 패턴을 따르지 않아도 되는 기타 유형의 문자 시퀀스입니다. 이 유형의 목록을 사용하는 경우, Amazon Macie는 목록의 항목과 정확히 일치하는 텍스트를 보고하지 않습니다. Macie는 각 목록 항목을 문자열 리터럴 값으로 취급합니다.

이 유형의 허용 목록을 사용하려면 먼저 텍스트 편집기에서 목록을 만든 다음 일반 텍스트 파일로 저장합니다. 그런 다음 목록을 S3 범용 버킷에 업로드합니다. 또한 버킷과 객체의 스토리지 및 암호화 설정에서 Macie가 목록을 검색하고 해독할 수 있도록 해야 합니다. 그런 다음 Macie에서 목록에 대한 설정을 생성하고 구성합니다.

Macie에서 설정을 구성한 후에는 계정이나 조직의 대표적인 작은 데이터 집합을 사용하여 허용 목록을 테스트하는 것이 좋습니다. 목록을 테스트하려면 일회성 작업을 만들고 데이터 분석에 일반적으로 사용하는 관리 데이터 식별자 및 사용자 지정 데이터 식별자 외에도 목록을 사용하도록 작업을 구성할 수 있습니다. 그런 다음 민감한 데이터 조사 결과, 민감한 데이터 검색 결과 또는 둘 다와 같은 작업 결과를 검토할 수 있습니다. 작업 결과가 예상과 다를 경우, 결과가 예상과 다를 때까지 목록을 변경하고 테스트할 수 있습니다.

허용 목록 구성 및 테스트를 완료한 후에는 허용 목록을 사용할 추가 작업을 만들고 구성하거나 계정의 민감한 데이터 자동 검색 설정에 추가할 수 있습니다. 이러한 작업이 실행되거나 다음 자동 검색 분

석 주기가 시작되면 Macie는 Amazon S3에서 최신 버전의 목록을 검색하여 임시 메모리에 저장합니다. 그러면 Macie는 S3 객체의 민감한 데이터를 검사할 때 이 임시 목록 사본을 사용합니다. 작업 실행이 끝나거나 분석 주기가 완료되면 Macie는 목록 사본을 메모리에서 영구적으로 삭제합니다. 목록은 Macie에 유지되지 않습니다. 목록의 설정만 Macie에서 유지됩니다.

> **Important**
>
> 미리 정의된 텍스트 목록은 Macie에서 유지되지 않으므로 정기적으로 허용 목록의 상태를 확인하는 것이 중요합니다. 작업이나 자동 검색을 사용하도록 구성한 목록을 Macie가 검색하거나 분석할 수 없는 경우, Macie는 해당 목록을 사용하지 않습니다. 이 경우, 목록에서 지정한 텍스트의 민감한 데이터가 발견되는 등 예상치 못한 결과가 발생할 수 있습니다.

주제

- 구문 요구 사항
- 스토리지 요구 사항
- 암호화/복호화 요구 사항
- 설계 고려 사항 및 권장 사항

구문 요구 사항

이 유형의 허용 목록을 생성할 때는 목록 파일에 대한 다음 요구 사항을 참고하세요.

- 목록은 .txt, .text 또는 .plain 파일과 같은 일반 텍스트(`text/plain`) 파일로 저장해야 합니다.
- 목록은 줄 바꿈을 사용하여 개별 항목을 구분해야 합니다. 예:

```
Akua Mansa
John Doe
Martha Rivera
425-555-0100
425-555-0101
425-555-0102
```

  Macie는 각 행을 목록에서 별개의 단일 항목으로 취급합니다. 가독성을 높이기 위해 파일에 빈 행을 포함할 수도 있습니다. Macie는 파일을 분석할 때 빈 행을 건너뜁니다.
- 각 항목은 1~90개의 UTF-8 문자를 포함할 수 있습니다.

- 텍스트가 무시되려면 각 항목이 완전하고 정확히 일치해야 합니다. Macie는 항목에 와일드카드 문자나 부분 값 사용을 지원하지 않습니다. Macie는 각 항목을 문자열 리터럴 값으로 취급합니다. 일치는 대/소문자를 구분하지 않습니다.
- 파일에는 1~100,000개의 항목이 포함될 수 있습니다.
- 파일의 총 저장 크기는 35MB를 초과할 수 없습니다.

스토리지 요구 사항

Amazon S3에서 허용 목록을 추가하고 관리할 때 다음 스토리지 요구 사항 및 권장 사항을 참고하세요.

- 지역 지원 — 허용 목록은 Macie 계정과 AWS 리전 동일한 버킷에 저장해야 합니다. Macie는 허용 목록이 다른 리전에 저장되어 있는 경우, 허용 목록에 액세스할 수 없습니다.
- 버킷 소유권 — 허용 목록은 자신이 소유한 버킷에 저장해야 합니다. AWS 계정다른 계정에서도 동일한 허용 목록을 사용하게 하려면 Amazon S3 복제 규칙을 생성하여 해당 계정이 소유한 버킷에 목록을 복제하는 것을 고려해 보십시오. S3 객체 복제에 대한 정보는 Amazon Simple Storage Service 사용 설명서의 객체 복제를 참조하세요.

  또한 AWS Identity and Access Management (IAM) ID에는 목록을 저장하는 버킷과 객체에 대한 읽기 권한이 있어야 합니다. 그렇지 않으면 Macie를 사용하여 목록 설정을 생성 또는 업데이트하거나 목록 상태를 확인할 수 없습니다.
- 스토리지 유형 및 클래스 - 허용 목록은 디렉터리 버킷이 아닌 범용 버킷에 저장해야 합니다. 또한 RRS (리듀던시), S3 Glacier 인스턴트 검색, S3 인텔리전트 티어링, S3 원 존-IA, S3 스탠다드 또는 S3 스탠다드-IA 스토리지 클래스 중 하나를 사용하여 저장해야 합니다.
- 버킷 정책 - 제한적인 버킷 정책이 있는 버킷에 허용 목록을 저장하는 경우, 정책에서 Macie가 목록을 검색할 수 있도록 허용하는지 확인하십시오. 이를 위해 Macie 서비스 연결 역할에 대한 조건을 버킷 정책에 추가할 수 있습니다. 자세한 정보는 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을 참조하세요.

  또한 정책에서 IAM ID가 버킷에 대한 읽기 액세스 권한을 갖도록 허용하는지 확인합니다. 그렇지 않으면 Macie를 사용하여 목록 설정을 생성 또는 업데이트하거나 목록 상태를 확인할 수 없습니다.
- 객체 경로 - Amazon S3에 하나 이상의 허용 목록을 저장하는 경우, 각 목록의 객체 경로는 고유해야 합니다. 즉, 각 허용 목록은 고유한 S3 객체로 별도로 저장해야 합니다.
- 버전 관리 - 허용 목록을 버킷에 추가할 때는 해당 버킷의 버전 관리도 활성화하는 것이 좋습니다. 그런 다음 날짜 및 시간 값을 사용하여 목록 버전을 민감한 데이터 검색 작업 및 해당 목록을 사용하는

자동화된 민감한 데이터 검색 주기의 결과와 상호 연관시킬 수 있습니다. 이는 수행하는 데이터 개인 정보 보호 및 보호 감사 또는 조사에 도움이 될 수 있습니다.

- 객체 잠금 - 허용 목록이 일정 기간 또는 무기한으로 삭제되거나 덮어쓰여지지 않도록 하려면 목록을 저장하는 버킷에 대해 객체 잠금을 활성화할 수 있습니다. 이 설정을 활성화해도 Macie가 목록에 액세스하는 것을 막을 수는 없습니다. 이 설정에 대한 정보는 Amazon Simple Storage Service 사용 설명서의 Amazon S3 객체 잠금 사용을 참조하세요.

암호화/복호화 요구 사항

Amazon S3에서 허용 목록을 암호화하는 경우, Macie 서비스 연결 역할에 대한 권한 정책은 일반적으로 Macie에게 목록을 해독하는 데 필요한 권한을 부여합니다. 하지만 사용되는 암호화 유형에 따라 달라질 수 있습니다.

- Amazon S3 관리 키 (SSE-S3) 를 사용한 서버 측 암호화를 사용하여 목록을 암호화하는 경우 Macie는 목록을 해독할 수 있습니다. Macie 계정의 서비스 연결 역할은 Macie에게 필요한 권한을 부여합니다.
- AWS 관리형 AWS KMS key (DSSE-KMS 또는 SSE-KMS) 을 사용한 서버 측 암호화를 사용하여 목록을 암호화한 경우 Macie는 목록을 해독할 수 있습니다. Macie 계정의 서비스 연결 역할은 Macie에게 필요한 권한을 부여합니다.
- 고객이 관리하는 서버 측 암호화 AWS KMS key (DSSE-KMS 또는 SSE-KMS) 를 사용하여 목록을 암호화하는 경우 Macie가 키를 사용하도록 허용한 경우에만 Macie가 목록을 해독할 수 있습니다. 이 작업을 수행하는 방법은 Macie가 고객 관리형을 사용할 수 있도록 허용 AWS KMS key 단원을 참조하십시오.

> **Note**
>
> 외부 키 저장소에서 관리하는 고객과 함께 목록을 암호화할 수 있습니다. AWS KMS key 하지만 이 키는 AWS KMS내에서 완전히 관리되는 키보다 속도가 느리고 안정성이 떨어질 수 있습니다. 지연 시간이나 가용성 문제로 인해 Macie가 목록을 해독할 수 없는 경우, Macie는 S3 객체를 분석할 때 목록을 사용하지 않습니다. 이 경우, 목록에서 지정한 텍스트의 민감한 데이터가 발견되는 등 예상치 못한 결과가 발생할 수 있습니다. 이러한 위험을 줄이려면 키를 S3 버킷 키로 사용하도록 구성된 S3 버킷에 목록을 저장하는 것이 좋습니다.
> 외부 키 저장소에 있는 KMS 키 사용에 대한 정보는 AWS Key Management Service 개발자 가이드의 외부 키 저장소를 참조하십시오. S3 버킷 키 사용에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 버킷 키로 SSE-KMS 비용 절감을 참조하세요.

- 고객 입력식 키를 사용하는 서버 측 암호화(SSE-C) 또는 클라이언트 측 암호화를 사용하여 목록을 암호화하면 Macie는 목록을 해독할 수 없습니다. 대신 SSE-S3, DSSE-KMS 또는 SSE-KMS 암호화를 사용해 보세요.

목록이 AWS 관리형 KMS 키 또는 고객 관리형 KMS 키로 암호화된 경우 AWS Identity and Access Management (IAM) ID에도 키 사용을 허용해야 합니다. 그렇지 않으면 Macie를 사용하여 목록 설정을 생성 또는 업데이트하거나 목록 상태를 확인할 수 없습니다. KMS 키의 권한을 확인하거나 변경하는 방법을 알아보려면 AWS Key Management Service 개발자 안내서의 AWS KMS의 키 정책을 참조하세요.

Amazon S3 데이터의 암호화 옵션에 대한 자세한 내용은 Amazon Simple Storage 서비스 사용 설명서의 암호화를 통한 데이터 보호를 참조하십시오.

설계 고려 사항 및 권장 사항

일반적으로 Macie는 허용 목록의 각 항목을 문자열 리터럴 값으로 취급합니다. 즉, Macie는 허용 목록의 전체 항목과 정확히 일치하는 텍스트가 나올 때마다 무시합니다. 일치는 대/소문자를 구분하지 않습니다.

하지만 Macie는 항목을 대규모 데이터 추출 및 분석 프레임워크의 일부로 사용합니다. 프레임워크에는 문법 및 구문 변형, 대부분의 경우, 키워드 근접성과 같은 차원을 고려하는 기계 학습 및 패턴 매칭 함수가 포함되어 있습니다. 프레임워크는 S3 객체의 파일 유형이나 스토리지 형식도 고려합니다. 따라서 허용 목록에 항목을 추가하고 관리할 때는 다음 고려 사항 및 권장 사항을 염두에 두세요.

다양한 파일 유형 및 스토리지 형식 대비

Adobe Portable Document Format(.pdf) 파일의 텍스트와 같은 비정형 데이터의 경우, Macie는 여러 행 또는 페이지에 걸친 텍스트를 포함하여 허용 목록의 전체 항목과 정확히 일치하는 텍스트를 무시합니다.

CSV 파일의 열 형식 데이터나 JSON 파일의 레코드 기반 데이터와 같은 정형 데이터의 경우, Macie는 모든 텍스트가 단일 필드, 셀 또는 배열에 저장되어 있는 경우, 허용 목록의 전체 항목과 정확히 일치하는 텍스트를 무시합니다. .pdf 파일의 테이블과 같이 비정형 파일에 저장된 정형 데이터에는 이 요구 사항이 적용되지 않습니다.

예를 들어 CSV 파일의 다음 콘텐츠를 고려합니다.

```
Name,Account ID
Akua Mansa,111111111111
```

```
John Doe,222222222222
```

Akua Mansa 및 John Doe가 허용 목록에 있는 항목인 경우, Macie는 CSV 파일에서 해당 이름을 무시합니다. 각 목록 항목의 전체 텍스트는 단일 Name 필드에 저장됩니다.

반대로, 다음과 같은 열과 필드가 포함된 CSV 파일을 고려해 보세요.

```
First Name,Last Name,Account ID
Akua,Mansa,111111111111
John,Doe,222222222222
```

Akua Mansa 및 John Doe가 허용 목록에 있는 항목인 경우, Macie는 CSV 파일에서 해당 이름을 무시하지 않습니다. CSV 파일의 모든 필드에는 허용 목록에 있는 항목의 전체 텍스트가 포함되지 않습니다.

일반적인 변형 포함

숫자 데이터, 고유 명사, 용어, 영숫자 문자 순서의 일반적인 변형에 대한 항목을 추가합니다. 예를 들어 단어 사이에 스페이스가 한 개만 포함된 이름이나 구를 추가하는 경우, 단어 사이에 두 개의 스페이스가 포함된 변형도 추가할 수 있습니다. 마찬가지로 특수 문자를 포함하거나 포함하지 않는 단어와 구문을 추가하고 일반적인 구문 및 의미 변형을 포함하는 것도 고려해 보세요.

예를 들어 미국 전화번호 425-555-0100의 경우, 다음 항목을 허용 목록에 추가할 수 있습니다.

```
425-555-0100
425.555.0100
(425) 555-0100
+1-425-555-0100
```

다국적 상황에서 2022년 2월 1일의 경우, 특수 문자를 포함하거나 포함하지 않는 변형을 포함하여 영어와 프랑스어의 일반적인 구문 변형이 포함된 항목을 추가할 수 있습니다.

```
February 1, 2022
1 février 2022
1 fevrier 2022
Feb 01, 2022
1 fév 2022
1 fev 2022
02/01/2022
01/02/2022
```

인물 이름에는 민감하지 않다고 생각되는 다양한 형태의 이름을 입력할 수 있습니다. 예를 들어 이름 뒤에 성, 성 다음에 이름, 한 스페이스로 구분된 성과 이름, 두 스페이스로 구분된 성과 이름, 닉네임 등을 포함하세요.

예를 들어 Martha Rivera라는 이름의 경우, 다음을 추가할 수 있습니다.

```
Martha Rivera
Martha  Rivera
Rivera, Martha
Rivera,  Martha
Rivera Martha
Rivera  Martha
```

여러 부분이 포함된 특정 이름의 변형을 무시하려면 정규 표현식을 대신 사용하는 허용 목록을 만드십시오. 예를 들어 Martha Lyda Rivera 박사, PhD라는 이름에는 다음과 같은 정규 표현식을 사용할 수 있습니다: `^(Dr. )?Martha\s(Lyda|L\.)?\s?Rivera,?( PhD)?$`.

허용 목록의 정규 표현식에 대한 옵션 및 요구 사항

이 유형의 허용 목록의 경우, 무시할 텍스트 패턴을 정의하는 정규 표현식(정규식)을 지정합니다. 예를 들어 조직의 공용 전화 번호, 조직 도메인의 전자 메일 주소 또는 조직에서 테스트에 사용하는 패턴화된 샘플 데이터 등이 이에 해당합니다. 정규식은 민감하지 않다고 생각되는 특정 종류의 데이터에 대한 공통 패턴을 정의합니다. 이 유형의 허용 목록을 사용하는 경우, Amazon Macie는 지정된 패턴과 완전히 일치하는 텍스트의 발생을 보고하지 않습니다. 미리 정의된 무시할 텍스트가 있는 허용 목록과 달리 Macie에서 정규식 및 기타 모든 목록 설정을 생성하고 저장합니다.

이 유형의 허용 목록을 만들거나 업데이트할 때 목록을 저장하기 전에 샘플 데이터로 목록의 정규식을 테스트할 수 있습니다. 여러 개의 샘플 데이터 세트를 사용하여 이 작업을 수행하는 것이 좋습니다. 너무 일반적인 정규식을 만들면, Macie는 민감하다고 생각되는 텍스트의 발생을 무시할 수 있습니다. 정규식이 너무 구체적일 경우, Macie는 사용자가 민감하다고 생각하지 않는 텍스트의 발생을 무시할 수 있습니다. 또한 형식이 잘못되었거나 오래 실행되는 표현식을 방지하기 위해 Macie는 샘플 텍스트 컬렉션에 대해 자동으로 정규식을 컴파일하고 테스트하여 해결해야 할 문제를 알려줍니다.

추가 테스트를 위해 계정이나 조직의 대표적인 작은 데이터 집합을 사용하여 목록의 정규식을 테스트하는 것이 좋습니다. 이렇게 하려면 일회성 작업을 만들고 데이터 분석에 일반적으로 사용하는 관리 데이터 식별자 및 사용자 지정 데이터 식별자 외에도 목록을 사용하도록 작업을 구성할 수 있습니다. 그런 다음 민감한 데이터 조사 결과, 민감한 데이터 검색 결과 또는 둘 다와 같은 작업 결과를 검토할 수 있습니다. 작업 결과가 예상과 다를 경우, 결과가 예상과 다를 때까지 정규식을 변경하고 테스트할 수 있습니다.

허용 목록을 구성 및 테스트한 후 이를 사용할 추가 작업을 생성 및 구성하거나 계정의 자동 민감 데이터 검색 설정에 추가할 수 있습니다. 이러한 작업이 실행되거나 Macie가 계정에 대한 자동 검색을 수행하면 Macie는 최신 버전의 목록 정규식을 사용하여 데이터를 분석합니다.

주제

구문 지원 및 권장 사항

허용 목록은 최대 512자를 포함하는 정규 표현식(정규식)을 지정할 수 있습니다. Macie는 펄 호환 정규 표현식(PCRE) 라이브러리에서 제공하는 정규식 패턴 구문의 하위 집합을 지원합니다. PCRE 라이브러리에서 제공하는 구문 중에서 Macie는 다음 패턴 요소를 지원하지 않습니다.

- 역참조
- 캡처 그룹
- 조건 패턴
- 임베디드 코드
- 글로벌 패턴 플래그(예: `/i`, `/m` 및 `/x`)
- 재귀 패턴
- 포지티브 및 네가티브 후방탐색 및 전방탐색 제로 폭 어설션(예: `?=`, `?!`, `?<=` 및 `?<!`)

허용 목록에 효과적인 정규식 패턴을 만들려면 다음 팁과 권장 사항도 참고하세요.

- 앵커 - 패턴이 줄의 시작이나 끝이 아닌 파일의 시작이나 끝에 나타날 것으로 예상되는 경우에만 앵커(^ 또는 $)를 사용하십시오.
- 제한된 반복 - 성능상의 이유로 Macie는 제한된 반복 그룹의 크기를 제한합니다. 예를 들어, Macie에서는 `\d{100,1000}` 컴파일되지 않습니다. 다음과 같은 서술형 반복을 사용하면 이 함수의 근사치를 계산할 수 있습니다(예: `\d{100,}`).
- 대소문자 구분 안 함 - 패턴의 일부를 대소문자를 구분하지 않도록 하려면 `/i` 플래그 대신 `(?i)` 구성을 사용할 수 있습니다.
- 성능 - 접두사나 대체를 수동으로 최적화할 필요가 없습니다. 예를 들어 `/h(?:ello|i|ey)/`를 `/hello|hi|hey/`로 변경해도 성능이 향상되지 않습니다.
- 와일드카드 - 성능상의 이유로 Macie는 반복되는 와일드카드 수를 제한합니다. 예를 들어, Macie에서는 `a*b*a*` 컴파일되지 않습니다.

- 대체 - 단일 허용 목록에서 둘 이상의 패턴을 지정하려면 대체 연산자(|)를 사용하여 패턴을 연결할 수 있습니다. 이렇게 하면 Macie는 OR 논리를 사용하여 패턴을 결합하여 새 패턴을 형성합니다. 예를 들어 `(apple|orange)`을 지정하는 경우, Macie는 사과와 오렌지를 모두 일치하는 것으로 인식하고 두 단어의 발생 빈도는 무시합니다. 패턴을 연결하는 경우, 연결된 표현식의 전체 길이를 512자 이하로 제한해야 합니다.

마지막으로, 정규식을 개발할 때는 다양한 파일 유형과 저장소 형식을 수용하도록 정규식을 설계해야 합니다. Macie는 대규모 데이터 추출 및 분석 프레임워크의 일부로 정규식을 사용합니다. 프레임워크는 S3 객체의 파일 유형 또는 스토리지 형식을 고려합니다. CSV 파일의 열 형식 데이터나 JSON 파일의 레코드 기반 데이터와 같은 정형 데이터의 경우, Macie는 모든 텍스트가 단일 필드, 셀 또는 배열에 저장된 경우에만 패턴과 완전히 일치하는 텍스트를 무시합니다. 이 요구 사항은 Adobe Portable Document Format(.pdf) 파일의 표와 같이 비정형 파일에 저장된 정형 데이터에는 적용되지 않습니다. .pdf 파일의 텍스트와 같은 비정형 데이터의 경우, Macie는 패턴과 완전히 일치하는 텍스트(예: 여러 줄 또는 페이지에 걸친 텍스트 포함)는 무시합니다.

예제

다음 예는 몇 가지 일반적인 시나리오에 적합한 정규식 패턴을 보여줍니다.

이메일 주소

사용자 지정 데이터 식별자를 사용하여 이메일 주소를 탐지하는 경우, 조직의 이메일 주소와 같이 민감하다고 간주되지 않는 이메일 주소는 무시해도 됩니다.

특정 2단계 및 최상위 도메인의 이메일 주소를 무시하려면 다음 패턴을 사용할 수 있습니다.

```
[a-zA-Z0-9_.+\\-]+@example\.com
```

여기서 *example*은 2단계 도메인의 이름이고 *com*은 최상위 도메인입니다. 이 경우, Macie는 johndoe@example.com 및 john.doe@example.com 같은 주소를 일치시키고 무시합니다.

.com 또는 .gov와 같은 일반 최상위 도메인(gTLD)에서 특정 도메인의 이메일 주소를 무시하려면 다음 패턴을 사용할 수 있습니다.

```
[a-zA-Z0-9_.+\\-]+@example\.[a-zA-Z]{2,}
```

여기에서 *example*은 도메인의 이름입니다. 이 경우, Macie는 johndoe@example.com, john.doe@example.gov 및 johndoe@example.edu 같은 주소를 일치시키고 무시합니다.

캐나다의 경우, .ca 또는 호주의 경우, .au와 같이 단일 국가 코드 최상위 도메인(ccTLD)에 있는 특정 도메인의 이메일 주소를 무시하려면 다음 패턴을 사용할 수 있습니다.

```
[a-zA-Z0-9_.+\\-]+@example\.(ca|au)
```

여기에서 *example*은 도메인의 이름이고 *ca*와 *au*는 무시할 특정 ccTLD입니다. 이 경우, Macie는 johndoe@example.ca 및 john.doe@example.au 같은 주소를 일치시키고 무시합니다.

특정 도메인과 gTLD의 이메일 주소를 무시하고 3단계 및 4단계 도메인을 포함하려면 다음 패턴을 사용할 수 있습니다.

```
[a-zA-Z0-9_.+\\-]+@([a-zA-Z0-9-]+\.)?[a-zA-Z0-9-]+\.example\.com
```

여기에서 *example*은 도메인 이름이고 *com*은 gTLD입니다. 이 경우, Macie는 johndoe@www.example.com 및 john.doe@www.team.example.com 같은 주소를 일치시키고 무시합니다.

전화 번호

Macie는 여러 국가 및 지역의 전화번호를 감지할 수 있는 관리형 데이터 식별자를 제공합니다. 조직의 무료 전화번호나 공용 전화번호와 같은 특정 전화번호를 무시하려면 다음과 같은 패턴을 사용하면 됩니다.

수신자 부담 전화를 무시하려면 800 지역 번호를 사용하는 (800) ###-#### 형식인 미국 전화 번호:

```
^\(?800\)?[ -]?\d{3}[ -]?\d{4}$
```

수신자 부담 전화를 무시하려면 888 지역 번호를 사용하는 (888) ###-#### 형식인 미국 전화 번호:

```
^\(?888\)?[ -]?\d{3}[ -]?\d{4}$
```

10자리 숫자를 무시하려면 33 국가 번호가 포함된 +33 ## ## ## ## ## 형식인 프랑스 전화번호:

```
^\+33 \d( \d\d){4}$
```

특정 지역 및 교환 코드를 사용하는 미국 및 캐나다 전화번호를 무시하려면 (###) ###-#### 형식으로 된 국가 번호를 포함하지 마십시오.

```
^\(?123\)?[ -]?555[ -]?\d{4}$
```

여기에서 *123*은 지역 번호이고 *555*는 교환 번호입니다.

특정 지역 및 교환 코드를 사용하는 미국 및 캐나다 전화번호를 무시하려면 +1 (###) ###-#### 형식으로 된 국가 번호를 포함합니다.

```
^\+1\(?123\)?[ -]?555[ -]?\d{4}$
```

여기에서 *123*은 지역 번호이고 *555*는 교환 번호입니다.

Amazon Macie에서 허용 목록 생성 및 관리

Amazon Macie에서 허용 목록은 특정 텍스트 또는 텍스트 패턴을 정의하여 Macie가 Amazon Simple Storage Service(S3) 객체에서 민감한 데이터를 검사할 때 무시하도록 할 수 있습니다. 데이터가 허용 목록의 항목 또는 패턴과 일치하는 경우, Macie는 텍스트가 관리형 데이터 식별자 또는 사용자 지정 데이터 식별자의 기준과 일치하더라도 민감한 데이터 조사 결과, 통계 또는 기타 유형의 결과에서 해당 텍스트를 보고하지 않습니다.

Macie에서 다음 유형의 허용 목록을 만들고 관리할 수 있습니다.

사전 정의된 텍스트

이 유형의 목록을 사용하여 민감하지 않고 변경될 가능성이 없으며 반드시 일반적인 패턴을 따르지 않는 단어, 구문 및 기타 종류의 문자 시퀀스를 지정할 수 있습니다. 가령, 조직의 공식 담당자 이름, 특정 전화번호, 조직에서 테스트에 사용하는 특정 샘플 데이터 등이 있습니다. 이 유형의 목록을 사용하면 Macie는 목록의 항목과 정확히 일치하는 텍스트를 무시합니다.

이 유형의 목록의 경우, 무시할 특정 텍스트를 나열하는 줄 바꿈으로 구분된 일반 텍스트 파일을 만듭니다. 이후 파일을 S3 버킷에 저장하고 Macie가 버킷의 목록에 액세스할 수 있도록 설정을 구성합니다. 그런 다음 해당 목록을 사용하도록 민감한 데이터 검색 작업을 만들고 구성하거나 계정의 민감한 데이터 자동 검색 설정에 목록을 추가할 수 있습니다. 각 작업이 실행되기 시작하거나 다음 자동 검색 분석 주기가 시작되면, Macie는 Amazon S3에서 최신 버전의 목록을 검색합니다. 그런 다음, Macie는 S3 객체의 민감한 데이터를 검사할 때 해당 버전의 목록을 사용합니다. Macie가 목록의 항목과 정확히 일치하는 텍스트를 발견하는 경우, Macie는 해당 텍스트를 민감한 데이터로 보고하지 않습니다.

정규식

이 유형의 목록을 사용하여 무시할 텍스트 패턴을 정의하는 정규 표현식(정규식)을 지정할 수 있습니다. 가령, 조직의 공용 전화번호, 조직 도메인의 이메일 주소, 조직에서 테스트할 때 사용하는 패턴화된 샘플 데이터 등이 있습니다. 이 유형의 목록을 사용하는 경우, Macie는 목록에서 정의된 정규식 패턴과 완전히 일치하는 텍스트는 무시합니다.

이 유형의 목록의 경우, 민감하지는 않지만 다양하거나 변경될 가능성이 있는 텍스트에 대한 공통 패턴을 정의하는 정규식을 생성합니다. 사전 정의된 텍스트용 목록과 달리, 정규식 및 기타 모든 목록 설정을 Macie에 생성하고 저장합니다. 그런 다음 해당 목록을 사용하도록 민감한 데이터 검색

작업을 만들고 구성하거나 계정의 민감한 데이터 자동 검색 설정에 목록을 추가할 수 있습니다. 이러한 작업이 실행되거나 Macie가 계정에 대한 자동 검색을 수행하면 Macie는 최신 버전의 목록 정규식을 사용하여 데이터를 분석합니다. Macie가 목록에 정의된 패턴과 완전히 일치하는 텍스트를 발견하는 경우, Macie는 해당 텍스트를 민감한 데이터로 보고하지 않습니다.

각 목록 유형에 대한 자세한 요구 사항, 권장 사항 및 예는 허용 목록 옵션 및 요구 사항을 참조하십시오. 지원되는 각 계정에서 최대 10개의 허용 목록을 만들 수 있으며 AWS 리전, 미리 정의된 텍스트를 지정하는 허용 목록은 최대 5개, 정규 표현식을 지정하는 허용 목록은 최대 5개까지 만들 수 있습니다. 아시아 태평양 (오사카) 지역을 제외하고 현재 Macie를 사용할 수 AWS 리전 있는 모든 지역에서 허용 목록을 생성하여 사용할 수 있습니다.

허용 목록을 생성하고 관리하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 다음 주제에서는 방법을 설명합니다. API의 경우 항목에는 AWS Command Line Interface (AWS CLI) 를 사용하여 이러한 작업을 수행하는 방법에 대한 예가 포함되어 있습니다. 최신 버전의 다른 AWS 명령줄 도구 또는 AWS SDK를 사용하거나 HTTPS 요청을 Macie에 직접 전송하여 이러한 작업을 수행할 수도 있습니다. AWS 도구 및 SDK에 대한 자세한 내용은 빌드할 도구를 참조하십시오. AWS

주제

- 허용 목록 생성
- 허용 목록의 상태 확인
- 허용 목록 변경
- 허용 목록 삭제

허용 목록 생성

Amazon Macie에서 허용 목록을 생성하는 방법은 생성하려는 목록 유형에 따라 다릅니다. 허용 목록은 무시할 사전 정의된 텍스트를 나열하는 파일일 수도 있고, 무시할 텍스트 패턴을 정의하는 정규 표현식(정규식)일 수 있습니다. 생성하려는 목록 유형에 해당하는 섹션을 선택합니다.

사전 정의된 텍스트

Macie에서 이러한 유형의 허용 목록을 생성하기 전에 다음 단계를 수행합니다.

1. 텍스트 편집기를 사용하여 무시할 특정 텍스트가 나열된 줄로 구분된 일반 텍스트 파일(예: .txt, .text 또는 .plain 파일)을 만듭니다. 자세한 정보는 사전 정의된 텍스트 목록의 구문 요구 사항을 참조하세요.

2. 파일을 S3 범용 버킷에 업로드하고 버킷 이름과 객체를 기록해 둡니다. Macie에서 정을 구성할 때 이러한 이름을 입력해야 합니다.
3. S3 버킷 및 객체 설정을 통해 사용자와 Macie와 함께 버킷에서 목록을 검색할 수 있는지 확인합니다. 자세한 정보는 사전 정의된 텍스트 목록의 스토리지 요구 사항을 참조하세요.
4. S3 객체를 암호화한 경우, 해당 객체가 사용자와 Macie와 사용할 수 있는 키로 암호화되어 있는지 확인해야 합니다. 자세한 정보는 사전 정의된 텍스트 목록에 대한 암호화/복호화 요구 사항을 참조하세요.

이 단계를 수행하면 Macie에서 목록 설정을 구성할 준비가 된 것입니다. Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 설정을 구성할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 허용 목록의 설정을 구성하려면 다음 단계를 따르십시오.

Macie에서 허용 목록 설정을 구성하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창의 설정에서 허용 목록을 선택합니다.
3. 허용 목록 페이지에서 생성을 선택합니다.
4. 목록 유형 선택에서 사전 정의된 텍스트를 선택합니다.
5. 목록 설정에서 다음 옵션을 사용하여 허용 목록에 대한 추가 설정을 입력합니다.
   - 이름에 목록의 이름을 입력합니다. 이름은 최대 128자까지 포함할 수 있습니다.
   - 설명에 선택 사항으로 간단한 설명을 입력합니다. 설명은 512자까지 포함할 수 있습니다.
   - S3 버킷 이름에 목록을 저장하는 버킷의 이름을 입력합니다.

     Amazon S3에서는 버킷 속성의 이름 필드에서 이 값을 찾을 수 있습니다. 이 값은 대소문자를 구분합니다. 추가로 이름에 와일드카드 문자나 부분 값을 입력하지 마십시오.
   - S3 객체 이름에는 목록을 저장하는 S3 객체의 이름을 입력합니다.

     Amazon S3에서는 객체 속성의 키 필드에서 이 값을 찾을 수 있습니다. 이름에 경로가 포함된 경우, 이름을 입력할 때 전체 경로(예: **`allowlists/macie/mylist.txt`**)를 입력해야 합니다. 이 값은 대소문자를 구분합니다. 추가로 이름에 와일드카드 문자나 부분 값을 입력하지 마십시오.
6. (선택 사항) 태그에서 태그 추가를 선택한 다음 허용 목록에 지정할 태그를 50개까지 입력합니다.

태그는 사용자가 정의하여 특정 유형의 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별, 분류, 관리하는 데 도움이 됩니다. 자세한 내용은 Amazon Macie에 리소스 태그 지정(을)를 참조하세요.

7. 마쳤으면 [생성]을 선택합니다.

Macie는 목록의 설정을 테스트합니다. 또한 Macie는 Amazon S3에서 목록을 검색하고 목록의 콘텐츠를 구문 분석할 수 있는지 확인합니다. 오류가 발생한 경우, Macie는 해당 오류를 설명하는 메시지를 표시합니다. 오류를 해결하는 데 도움이 되는 자세한 정보는 사전 정의된 텍스트 목록의 옵션 및 요구 사항을 참조하십시오. 오류를 해결한 후, 목록의 설정을 저장할 수 있습니다.

API

허용 목록 설정을 프로그래밍 방식으로 구성하려면 Amazon Macie API의 CreateAllowList작업을 사용하고 필수 파라미터에 적절한 값을 지정하십시오.

`criteria` 매개 변수에는 `s3WordsList` 객체를 사용하여 S3 버킷 이름(`bucketName`)과 목록을 저장하는 S3 객체(`objectKey`)의 이름을 지정합니다. 버킷 이름은 Amazon S3의 `Name` 필드를 참조하십시오. 객체 이름은 Amazon S3의 `Key` 필드를 참조하십시오. 이러한 값은 대소문자를 구분합니다. 추가로 이름을 지정할 때 와일드카드 문자나 부분 값을 사용하지 마십시오.

를 사용하여 설정을 구성하려면 create-allow-list명령을 실행하고 필요한 파라미터에 적합한 값을 지정합니다. AWS CLI다음 예제는 *`DOC-EXAMPLE-BUCKET`*이라는 이름의 S3 버킷에 저장된 허용 목록의 설정을 구성하는 방법입니다. 목록을 저장하는 S3 객체의 이름은 *`allowlists/macie/mylist.txt`*입니다.

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

```
$ aws macie2 create-allow-list \
--criteria '{"s3WordsList":{"bucketName":"DOC-EXAMPLE-
BUCKET","objectKey":"allowlists/macie/mylist.txt"}}' \
--name my_allow_list \
--description "Lists public phone numbers and names for Example Corp."
```

이 예제는 Microsoft Windows용으로 포맷되었으며 가독성을 높이기 위해 캐럿(^) 줄 연속 문자를 사용합니다.

```
C:\> aws macie2 create-allow-list ^
```

```
--criteria={\"s3WordsList\":{\"bucketName\":\"DOC-EXAMPLE-BUCKET\",\"objectKey\":
\"allowlists/macie/mylist.txt\"}} ^
--name my_allow_list ^
--description "Lists public phone numbers and names for Example Corp."
```

요청을 제출하면, Macie는 목록 설정을 테스트합니다. 또한 Macie는 Amazon S3에서 목록을 검색하고 목록의 콘텐츠를 구문 분석할 수 있는지 확인합니다. 오류가 발생하면 요청이 실패하고 Macie는 오류를 설명하는 메시지를 반환합니다. 오류를 해결하는 데 도움이 되는 자세한 정보는 사전 정의된 텍스트 목록의 옵션 및 요구 사항을 참조하십시오.

Macie가 목록을 검색하고 구문 분석할 수 있으면, 요청이 성공하고 다음과 비슷한 출력이 표시됩니다.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
nkr81bmtu2542yyexample",
    "id": "nkr81bmtu2542yyexample"
}
```

여기서 `arn`은 생성된 허용 목록의 Amazon 리소스 이름(ARN)이고, `id`는 목록의 고유 식별자입니다.

목록의 설정을 저장한 후에는, 이 목록을 사용하도록 민감한 데이터 검색 작업을 생성하고 구성하거나, 민감한 데이터 자동 검색 설정에 목록을 추가할 수 있습니다. 각 작업이 실행되기 시작하거나 다음 자동 검색 분석 주기가 시작될 때마다 Macie는 Amazon S3에서 최신 버전의 목록을 검색합니다. 그런 다음 Macie는 데이터를 분석할 때 해당 버전의 목록을 사용합니다.

정규식

정규 표현식(정규식)을 지정하는 허용 목록을 생성할 때, Macie에서 직접 정규식과 기타 모든 목록 설정을 정의합니다. Macie는 펄 호환 정규 표현식(PCRE) 라이브러리에서 제공하는 정규식 패턴 구문의 하위 집합을 지원합니다. 자세한 정보는 구문 지원 및 권장 사항을 참조하세요.

이러한 유형의 목록은 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 생성할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 허용 목록을 생성하려면 다음 단계를 따르세요.

허용 목록을 생성하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창의 설정에서 허용 목록을 선택합니다.
3. 허용 목록 페이지에서 생성을 선택합니다.
4. 목록 유형 선택에서 정규 표현식을 선택합니다.
5. 목록 설정에서 다음 옵션을 사용하여 허용 목록에 대한 추가 설정을 입력합니다.

   - 이름에 목록의 이름을 입력합니다. 이름은 최대 128자까지 포함할 수 있습니다.
   - 설명에 선택 사항으로 간단한 설명을 입력합니다. 설명은 512자까지 포함할 수 있습니다.
   - 정규 표현식의 경우, 무시할 텍스트 패턴을 정의하는 정규식(regex)을 입력합니다. Regex는 최대 512자까지 포함할 수 있습니다.
6. (선택 사항) 평가 시, 샘플 데이터 상자에 최대 1,000자를 입력한 다음 테스트를 선택하여 정규식을 테스트합니다. Macie는 샘플 데이터를 평가하여 정규식과 일치하는 텍스트의 발생 횟수를 보고합니다. 이 단계를 원하는 만큼 반복하여 정규식을 세분화하고 최적화할 수 있습니다.

   > **Note**
   >
   > 여러 샘플 데이터 세트를 사용하여 정규식을 테스트하고 수정하는 것이 좋습니다. 너무 일반적인 정규식을 만들면, Macie는 민감하다고 생각되는 텍스트의 발생을 무시할 수 있습니다. 정규식이 너무 구체적일 경우, Macie는 사용자가 민감하다고 생각하지 않는 텍스트의 발생을 무시할 수 있습니다.
7. (선택 사항) 태그에서 태그 추가를 선택한 다음 허용 목록에 지정할 태그를 50개까지 입력합니다.

   태그는 사용자가 정의하여 특정 유형의 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별, 분류, 관리하는 데 도움이 됩니다. 자세한 내용은 Amazon Macie에 리소스 태그 지정(을)를 참조하세요.
8. 마쳤으면 [생성]을 선택합니다.

Macie는 목록의 설정을 테스트합니다. Macie는 또한 정규식을 테스트하여 표현식을 컴파일할 수 있는지 확인합니다. 오류가 발생한 경우, Macie는 해당 오류를 설명하는 메시지를 표시합니다. 오류를 해결하는 데 도움이 되는 자세한 정보는 허용 목록의 정규 표현식에 대한 옵션 및 요구 사항을 참조하십시오. 오류를 해결한 후 허용 목록을 저장할 수 있습니다.

API

Macie에서 이러한 유형의 허용 목록을 만들기 전에 여러 샘플 데이터 세트를 사용하여 정규 표현식을 테스트하고 수정하는 것이 좋습니다. 너무 일반적인 정규식을 만들면, Macie는 민감하다고 생각되는 텍스트의 발생을 무시할 수 있습니다. 정규식이 너무 구체적일 경우, Macie는 사용자가 민감하다고 생각하지 않는 텍스트의 발생을 무시할 수 있습니다.

Macie로 표현식을 테스트하려면 Amazon Macie API의 TestCustomDataIdentifier작업을 사용하거나 의 경우 AWS CLI명령을 실행할 test-custom-data-identifier수 있습니다. Macie는 동일한 기본 코드를 사용하여 허용 목록 및 사용자 지정 데이터 식별자에 대한 표현식을 컴파일합니다. 이러한 방식으로 표현식을 테스트하는 경우 `regex` 및 `sampleText` 매개 변수에 대한 값만 지정해야 합니다. 그렇지 않으면 부정확한 결과를 얻을 수 있습니다.

이 유형의 허용 목록을 생성할 준비가 되면 Amazon Macie API의 CreateAllowList작업을 사용하고 필수 파라미터에 적절한 값을 지정하십시오. `criteria` 매개 변수의 경우, `regex` 필드를 사용하여 무시할 텍스트 패턴을 정의하는 정규 표현식을 지정합니다. 표현식에는 512자까지 포함할 수 있습니다.

를 사용하여 이러한 유형의 목록을 생성하려면 create-allow-list명령을 실행하고 필수 파라미터에 적합한 값을 지정하십시오. AWS CLI다음 예제에서는 *my_allow_list*라는 이름의 허용 목록을 만듭니다. 이 정규식은 사용자 지정 데이터 식별자가 `example.com` 도메인에 대해 감지할 수 있는 모든 이메일 주소를 무시하도록 설계되었습니다.

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

```
$ aws macie2 create-allow-list \
--criteria '{"regex":"[a-z]@example.com"}' \
--name my_allow_list \
--description "Ignores all email addresses for Example Corp."
```

이 예제는 Microsoft Windows용으로 포맷되었으며 가독성을 높이기 위해 캐럿(^) 줄 연속 문자를 사용합니다.

```
C:\> aws macie2 create-allow-list ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--name my_allow_list ^
--description "Ignores all email addresses for Example Corp."
```

요청을 제출하면, Macie는 목록 설정을 테스트합니다. Macie는 또한 정규식을 테스트하여 표현식을 컴파일할 수 있는지 확인합니다. 오류가 발생하면, 요청이 실패하고 Macie는 오류를 설명하는 메시지를 반환합니다. 오류를 해결하는 데 도움이 되는 자세한 정보는 허용 목록의 정규 표현식에 대한 옵션 및 요구 사항을 참조하십시오.

Macie가 표현식을 컴파일할 수 있으면, 요청이 성공하고 다음과 유사한 출력이 표시됩니다.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

여기서 `arn`은 생성된 허용 목록의 Amazon 리소스 이름(ARN)이고, `id`는 목록의 고유 식별자입니다.

목록을 저장한 후에는, 이 목록을 사용하도록 민감한 데이터 검색 작업을 생성하고 구성하거나, 민감한 데이터 자동 검색 설정에 목록을 추가할 수 있습니다. 이러한 작업이 실행되거나 Macie가 계정에 대한 자동 검색을 수행하면 Macie는 최신 버전의 목록 정규식을 사용하여 데이터를 분석합니다.

허용 목록의 상태 확인

허용 목록의 상태를 정기적으로 확인하는 것이 중요합니다. 그렇지 않으면 오류로 인해 허용 목록에 지정한 텍스트에 대한 민감한 데이터 검색과 같은 예기치 않은 분석 결과가 Amazon Macie에서 생성될 수 있습니다.

허용 목록을 사용하도록 민감한 데이터 검색 작업을 구성했는데 작업이 실행되기 시작할 때 Macie가 해당 목록에 액세스하거나 목록을 사용할 수 없더라도 작업은 계속 실행됩니다. 하지만 Macie는 S3 객체를 분석할 때 이 목록을 사용하지 않습니다. 마찬가지로, 민감한 데이터 자동 검색을 위한 분석 주기가 시작되고 Macie가 지정된 허용 목록에 액세스하거나 이를 사용할 수 없는 경우에도 분석은 계속되지만 Macie는 해당 목록을 사용하지 않습니다.

정규 표현식(정규식)을 지정하는 허용 목록에서는 오류가 발생할 가능성이 거의 없습니다. 이는 목록 설정을 만들거나 업데이트할 때 Macie가 자동으로 정규식을 테스트하기 때문입니다. 또한 정규식 및 기타 모든 목록 설정을 Macie에 저장됩니다.

하지만 미리 정의된 텍스트를 지정하는 허용 목록에 오류가 발생할 수 있는데, 이는 부분적으로 목록을 Macie 대신 Amazon S3에 저장하기 때문입니다. 일반적인 오류 원인은 다음과 같습니다.

- S3 버킷 또는 객체를 삭제한 경우.

- S3 버킷 또는 객체의 이름이 변경되었지만 Macie의 목록 설정에 새 이름이 지정되지 않은 경우.
- S3 버킷의 권한 설정이 변경되고 Macie가 버킷 및 객체에 대한 액세스 권한을 상실한 경우.
- S3 버킷의 암호화 설정이 변경되어 Macie가 목록을 저장하는 객체의 암호를 해독할 수 없는 경우.
- 암호화 키에 대한 정책이 변경되어 Macie가 키에 대한 액세스 권한을 잃은 경우. Macie가 목록을 저장한 S3 객체를 해독할 수 없는 경우.

> **Important**
>
> 이러한 오류는 분석 결과에 영향을 미치므로 허용 목록의 상태를 주기적으로 확인하는 것이 좋습니다. 허용 목록을 저장하는 S3 버킷의 권한 또는 암호화 설정을 변경하거나 목록을 암호화하는 데 사용되는 AWS Key Management Service (AWS KMS) 키의 정책을 변경하는 경우에도 이 작업을 수행하는 것이 좋습니다.

허용 목록의 상태는 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 확인할 수 있습니다. 오류를 해결하는 데 도움이 되는 자세한 정보는 사전 정의된 텍스트 목록의 옵션 및 요구 사항을 참조하십시오.

Console

Amazon Macie 콘솔을 사용하여 허용 목록의 상태를 확인하려면 다음 단계를 따르세요.

허용 목록의 상태를 확인하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창의 설정에서 허용 목록을 선택합니다.
3. 허용 목록 페이지에서 새로 고침 ()을 선택합니다. Macie는 모든 허용 목록의 설정을 테스트하고 각 목록의 현재 상태가 표시되도록 상태 필드를 업데이트합니다.

   목록에 정규 표현식이 지정되어 있는 경우, 해당 상태는 일반적으로 정상입니다. 즉, Macie가 표현식을 컴파일할 수 있다는 뜻입니다. 목록에 사전 정의된 텍스트가 지정된 경우 상태는 다음 값 중 하나일 수 있습니다.

정상

Macie는 목록의 내용을 검색하고 구문 분석할 수 있습니다.

액세스 거부됨

Macie는 목록을 저장하는 S3 객체에 액세스할 수 없습니다. Amazon S3가 객체 검색 요청을 거부했습니다. Macie가 사용할 수 없는 고객 관리 AWS KMS key 대상으로 객체가 암호화된 경우에도 목록이 이 상태가 될 수 있습니다.

이 오류를 해결하려면, 버킷 및 객체에 대한 버킷 정책 및 기타 권한 설정을 확인합니다. Macie가 객체에 액세스하고 검색할 수 있는지 확인합니다. 객체가 고객 관리형 AWS KMS 키로 암호화된 경우 키 정책을 살펴보고 Macie에서 키를 사용할 수 있는지 확인합니다.

오류

Macie가 목록의 내용을 검색하거나 구문 분석하려고 할 때 일시적인 또는 내부 오류가 발생했습니다. 허용 목록이 Amazon S3와 Macie가 액세스하거나 사용할 수 없는 암호화 키로 목록을 암호화한 경우에도 이 상태가 될 수 있습니다.

이 오류를 해결하려면 몇 분 정도 기다렸다가 새로 고침
()
을 선택합니다. 상태가 계속 오류로 표시되면 S3 객체의 암호화 설정을 확인합니다. 객체가 Amazon S3와 Macie가 액세스하고 사용할 수 있는 키로 암호화되어 있는지 확인합니다.

객체가 비어 있음

Macie는 Amazon S3에서 목록을 검색할 수 있지만 목록에 콘텐츠가 없습니다.

이 오류를 해결하려면 Amazon S3에서 객체를 다운로드하고 객체에 포함된 항목이 올바른지 확인합니다. 항목이 올바르면 Macie에서 목록의 설정을 검토합니다. 지정된 버킷과 객체 이름이 정확한지 확인합니다.

객체를 찾을 수 없음

Amazon S3에 목록이 없습니다.

이 오류를 해결하려면, Macie에서 목록의 설정을 검토합니다. 지정된 버킷과 객체 이름이 정확한지 확인합니다.

할당량 초과

Macie는 Amazon S3에 있는 목록에 액세스할 수 있습니다. 하지만 목록의 항목 수 또는 목록의 스토리지 크기가 허용 목록의 할당량을 초과합니다.

이 오류를 해결하려면, 목록을 여러 파일로 나누십시오. 각 파일에 포함된 항목이 100,000개 미만인지 확인합니다. 또한 각 파일의 크기가 35MB 미만이어야 합니다. 그런 다음 각 파일을 Amazon S3에 업로드합니다. 이후 Macie에서 각 파일의 목록 설정을 구성합니다. 지원되는 각 AWS 리전에 사전 정의된 텍스트 목록을 최대 5개까지 포함할 수 있습니다.

병목 현상 발생

Amazon S3가 목록 검색 요청을 제한했습니다.

이 오류를 해결하려면 몇 분 정도 기다렸다가 새로 고침
()
을 선택합니다.

사용자 액세스 거부됨

Amazon S3가 객체 검색 요청을 거부했습니다. 지정된 개체가 있는 경우 해당 개체에 액세스할 수 없거나 사용할 수 없는 AWS KMS 키로 암호화되어 있습니다.

이 오류를 해결하려면 AWS 관리자에게 문의하여 목록 설정에 올바른 버킷 및 객체 이름이 지정되어 있는지, 그리고 버킷과 객체에 대한 읽기 권한이 있는지 확인하세요. 객체가 암호화된 경우, 사용할 수 있는 키로 해당 객체를 암호화해야 합니다.

4. 특정 목록의 설정과 상태를 검토하려면, 해당 목록 이름을 선택합니다.

API

허용 목록의 상태를 프로그래밍 방식으로 확인하려면 Amazon Macie API의 GetAllowList작업을 사용하거나 명령을 실행하십시오 get-allow-list. AWS CLI

`id` 매개 변수에 상태를 확인하려는 허용 목록의 고유 식별자를 지정합니다. 이 식별자를 가져오려면 작업을 사용하면 됩니다. ListAllowLists 이 ListAllowLists 작업은 계정의 모든 허용 목록에 대한 정보를 검색합니다. 를 사용하는 경우 list-allow-lists명령을 실행하여 이 정보를 검색할 수 있습니다. AWS CLI

GetAllowList 요청을 제출하면, Macie는 허용 목록에 대한 모든 설정을 테스트합니다. 설정에 정규 표현식(정규식)이 지정되어 있는 경우, Macie에서 해당 표현식을 컴파일할 수 있는지 확인합니다.

설정에 사전 정의된 텍스트 목록이 지정된 경우, Macie는 목록을 검색하고 구문 분석할 수 있는지 확인합니다.

그러면 Macie는 허용 목록의 세부 정보를 제공하는 `GetAllowListResponse` 객체를 반환합니다. `GetAllowListResponse` 객체에서 `status` 객체는 목록의 현재 상태, 즉 상태 코드(`code`)와 상태 코드에 따라 목록의 상태에 대한 간략한 설명(`description`)을 표시합니다.

허용 목록에 정규식이 지정되어 있는 경우, 상태 코드는 일반적으로 `OK`이며 관련 설명은 없습니다. 이는 Macie가 표현식을 성공적으로 컴파일했음을 뜻합니다.

허용 목록에 사전 정의된 텍스트가 지정되어 있는 경우, 다음과 같이 상태 코드는 테스트 결과에 따라 달라집니다.

- Macie가 목록을 성공적으로 검색하고 구문 분석하면 상태 코드는 `OK` 이며 관련 설명은 없습니다.
- 오류로 인해 Macie가 목록을 검색하거나 구문 분석을 할 수 없는 경우, 상태 코드와 설명에 발생한 오류의 특성이 표시됩니다.

가능한 상태 코드 목록과 각 상태 코드에 대한 설명은 Amazon Macie API 참조를 참조하십시오 AllowListStatus.

허용 목록 변경

허용 목록을 생성한 후, Amazon Macie에서 목록 설정 대부분을 변경할 수 있습니다. 예를 들어, 목록의 이름과 설명을 변경하고 목록의 태그를 추가 및 편집할 수 있습니다. 목록 유형만 유일하게 변경할 수 없습니다. 예를 들어, 기존 허용 목록에 정규 표현식이 지정된 경우 해당 유형을 사전 정의된 텍스트로 변경할 수 없습니다.

허용 목록에 사전 정의된 텍스트가 지정되어 있는 경우, 목록에 있는 항목을 변경할 수 있습니다. 이렇게 하려면 항목이 포함된 파일을 업데이트한 다음 새 버전의 파일을 Amazon S3에 업로드합니다. 다음에 Macie가 목록을 사용할 준비를 할 때 Macie는 Amazon S3에서 최신 버전의 파일을 검색합니다. 새 파일을 업로드할 때, 동일한 S3 버킷과 객체에 저장해야 합니다. 또는 버킷 또는 객체의 이름을 변경하는 경우, Macie에서 목록의 설정을 업데이트해야 합니다.

허용 목록의 설정은 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 변경할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 허용 목록의 설정을 변경하려면 다음 단계를 따르세요.

허용 목록을 변경하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창의 설정에서 허용 목록을 선택합니다.
3. 허용 목록 페이지에서 변경할 허용 목록의 이름을 선택합니다. 허용 목록 페이지가 열리고 목록의 현재 설정이 표시됩니다.
4. 허용 목록에 태그를 할당하거나 편집하려면, 태그 섹션에서 태그 관리를 선택합니다. 그런 다음 필요에 따라 태그를 변경합니다. 마쳤으면 저장을 선택합니다.
5. 허용 목록의 다른 설정을 변경하려면 목록 설정 섹션에서 편집을 선택합니다. 그런 다음 원하는 설정을 변경합니다.

   - 이름 - 목록의 새 이름을 입력합니다. 이름은 최대 128자까지 포함할 수 있습니다.
   - 설명 - 목록에 대한 새 설명을 입력합니다. 설명은 512자까지 포함할 수 있습니다.
   - 허용 목록에 사전 정의된 텍스트가 지정된 경우:
     - S3 버킷 이름 - 현재 목록을 저장하고 있는 버킷의 이름을 입력합니다.

       Amazon S3에서는 버킷 속성의 이름 필드에서 이 값을 찾을 수 있습니다. 이 값은 대소문자를 구분합니다. 추가로 이름에 와일드카드 문자나 부분 값을 입력하지 마십시오.
     - S3 객체 이름 - 현재 목록을 저장하고 있는 S3 객체의 이름을 입력합니다.

       Amazon S3에서는 객체 속성의 키 필드에서 이 값을 찾을 수 있습니다. 이름에 경로가 포함된 경우, 이름을 입력할 때 전체 경로(예: **`allowlists/macie/mylist.txt`**)를 입력해야 합니다. 이 값은 대소문자를 구분합니다. 추가로 이름에 와일드카드 문자나 부분 값을 입력하지 마십시오.
   - 허용 목록에서 정규 표현식(정규식)을 지정하는 경우, 정규식 상자에 새 정규식을 입력합니다. Regex는 최대 512자까지 포함할 수 있습니다.

     새 정규식을 입력한 후, 선택 사항으로 테스트할 수 있습니다. 이렇게 하려면, 샘플 데이터 상자에 텍스트를 1,000자까지 입력한 다음 테스트를 선택합니다. Macie는 샘플 데이터를 평가하여 정규식과 일치하는 텍스트의 발생 횟수를 보고합니다. 변경 사항을 저장하기 전에 이 단계를 원하는 만큼 반복하여 정규식을 세분화하고 최적화할 수 있습니다.

   설정 변경을 마치면 저장을 선택합니다.

Macie는 목록의 설정을 테스트합니다. 사전 정의된 텍스트 목록의 경우, Macie는 Amazon S3에서 목록을 검색하고 목록의 콘텐츠를 구문 분석할 수 있는지 확인합니다. 정규식의 경우, Macie는 표

현식을 컴파일할 수 있는지 확인합니다. 오류가 발생한 경우, Macie는 해당 오류를 설명하는 메시지를 표시합니다. 오류를 해결하는 데 도움이 되는 자세한 정보는 허용 목록 옵션 및 요구 사항을 참조하십시오. 오류를 해결한 후, 변경 사항을 저장할 수 있습니다.

API

허용 목록을 프로그래밍 방식으로 변경하려면 Amazon Macie API의 UpdateAllowList작업을 사용하거나 AWS CLI의 경우 명령을 실행하십시오 update-allow-list. 요청에서 지원되는 매개 변수를 사용하여 변경하려는 각 설정에 대해 새 값을 지정합니다. `criteria`, `id` 및 `name` 매개 변수가 필요합니다. 필수 매개 변수의 값을 변경하지 않으려면, 매개 변수의 현재 값을 지정합니다.

예를 들어, 다음 명령은 기존 허용 목록의 이름과 설명을 변경합니다. 이 예제는 Microsoft Windows용으로 포맷되었으며 가독성을 높이기 위해 캐럿 (^) 줄 연속 문자를 사용합니다.

```
C:\> aws macie2 update-allow-list ^
--id km2d4y22hp6rv05example ^
--name my_allow_list-email ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--description "Ignores all email addresses for the example.com domain"
```

위치:

- *km2d4y22hp6rv05example*는 목록의 고유 식별자입니다.
- *my_allow_list-email*는 목록의 새 이름입니다.
- *[a-z]@example.com*은 목록의 기준이고, 정규 표현식입니다.
- *example.com #### ## ### ## ##*는 목록에 대한 새 설명입니다.

요청을 제출하면, Macie는 목록 설정을 테스트합니다. 사전 정의된 텍스트 목록의 경우, Macie는 Amazon S3에서 목록을 검색하고 목록의 콘텐츠를 구문 분석할 수 있는지 확인합니다. 목록에 정규식이 지정되어 있는 경우, 여기에는 Macie가 표현식을 컴파일할 수 있는지 확인하는 작업이 포함됩니다.

Macie가 설정을 테스트할 때 오류가 발생하면 요청이 실패하고 Macie는 오류를 설명하는 메시지를 반환합니다. 오류를 해결하는 데 도움이 되는 자세한 정보는 허용 목록 옵션 및 요구 사항을 참조하십시오. 다른 이유로 요청이 실패하면 Macie는 작업이 실패한 이유를 나타내는 HTTP 4 xx 또는 500 응답을 반환합니다.

요청이 성공하면, Macie가 목록 설정을 업데이트하고 다음과 유사한 출력이 표시됩니다.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

`arn`은 안 보이게 하기 규칙의 Amazon 리소스 이름(ARN)이 있는 곳이며, `id`는 규칙의 고유 식별자입니다.

허용 목록 삭제

Amazon Macie에서 허용 목록을 삭제하면 목록의 모든 설정이 영구적으로 삭제됩니다. 이러한 설정은 삭제한 후에는 복구할 수 없습니다. 설정에 Amazon S3에 저장한 사전 정의된 텍스트 목록이 지정되어 있더라도 Macie는 목록이 저장된 S3 객체를 삭제하지 않습니다. Macie의 설정만 삭제됩니다.

허용 목록을 사용하도록 민감한 데이터 검색 작업을 구성한 후 목록을 삭제하더라도 검색 작업은 예정대로 실행됩니다. 하지만 민감한 데이터 결과와 민감한 데이터 검색 결과 모두 작업 결과에서 이전에 허용 목록에 지정한 텍스트를 보고할 수 있습니다. 마찬가지로, 목록을 사용하도록 민감한 데이터 자동 검색을 구성한 후 목록을 삭제하더라도 일일 분석 주기는 계속 진행됩니다. 하지만 민감한 데이터 결과, 통계 또는 기타 유형의 결과에서 이전에 허용 목록에 지정한 텍스트를 보고할 수 있습니다.

허용 목록을 삭제하기 전에 작업 인벤토리를 검토하여 해당 목록을 사용하고 향후 실행이 예정된 작업을 파악하는 것이 좋습니다. 인벤토리의 세부 정보 패널에는 작업이 허용 목록을 사용하도록 구성되었는지 여부와 허용 목록이 있는 경우 해당 목록이 표시됩니다. 또한 민감한 데이터 자동 검색 설정도 확인합니다. 목록을 삭제하는 것보다 변경하는 것이 최선이라고 판단할 수도 있습니다.

추가 보호 수단으로 Macie는 허용 목록을 삭제하려고 할 때 모든 작업의 설정을 확인합니다. 목록을 사용하도록 작업을 구성했는데 해당 작업의 상태가 완료 또는 취소됨이 아닌 다른 상태가 표시되는 경우 Macie는 사용자가 추가로 확인하지 않는 한 해당 목록을 삭제하지 않습니다.

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 허용 목록을 삭제할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 허용 목록을 삭제하려면 다음 단계를 따르세요.

허용 목록을 삭제하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.

2. 탐색 창의 설정에서 허용 목록을 선택합니다.
3. 허용 목록 페이지에서 삭제할 허용 목록의 확인란을 선택합니다.
4. [Actions] 메뉴에서 [Delete]를 선택합니다.
5. 확인 메시지가 나타나면 **delete**를 입력한 다음 삭제(Delete)를 선택합니다.

API

허용 목록을 프로그래밍 방식으로 삭제하려면 Amazon DeleteAllowListMacie API의 작업을 사용하십시오. `id`매개 변수에 삭제할 허용 목록의 고유 식별자를 지정하십시오. 작업을 사용하여 이 식별자를 얻을 수 있습니다. ListAllowLists 이 ListAllowLists 작업은 계정의 모든 허용 목록에 대한 정보를 검색합니다. 를 사용하는 경우 list-allow-lists명령을 실행하여 이 정보를 검색할 수 있습니다. AWS CLI

`ignoreJobChecks` 매개 변수의 경우 민감한 데이터 검색 작업이 해당 목록을 사용하도록 구성된 경우에도 목록을 강제로 삭제할지 여부를 지정합니다.

- `false`가 지정되어 있는 경우 Macie는 상태가 `COMPLETE` 또는 `CANCELLED` 외 다른 상태로 표시된 모든 작업의 설정을 확인합니다. 목록을 사용하도록 구성된 작업이 없는 경우 Macie는 해당 목록을 영구적으로 삭제합니다. 이러한 작업 중 목록을 사용하도록 구성된 작업이 있는 경우 Macie는 요청을 거부하고 HTTP 400(`ValidationException`) 오류를 반환합니다. 오류 메시지는 최대 200개의 작업 중 해당되는 작업의 수를 나타냅니다.
- `true`가 지정되어 있는 경우 Macie는 작업 설정을 확인하지 않고 목록을 영구적으로 삭제합니다.

를 사용하여 허용 목록을 삭제하려면 delete-allow-list명령을 실행합니다. AWS CLI예:

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks
 false
```

여기서 *nkr81bmtu2542yyexample*은 삭제할 허용 목록의 고유 식별자입니다.

요청이 성공하면, Macie는 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Macie는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

허용 목록에 사전 정의된 텍스트가 지정된 경우, 목록을 저장하는 S3 객체를 선택적으로 삭제할 수 있습니다. 하지만, 이 객체를 보관하면 개인 정보 보호 및 보호 감사 또는 조사에 대한 민감한 데이터 조사 결과를 발견하고 검색 결과의 변경 불가능한 기록을 확보하는 데 도움이 됩니다.

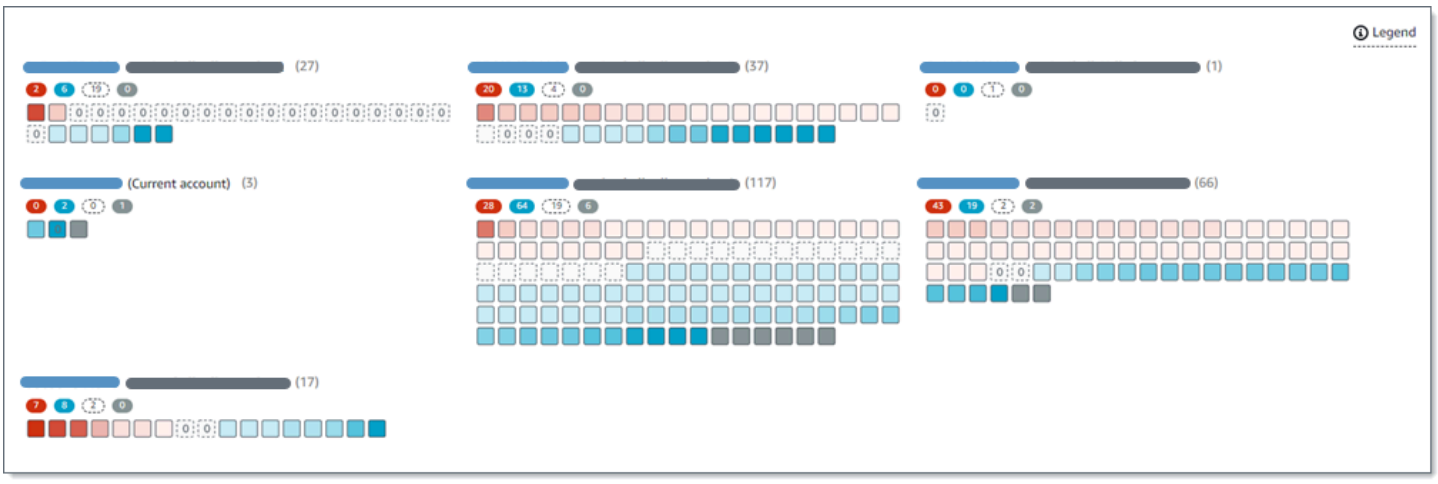
Amazon Macie를 사용하여 민감한 데이터 자동 검색 수행

Amazon Simple Storage Service(S3) 데이터 자산에서 민감한 데이터가 있을 수 있는 위치를 폭넓게 볼 수 있으려면, 계정 또는 조직에 대해 민감한 데이터 자동 검색을 수행하도록 Amazon Macie를 구성하세요. Macie는 민감한 데이터 자동 검색을 통해 S3 버킷 인벤토리를 지속적으로 평가하고 샘플링 기법을 사용하여 버킷의 대표적인 S3 객체를 식별하고 선택합니다. 그런 다음 Macie는 선택한 객체를 검색 및 분석하여 민감한 데이터가 있는지 검사합니다.

기본적으로 Macie는 모든 S3 범용 버킷에서 객체를 선택하고 분석합니다. 조직의 Macie 관리자인 경우 여기에는 구성원 계정이 소유한 버킷의 객체도 포함됩니다. 특정 버킷 (예: 일반적으로 로깅 데이터를 저장하는 버킷) 을 제외하여 분석 범위를 조정할 수 있습니다. AWS Macie 관리자인 경우 조직의 개별 계정을 case-by-case 기준으로 민감한 데이터 자동 검색을 활성화하거나 비활성화할 수 있는 추가 옵션이 있습니다.

특정 유형의 민감한 데이터에 초점을 맞추도록 분석을 조정할 수 있습니다. 기본적으로 Macie는 민감한 데이터 자동 검색에 권장되는 관리형 데이터 식별자 세트를 사용하여 S3 객체를 분석합니다. 분석을 맞춤화하려면 Macie에서 제공하는 특정 관리 데이터 식별자, 사용자가 정의하는 사용자 지정 데이터 식별자 또는 이 둘의 조합을 사용하도록 Macie를 구성하십시오. 지정한 허용 목록을 사용하도록 Macie를 구성하여 분석을 구체화할 수도 있습니다.

매일 분석이 진행됨에 따라 Macie는 발견한 민감한 데이터와 수행하는 분석에 대한 기록을 생성합니다. 민감한 데이터 검색 결과는 Macie가 개별 S3 객체에서 발견한 민감한 데이터를 보고하고 민감한 데이터 검색 결과는 개별 S3 객체의 분석에 대한 세부 정보를 기록합니다. 또한 Macie는 Amazon S3 데이터에 대해 제공하는 통계, 인벤토리 데이터 및 기타 정보를 업데이트합니다. 예를 들어, 콘솔의 다음과 같은 대화형 히트 맵은 데이터 자산 전반의 데이터 민감도를 시각적으로 보여줍니다.



이러한 기능은 Amazon S3 데이터 자산 전반의 데이터 민감도를 평가하고 개별 계정, 버킷 및 객체를 자세히 조사 및 평가하는 데 도움이 되도록 설계되었습니다. 또한 민감한 데이터 검색 작업을 실행하여

더 심층적이고 즉각적인 분석을 수행할 위치를 결정하는 데도 도움이 됩니다. Macie는 Amazon S3 데이터의 보안 및 개인 정보 보호에 대해 제공하는 정보와 와 결합되어 이러한 기능을 사용하여 즉각적인 수정이 필요한 경우를 식별할 수도 있습니다(예: Macie가 민감한 데이터를 발견한 공개적으로 액세스할 수 있는 버킷).

민감한 데이터 자동 검색을 구성하고 관리하려면 계정이 조직의 Macie 관리자 계정이거나 독립형 Macie 계정이어야 합니다.

주제

민감한 데이터 자동 검색의 작동 방식

Amazon Macie를 활성화하면 Macie는 현재 계정에 AWS 계정대해 AWS Identity and Access Management (IAM) 서비스 연결 역할을 생성합니다. AWS 리전이 역할에 대한 권한 정책을 통해 Macie는 사용자를 대신하여 다른 사람에게 전화를 AWS 서비스 걸고 리소스를 모니터링할 수 있습니다. AWS 이 역할을 사용하여 Macie는 리전에서 Amazon Simple Storage Service (Amazon S3) 범용 버킷의 전체 인벤토리를 생성하고 유지 관리합니다. 인벤토리에는 각 S3 버킷 및 버킷 내 객체에 대한 정보가 포함됩니다. 조직의 Macie 관리자인 경우 인벤토리에는 구성원 계정이 소유한 버킷에 대한 정보가 포함됩니다. 자세한 정보는 여러 계정 관리을 참조하세요.

민감한 데이터 자동 검색을 활성화한 경우 Macie는 매일 인벤토리 데이터를 평가하여 자동 검색에 적합한 S3 객체를 식별합니다. 평가의 일환으로 Macie는 분석할 대표적인 객체의 샘플도 선택합니다. 그런 다음 Macie는 선택한 각 객체의 최신 버전을 검색하고 분석하여 민감한 데이터가 있는지 검사합니다.

매일 분석이 진행됨에 따라 Macie는 Amazon S3 데이터에 대해 제공하는 통계, 인벤토리 데이터 및 기타 정보를 업데이트합니다. 또한 Macie는 찾은 민감한 데이터와 수행한 분석에 대한 기록을 생성합니다. 결과 데이터를 통해 Macie가 Amazon S3 데이터 자산에서 민감한 데이터를 발견한 위치를 파악할 수 있습니다. 이 데이터는 Macie가 사용자 계정에 대해 모니터링하고 분석하는 모든 S3 범용 버킷에

걸쳐 있을 수 있습니다. 이 데이터는 Amazon S3 데이터의 보안 및 개인 정보 보호를 평가하고, 심층 조사를 수행할 위치를 결정하고, 수정이 필요한 사례를 식별하는 데 도움이 될 수 있습니다.

민감한 데이터 자동 검색의 작동 방식에 대한 간략한 데모를 보려면 다음 동영상을 시청하세요. Amazon Macie automated data discovery overview

민감한 데이터 자동 검색을 구성하고 관리하려면 계정이 조직의 Macie 관리자 계정이거나 독립형 Macie 계정이어야 합니다. 계정이 조직의 일부인 경우 조직의 Macie 관리자만 조직 내 계정에 대한 민감한 데이터 자동 검색을 활성화하거나 비활성화할 수 있습니다. 또한 Macie 관리자만 계정에 대한 민감한 데이터 자동 검색 설정을 구성하고 관리할 수 있습니다.

주제

핵심 구성 요소

Amazon Macie는 여러 기능과 기법을 조합하여 민감한 데이터 검색을 자동으로 수행합니다. 이러한 기능은 Macie가 제공하는 기능과 함께 작동하여 보안 및 액세스 제어를 위해 Amazon S3 데이터를 모니터링하는 데 도움이 됩니다.

분석할 S3 객체 선택

Macie는 매일 Amazon S3 인벤토리 데이터를 평가하여 민감한 데이터 자동 검색을 통해 분석에 적합한 S3 객체를 식별합니다. 조직의 Macie 관리자인 경우 기본적으로 회원 계정이 소유한 S3 버킷에 대한 데이터가 평가에 포함됩니다.

평가의 일환으로 Macie는 샘플링 기법을 사용하여 분석할 대표적인 S3 객체를 선택합니다. 이 기법은 메타데이터가 비슷하고 내용이 비슷할 가능성이 높은 객체 그룹을 정의합니다. 그룹은 버킷 이름, 접두사, 스토리지 클래스, 파일 이름 확장자, 마지막 수정 날짜 등의 차원을 기반으로 합니다. 그런 다음 Macie는 각 그룹에서 대표적인 샘플 세트를 선택하고, Amazon S3에서 선택한 각 객체의 최신 버전을 검색하고 선택한 각 객체를 분석하여 객체에 민감한 데이터가 포함되어 있는지 확인합니다. 분석이 완료되면 Macie는 객체 사본을 폐기합니다.

샘플링 전략은 분산 분석의 우선 순위를 지정합니다. 일반적으로 Amazon S3 데이터 자산에는 폭우선 접근 방식을 사용합니다. Amazon S3 데이터 에스테이트에 있는 분류 가능한 모든 객체의 총 스토리지 크기를 기준으로 가능한 한 많은 범용 버킷에서 매일 대표적인 S3 객체 세트를 선택합니다. 예를 들어 Macie가 이미 한 버킷의 객체에서 민감한 데이터를 분석하고 발견했지만 다른 버킷

의 객체를 아직 분석하지 않은 경우 후자의 버킷이 분석 우선 순위가 더 높습니다. 이 접근 방식을 사용하면 Amazon S3 데이터의 민감도를 보다 빠르고 폭넓게 파악할 수 있습니다. 데이터 자산의 규모에 따라 48시간 이내에 분석 결과가 나타나기 시작할 수 있습니다.

또한 샘플링 전략은 다양한 종류의 S3 객체와 최근에 생성되거나 변경된 객체에 대한 분석의 우선 순위를 지정합니다. 단일 객체 샘플을 확실하다고 보장할 수는 없습니다. 따라서 다양한 객체 세트를 분석하면 S3 버킷에 포함될 수 있는 민감한 데이터의 유형 및 양을 더 잘 파악할 수 있습니다. 또한 새 객체 또는 최근에 변경된 객체의 우선 순위를 지정하면 분석을 버킷 인벤토리의 변화에 맞게 조정할 수 있습니다. 예를 들어 이전 분석 후에 객체를 만들거나 변경한 경우, 후속 분석에서는 해당 객체의 우선 순위가 더 높습니다. 반대로, 이전에 분석된 객체가 있고 그 분석 이후 변경되지 않은 경우, Macie는 해당 객체를 다시 분석하지 않습니다. 이 접근 방식은 개별 S3 버킷의 민감도 기준을 설정하는 데 도움이 됩니다. 그러면 계정에 지속적인 증분 분석이 진행됨에 따라 개별 버킷에 대한 민감도 평가가 예측 가능한 속도로 점점 더 심층적이고 상세해질 수 있습니다.

분석 범위 정의

기본적으로 Macie에는 인벤토리 데이터를 평가하고 분석할 S3 객체를 선택할 때 계정에 대해 모니터링하고 분석하는 모든 S3 범용 버킷이 포함되어 있습니다. 사용자가 조직의 Macie 관리자인 경우, 여기에는 멤버 계정이 소유한 버킷이 포함됩니다.

특정 S3 버킷을 제외하여 분석 범위를 조정할 수 있습니다. 예를 들어, 이벤트 로그와 같이 일반적으로 AWS 로깅 데이터를 저장하는 버킷은 제외하는 것이 좋을 수 있습니다. AWS CloudTrail 버킷을 제외하려면 계정 또는 버킷의 민감 데이터 자동 검색 설정을 변경할 수 있습니다. 이렇게 하면 Macie는 다음 일일 평가 및 분석 주기가 시작될 때 버킷을 제외하기 시작합니다. 분석에서 최대 1,000개의 버킷을 제외할 수 있습니다. S3 버킷을 제외하면 이후에 다시 포함시킬 수 있습니다. 이렇게 하려면 계정 또는 버킷의 설정을 다시 변경하십시오. 그러면 Macie는 다음 일일 평가 및 분석 주기가 시작될 때 버킷을 포함하기 시작합니다.

조직의 Macie 관리자인 경우 조직의 개별 계정에 대해 민감한 데이터 자동 검색을 활성화하거나 비활성화할 수도 있습니다. 계정에 대한 자동 검색을 비활성화하면 Macie는 계정이 소유한 모든 S3 버킷을 제외합니다. 이후에 계정에 대한 자동 검색을 다시 활성화하면 Macie가 버킷을 다시 포함하기 시작합니다.

감지 및 보고할 민감한 데이터 유형 결정

기본적으로 Macie는 민감한 데이터 자동 검색에 권장되는 관리형 데이터 식별자 세트를 사용하여 S3 객체를 검사합니다. 이러한 관리형 데이터 식별자 목록은 민감한 데이터 자동 검색을 위한 기본 설정 섹션을 참조하세요.

특정 유형의 민감한 데이터에 초점을 맞추도록 분석을 조정할 수 있습니다. 이렇게 하려면 다음과 같은 방법으로 계정의 민감한 데이터 자동 검색 설정을 변경합니다.

- 관리형 데이터 식별자 추가 또는 제거 - 관리형 데이터 식별자는 특정 국가 또는 지역의 신용 카드 번호, AWS 비밀 액세스 키 또는 여권 번호와 같은 특정 유형의 민감한 데이터를 탐지하도록 설계된 일련의 기본 제공 기준 및 기법입니다. 자세한 정보는 관리형 데이터 식별자 사용을 참조하세요.
- 사용자 지정 데이터 식별자 추가 또는 제거 - 사용자 지정 데이터 식별자는 민감한 데이터를 탐지하기 위해 정의하는 일련의 기준입니다. 사용자 지정 데이터 식별자를 사용하면 조직의 특정 시나리오, 지적 재산 또는 독점 데이터(예: 직원 ID, 고객 계정 번호 또는 내부 데이터 분류)를 반영하는 민감한 데이터를 감지할 수 있습니다. 자세한 정보는 사용자 지정 데이터 식별자 빌드을 참조하세요.
- 허용 목록 추가 또는 제거 - Macie의 허용 목록은 Macie가 S3 객체에서 무시할 텍스트 또는 텍스트 패턴을 지정합니다. 이는 일반적으로 조직의 공개 이름이나 전화번호, 조직에서 테스트에 사용하는 샘플 데이터 등 특정 시나리오나 환경에 대한 민감한 데이터 예외입니다. 자세한 정보는 허용 목록을 사용하여 민감한 데이터 예외사항 정의을 참조하세요.

설정을 변경하면 Macie는 다음 일일 분석 주기가 시작될 때 변경 내용을 적용합니다. 조직의 Macie 관리자인 경우 Macie는 조직의 다른 계정에 대한 S3 객체를 분석할 때 해당 계정의 설정을 사용합니다.

버킷 민감도 평가에 특정 유형의 민감한 데이터를 포함할지 여부를 결정하는 버킷 수준 설정을 조정할 수도 있습니다. 자세한 방법은 개별 S3 버킷에 대한 민감한 데이터 자동 검색 관리(을)를 참조하세요.

민감도 점수 계산

기본적으로 Macie는 계정에 대해 모니터링하고 분석하는 각 S3 범용 버킷의 민감도 점수를 자동으로 계산합니다. 사용자가 조직의 Macie 관리자인 경우, 여기에는 멤버 계정이 소유한 버킷이 포함됩니다.

Macie에서 민감도 점수는 Macie가 버킷에서 발견한 민감한 데이터의 양과 Macie가 버킷에서 분석한 데이터의 양, 이 두 가지 기본 차원의 교차점을 정량적으로 측정한 것입니다. 버킷의 민감도 점수에 따라 Macie가 버킷에 할당하는 민감도 레이블이 결정됩니다. 민감도 레이블은 버킷의 민감도 점수를 정성적으로 표현한 것입니다(예: 민감함, 민감하지 않음, 아직 분석되지 않음). Macie가 정의하는 민감도 점수 및 레이블의 범위에 대한 자세한 내용은 S3 버킷의 민감도 점수 섹션을 참조하세요.

> **Important**
>
> S3 버킷의 민감도 점수 및 레이블은 해당 버킷 또는 버킷 객체가 조직에 미칠 수 있는 중요도나 중요성을 암시하거나 나타내지 않습니다. 대신 잠재적 보안 위험을 식별하고 모니터링하는 데 도움이 되는 참조 지점을 제공합니다.

처음에 민감한 데이터 자동 검색을 활성화하면 Macie는 각 S3 버킷에 민감도 점수 50과 아직 분석되지 않음 레이블을 자동으로 할당합니다. 빈 버킷은 예외입니다. 빈 버킷은 객체를 저장하지 않거나 모든 버킷의 객체에 0바이트의 데이터가 포함된 버킷입니다. 버킷이 이 경우에 해당하면 Macie는 버킷에 점수 1을 할당하고 버킷에는 민감하지 않음 레이블을 할당합니다.

민감한 데이터 자동 검색이 진행됨에 따라 Macie는 분석 결과를 반영하도록 민감도 점수와 레이블을 업데이트합니다. 예:

- Macie가 객체에서 민감한 데이터를 찾지 못하면 Macie는 버킷의 민감도 점수를 낮추고 필요에 따라 버킷의 민감도 레이블을 업데이트합니다.
- Macie가 객체에서 민감한 데이터를 발견하면 Macie는 버킷의 민감도 점수를 높이고 필요에 따라 버킷의 민감도 레이블을 업데이트합니다.
- Macie가 이후에 변경된 객체에서 민감한 데이터를 발견하면 Macie는 해당 객체에 대한 민감한 데이터 감지를 버킷의 민감도 점수에서 제거하고, 필요에 따라 버킷의 민감도 레이블을 업데이트합니다.
- Macie가 이후에 삭제된 객체에서 민감한 데이터를 발견하면 해당 객체에 대한 민감한 데이터 감지를 버킷의 민감도 점수에서 제거하고, 필요에 따라 버킷의 민감도 레이블을 업데이트합니다.

버킷 점수에서 특정 유형의 민감한 데이터를 포함하거나 제외하여 개별 S3 버킷의 민감도 점수 설정을 조정할 수 있습니다. 또한 버킷에 최대 점수(100)를 수동으로 할당하여 버킷의 계산된 점수를 재정의할 수 있습니다. 최대 점수를 할당하는 경우, 버킷에는 민감함 레이블이 지정됩니다. 자세한 정보는 개별 S3 버킷에 대한 자동화된 데이터 검색 관리을 참조하세요.

메타데이터, 통계 및 결과 생성

민감한 데이터 자동 검색을 활성화하면 Macie는 계정에 대해 모니터링하고 분석하는 S3 범용 버킷에 대한 추가 인벤토리 데이터, 통계 및 기타 정보를 생성하고 유지 관리하기 시작합니다. 조직의 Macie 관리자인 경우 기본적으로 여기에는 구성원 계정이 소유한 버킷이 포함됩니다.

추가 정보는 Macie가 지금까지 수행한 자동화된 민감한 데이터 검색 활동의 결과를 캡처합니다. 또한 개별 버킷의 퍼블릭 액세스 및 공유 액세스 설정과 같이 Macie가 Amazon S3 데이터에 대해 제공하는 기타 정보를 보완합니다. 추가 정보에는 다음이 포함됩니다.

- 집계된 데이터 민감도 통계(예: Macie가 민감한 데이터를 발견한 총 버킷 수, 공개 액세스할 수 있는 버킷 수)
- Amazon S3 데이터 자산 전반의 데이터 민감도를 대화식형으로 시각적으로 표현.
- 분석의 현재 상태를 나타내는 버킷 수준의 세부 정보. Macie가 버킷에서 분석한 객체 목록, Macie가 버킷에서 발견한 민감한 데이터의 유형, Macie가 발견한 각 유형의 민감한 데이터 발생 횟수 등을 예로 들 수 있습니다.

이 정보에는 Amazon S3 데이터의 적용 범위를 평가하고 모니터링하는 데 도움이 되는 통계 및 세부 정보도 포함되어 있습니다. 전체 데이터 자산과 버킷 인벤토리의 개별 S3 버킷에 대한 분석 상태를 확인할 수 있습니다. 또한 Macie가 특정 버킷의 객체를 분석하지 못하게 하는 문제를 식별할 수 있습니다. 문제를 해결하면 후속 분석 주기 동안 Amazon S3 데이터의 적용 범위를 늘릴 수 있습니다. 자세한 정보는 민감한 데이터 자동 검색 범위 평가을 참조하세요.

Macie는 자동화된 민감한 데이터 검색을 수행하는 동안 이 정보를 자동으로 재계산하고 업데이트합니다. 예를 들어 Macie가 이후에 변경되거나 삭제된 S3 객체에서 민감한 데이터를 발견하면 Macie는 해당 버킷의 메타데이터를 업데이트합니다. 즉, 분석된 객체 목록에서 해당 객체를 제거하고, Macie가 객체에서 발견한 민감한 데이터의 발생을 제거하고, 점수가 자동으로 계산되면 민감도 점수를 다시 계산하고, 필요에 따라 민감도 레이블을 업데이트하여 새 점수를 반영합니다.

메타데이터 및 통계 외에도 Macie는 Macie가 개별 S3 객체에서 발견한 민감한 데이터를 보고하는 민감한 데이터 검색 결과, 개별 S3 객체의 분석에 대한 세부 정보를 기록하는 민감한 데이터 검색 결과 등 찾은 민감한 데이터와 수행하는 분석에 대한 기록을 생성합니다.

자세한 정보는 민감한 데이터 자동 검색 통계 및 결과 검토을 참조하세요.

고려 사항

Amazon Macie를 구성하고 사용하여 Amazon S3 데이터에 대한 민감한 데이터 자동 검색을 수행할 때는 다음 사항에 유의하십시오.

- 자동 검색 설정은 현재 AWS 리전설정에만 적용됩니다. 따라서 결과 분석 및 데이터는 현재 지역의 S3 범용 버킷 및 객체에만 적용됩니다. 자동 검색을 수행하고 추가 지역의 결과 데이터에 액세스하려면 각 추가 리전에서 자동 검색을 활성화하고 구성하세요.
- 조직의 Macie 관리자인 경우
  - 현재 리전의 계정에 Macie가 활성화된 경우에만 멤버 계정에 대해 자동 검색을 수행할 수 있습니다. 또한 해당 지역의 계정에 대해 자동 검색을 활성화해야 합니다. 구성원은 자신의 계정에 대해 자동 검색을 활성화할 수 없습니다.
  - 회원 계정에 대한 자동 검색을 활성화하면 Macie는 구성원 계정의 데이터를 분석할 때 관리자 계정의 자동 검색 설정을 사용합니다. 적용 가능한 설정은 분석에서 제외할 S3 버킷 목록과 S3 객체를 분석할 때 사용할 관리 데이터 식별자, 사용자 지정 데이터 식별자, 허용 목록입니다. 구성원은 자신의 계정에 대해 이러한 설정을 구성할 수 없습니다.
  - 구성원은 S3 버킷의 자동 검색 설정에 액세스할 수 없습니다. 예를 들어 구성원은 자신이 소유한 버킷의 민감도 점수 설정을 조정할 수 없습니다. Macie 관리자만 이러한 설정에 액세스할 수 있습니다.

  - 구성원은 Macie가 S3 버킷에 직접 제공하는 민감한 데이터 검색 통계 및 기타 결과에 액세스할 수 없습니다. 예를 들어 구성원은 Macie를 사용하여 S3 버킷의 민감도 점수를 검토하거나 자동 검색이 S3 객체에 대해 생성한 결과에 액세스할 수 없습니다. Macie 관리자만 Macie를 사용하여 이 데이터에 액세스할 수 있습니다.
- S3 버킷의 권한 설정으로 인해 Macie가 버킷 또는 버킷의 객체에 대한 정보를 검색하거나 액세스할 수 없는 경우, Macie는 버킷에 대한 자동 검색을 수행할 수 없습니다. Macie는 버킷을 소유한 AWS 계정 의 계정 ID, 버킷 이름, Macie가 가장 최근 일일 새로 고침 주기의 일부로 버킷에 대한 버킷 및 객체 메타데이터를 검색한 시기 등 버킷에 대한 일부 정보만 제공할 수 있습니다. 버킷 인벤토리에서 이러한 버킷의 민감도 점수는 50이며 민감도 레이블은 아직 분석되지 않음입니다.

  이러한 경우, S3 버킷을 빠르게 식별하려면 자동 검색 범위 데이터를 참조하세요. 자세한 정보는 민감한 데이터 자동 검색 범위 평가을 참조하세요. 특정 버킷의 문제를 조사하려면 Amazon S3의 버킷 정책 및 권한 설정을 검토하세요. 예를 들어 버킷에 제한적인 버킷 정책이 있을 수 있습니다. 자세한 정보는 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을 참조하세요.
- 선택 및 분석 대상이 되려면 S3 객체를 범용 버킷에 저장하고 분류할 수 있어야 합니다. 분류 가능한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하며 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가집니다. 자세한 정보는 지원하는 스토리지 클래스 및 형식을 참조하세요.
- S3 객체가 암호화된 경우, Macie는 Macie가 액세스할 수 있고 사용할 수 있는 키로 해당 객체를 암호화한 경우에만 해당 객체를 분석할 수 있습니다. 자세한 정보는 암호화된 S3 객체 분석을 참조하세요. 암호화 설정으로 인해 Macie가 버킷에 있는 하나 이상의 객체를 분석하지 못한 경우를 파악하려면 자동 검색 범위 데이터를 참조하세요. 자세한 내용은 민감한 데이터 자동 검색 범위 평가을(를) 참조하세요.

민감한 데이터 자동 검색 구성

Amazon Macie는 자동 민감한 데이터 검색을 통해 Amazon Simple Storage Service (Amazon S3) 범용 버킷에서 샘플 객체를 지속적으로 선택하고 객체를 분석하여 민감한 데이터가 포함되어 있는지 확인합니다. 조직의 Macie 관리자인 경우 기본적으로 여기에는 구성원 계정이 소유한 S3 버킷의 객체가 포함됩니다. 분석이 진행됨에 따라 Macie는 Amazon S3 데이터에 대해 제공하는 통계, 인벤토리 데이터 및 기타 정보를 업데이트합니다. 또한 Macie는 찾은 민감한 데이터와 수행한 분석에 대한 기록을 생성합니다.

민감한 데이터 자동 검색을 구성하고 관리하려면 계정이 조직의 Macie 관리자 계정이거나 독립형 Macie 계정이어야 합니다. 계정이 조직의 일부인 경우 조직의 Macie 관리자만 조직 내 계정에 대한 민감한 데이터 자동 검색을 활성화하거나 비활성화할 수 있습니다. 또한 Macie 관리자만 계정에 대한 민

감한 데이터 자동 검색 설정을 구성할 수 있습니다. 멤버 계정이 있고 Macie가 S3 버킷에 대한 민감한 데이터 자동 검색을 수행하도록 하려면 Macie 관리자에게 문의하십시오.

주제

- 시작하기 전 준비 사항
- 조직을 위한 구성 옵션
- 민감한 데이터 자동 검색 활성화
- 자동 민감 데이터 검색 설정 구성
- 민감한 데이터 자동 검색 비활성화

민감한 데이터 자동 검색을 활성화, 구성 또는 비활성화하는 경우 변경 사항은 현재에만 적용됩니다. AWS 리전추가 리전에서도 동일한 변경을 적용하려면 각 추가 리전에서 해당 단계를 반복합니다.

시작하기 전 준비 사항

민감한 데이터 자동 검색을 활성화하거나 구성하기 전에 다음 작업을 완료하여 필요한 리소스와 권한이 있는지 확인하십시오.

Tasks

- 민감한 데이터 검색 결과를 위한 리포지토리를 구성합니다.
- 권한을 확인하세요.

민감한 데이터 자동 검색을 이미 활성화 및 구성한 상태에서 설정만 변경하거나 비활성화하려는 경우 이러한 작업은 선택 사항입니다.

민감한 데이터 검색 결과를 위한 리포지토리를 구성합니다.

Amazon Macie는 자동화된 민감한 데이터 검색을 수행할 때 분석을 위해 선택한 각 Amazon Simple Storage Service (Amazon S3) 객체에 대한 분석 레코드를 생성합니다. 민감한 데이터 검색 결과라고 하는 이러한 레코드는 개별 S3 객체 분석에 대한 세부 정보를 기록합니다. 여기에는 Macie가 민감한 데이터를 찾지 못한 객체 및 권한 설정과 같은 오류나 문제로 인해 Macie가 분석할 수 없는 객체가 포함됩니다. Macie가 개체에서 민감한 데이터를 찾은 경우 Macie가 발견한 민감한 데이터에 대한 정보가 중요 데이터 검색 결과에도 포함됩니다. 민감한 데이터 검색 결과에는 데이터 프라이버시 및 보호 감사 또는 조사에 도움이 될 수 있는 분석 기록이 표시됩니다.

Macie는 민감한 데이터 검색 결과를 90일 동안만 저장합니다. 결과에 액세스하고 해당 결과를 장기간 저장 및 보존하려면 결과를 S3 버킷에 저장하도록 Macie를 구성합니다. 버킷은 모든 민감한 데이터 검색 결과를 위한 확정적이고 장기적인 리포지토리 역할을 할 수 있습니다.

이 리포지토리를 구성했는지 확인하려면 Amazon Macie 콘솔의 탐색 창에서 검색 결과를 선택합니다. 프로그래밍 방식으로 이 작업을 수행하려면 Amazon Macie GetClassificationExportConfigurationAPI의 작업을 사용하십시오. 민감한 데이터 검색 결과와 이 리포지토리를 구성하는 방법에 대한 자세한 내용은 민감한 데이터 검색 결과 저장 및 유지 섹션을 참조하세요.

리포지토리를 구성한 경우 처음으로 민감한 데이터 자동 검색을 활성화하면 Macie는 `automated-sensitive-data-discovery` 리포지토리에 이름이 지정된 폴더를 생성합니다. 이 폴더에는 Macie가 계정 또는 조직에 대해 자동 검색을 수행하는 동안 생성하는 민감한 데이터 검색 결과가 저장됩니다.

권한을 확인하세요.

권한을 확인하려면 AWS Identity and Access Management (IAM) 을 사용하여 IAM 자격 증명에 연결된 IAM 정책을 검토하십시오. 그런 다음 해당 정책의 정보와 수행할 수 있어야 하는 다음 작업 목록과 비교합니다.

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`
- `macie2:ListClassificationScopes`
- `macie2:UpdateClassificationScope`
- `macie2:ListSensitivityInspectionTemplates`
- `macie2:UpdateSensitivityInspectionTemplate`

첫 번째 작업을 통해 Amazon Macie 계정에 액세스할 수 있습니다. 두 번째 작업을 통해 계정 또는 조직의 민감한 데이터 자동 검색을 활성화하거나 비활성화할 수 있습니다. 조직의 경우 조직 내 계정에 대해 민감한 데이터 자동 검색을 자동으로 활성화할 수도 있습니다. 나머지 작업을 통해 구성 설정을 식별하고 변경할 수 있습니다.

Amazon Macie 콘솔을 사용하여 구성 설정을 검토하거나 변경하려는 경우 다음 작업을 수행할 수 있는지도 확인하십시오.

- `macie2:GetAutomatedDiscoveryConfiguration`
- `macie2:GetClassificationScope`
- `macie2:GetSensitivityInspectionTemplate`

이러한 작업을 통해 현재 구성 설정과 계정 또는 조직의 자동화된 민감한 데이터 검색 상태를 검색할 수 있습니다. 구성 설정을 프로그래밍 방식으로 변경하려는 경우 이러한 작업을 수행할 수 있는 권한은 선택 사항입니다.

조직의 Macie 관리자인 경우 다음 작업도 수행할 수 있어야 합니다.

- `macie2:ListAutomatedDiscoveryAccounts`
- `macie2:BatchUpdateAutomatedDiscoveryAccounts`

첫 번째 작업을 통해 조직의 개별 계정에 대한 자동화된 민감한 데이터 검색 상태를 검색할 수 있습니다. 두 번째 작업을 통해 조직의 개별 계정에 대해 민감한 데이터 자동 검색을 활성화하거나 비활성화할 수 있습니다.

필요한 조치를 수행할 수 없는 경우 AWS 관리자에게 도움을 요청하세요.

조직을 위한 구성 옵션

계정이 여러 Amazon Macie 계정을 중앙에서 관리하는 조직의 일부인 경우 조직의 Macie 관리자는 조직 내 계정에 대한 민감한 데이터 자동 검색을 구성하고 관리합니다. 여기에는 Macie가 계정에 대해 수행하는 분석의 범위와 특성을 정의하는 설정이 포함됩니다. 구성원은 자신의 계정으로는 이러한 설정에 액세스할 수 없습니다.

조직의 Macie 관리자인 경우 다음과 같은 여러 방법으로 분석 범위를 정의할 수 있습니다.

- 계정에 대한 민감한 데이터 자동 검색 활성화 - 민감한 데이터 자동 검색을 사용하도록 설정하는 경우 모든 기존 계정과 새 구성원 계정에 대해 자동으로 활성화할지, 새 구성원 계정에만 활성화할지, 아니면 계정은 사용하지 않을지 지정합니다. 새 회원 계정에 대해 자동으로 활성화하면 Macie에서 해당 계정이 조직에 가입할 때 이후에 조직에 가입하는 모든 계정에서 활성화됩니다. 계정에 대해 활성화된 경우 Macie는 해당 계정이 소유한 S3 버킷을 포함합니다. 계정에 대해 비활성화된 경우 Macie는 해당 계정이 소유한 버킷을 제외합니다.
- 계정에 대한 민감한 데이터 자동 검색을 선택적으로 활성화 - 이 옵션을 사용하면 개별 계정에 대해 민감한 데이터 자동 검색을 활성화하거나 비활성화할 수 있습니다. case-by-case 계정에서 이 기능을 활성화하면 Macie는 해당 계정이 소유한 S3 버킷을 포함합니다. 활성화하지 않거나 계정에서 비활성화하면 Macie는 해당 계정이 소유한 버킷을 제외합니다.
- 자동화된 민감한 데이터 검색에서 특정 S3 버킷 제외 - 하나 이상의 계정에 대해 자동 민감한 데이터 검색을 활성화하면 해당 계정이 소유한 특정 S3 버킷을 제외할 수 있습니다. 그러면 Macie는 조직을 위한 자동 검색을 수행할 때 버킷을 건너뛰게 됩니다. 특정 버킷을 제외하려면 관리자 계정의 구성 설정에 있는 버킷 제외 목록에 추가하십시오. 조직의 버킷을 1,000개까지 제외할 수 있습니다.

기본적으로 민감한 데이터 자동 검색은 조직의 모든 신규 및 기존 계정에 대해 자동으로 활성화됩니다. 또한 Macie에는 계정이 소유한 모든 S3 버킷이 포함됩니다. 기본 설정을 유지할 경우 Macie는 관리자 계정에 대해 모니터링하고 분석하는 모든 버킷 (구성원 계정이 소유한 모든 버킷 포함) 에 대해 자동 검색을 수행합니다.

또한 Macie 관리자는 Macie가 조직을 위해 수행하는 분석의 성격도 정의할 수 있습니다. Macie가 S3 객체를 분석할 때 사용할 관리 데이터 식별자, 사용자 지정 데이터 식별자, 허용 목록 등 관리자 계정에 대한 추가 설정을 구성하면 됩니다. Macie는 조직의 다른 계정에 대해 S3 객체를 분석할 때 관리자 계정의 설정을 사용합니다.

민감한 데이터 자동 검색 활성화

민감한 데이터 자동 검색을 활성화하면 Amazon Macie는 Amazon S3 인벤토리 데이터를 평가하고 현재 계정에 대한 기타 자동 검색 활동을 수행하기 시작합니다. AWS 리전조직의 Macie 관리자인 경우 기본적으로 여기에는 구성원 계정이 소유한 S3 버킷이 포함됩니다. Amazon S3 데이터 자산의 크기에 따라 민감한 데이터 검색 통계 및 기타 결과가 48시간 이내에 나타나기 시작할 수 있습니다.

계정 또는 조직에 대한 민감한 데이터 자동 검색을 활성화하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 콘솔을 사용하여 활성화하려면 다음 단계를 따르십시오. 프로그래밍 방식으로 활성화하려면 Amazon Macie BatchUpdateAutomatedDiscoveryAccountsAPI의 다음 작업을 사용하십시오. 조직의 경우 개별 계정의 경우, 조직의 경우 Macie 관리자 계정 UpdateAutomatedDiscoveryConfiguration또는 독립형 Macie 계정을 사용하십시오.

민감한 데이터 자동 검색을 활성화하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 민감한 데이터 자동 검색을 활성화할 지역을 선택합니다.
3. 탐색 창의 설정에서 민감한 데이터 자동 검색을 선택합니다.
4. 독립형 Macie 계정이 있는 경우 상태 섹션에서 활성화를 선택합니다.
5. 조직의 Macie 관리자인 경우 상태 섹션에서 옵션을 선택하여 다음에 대해 민감한 데이터 자동 검색을 활성화할 계정을 지정합니다.

    - 조직의 모든 계정에서 이 기능을 활성화하려면 활성화를 선택합니다. 표시되는 대화 상자에서 내 조직을 선택합니다. 이후에 조직에 가입하는 계정에도 자동으로 활성화하려면 새 계정에 대해 자동으로 활성화를 선택합니다. 작업을 마치면 활성화를 선택합니다.

- 특정 멤버 계정에만 활성화하려면 계정 관리를 선택합니다. 그런 다음 계정 페이지의 표에서 활성화하려는 각 계정의 확인란을 선택합니다. 작업을 마치면 작업 메뉴에서 민감한 데이터 자동 검색 활성화를 선택합니다.
- Macie 관리자 계정에서만 활성화하려면 활성화를 선택합니다. 표시되는 대화 상자에서 내 계정을 선택하고 새 계정 자동 활성화를 선택 해제합니다. 작업을 마치면 [활성화] 를 선택합니다.

이후에 조직의 개별 계정에 대한 자동 민감 데이터 검색 상태를 확인하거나 변경하려면 탐색 창에서 계정을 선택합니다. 계정 페이지에서 표의 자동 민감 데이터 검색 필드는 계정에 대한 자동 검색의 현재 상태를 나타냅니다. 계정 상태를 변경하려면 계정을 선택한 다음 작업 메뉴를 사용하여 계정에 대한 자동 검색을 비활성화할 수 있도록 설정합니다.

민감한 데이터 자동 검색을 활성화한 후에는 설정을 검토 및 구성하여 Macie가 수행하는 분석을 구체화하십시오.

자동 민감 데이터 검색 설정 구성

계정 또는 조직에 대해 민감한 데이터 자동 검색을 활성화하는 경우, 자동 검색 설정을 조정하여 Amazon Macie가 수행하는 분석을 세분화할 수 있습니다. 이러한 설정은 분석에서 제외할 S3 버킷을 지정합니다. 또한 S3 객체를 분석할 때 사용할 관리형 데이터 식별자, 사용자 지정 데이터 식별자, 허용 목록 등 탐지 및 보고할 민감한 데이터의 유형과 발생 빈도를 지정합니다.

기본적으로 Macie는 사용자 계정에 대해 모니터링하고 분석하는 모든 S3 범용 버킷에 대해 민감한 데이터 자동 검색을 수행합니다. 사용자가 조직의 Macie 관리자인 경우, 여기에는 멤버 계정이 소유한 버킷이 포함됩니다. 분석에서 특정 버킷을 제외할 수 있습니다. 예를 들어 이벤트 로그와 같이 AWS CloudTrail 일반적으로 AWS 로깅 데이터를 저장하는 버킷을 제외할 수 있습니다. 버킷을 제외하고 나중에 다시 포함시킬 수 있습니다.

또한 Macie는 민감한 데이터 자동 검색에 권장되는 관리형 데이터 식별자 세트만 사용하여 S3 객체를 분석합니다. Macie는 사용자가 정의한 사용자 지정 데이터 식별자나 허용 목록을 사용하지 않습니다. 분석을 사용자 지정하려면 Macie가 특정 관리형 데이터 식별자, 사용자 지정 데이터 식별자, 허용 목록을 사용하도록 구성할 수 있습니다.

다음 섹션에서는 각 설정 유형에 대한 추가 정보를 제공합니다. 또한 Amazon Macie 콘솔을 사용하여 설정을 변경하는 방법도 설명합니다. 자세히 알아보려면 섹션을 선택하세요. 프로그래밍 방식으로 설정을 검토하거나 변경하려면 Amazon Macie UpdateClassificationScopeAPI의 다음 작업을 사용하여 분석에서 제외할 S3 버킷을 지정하고 사용할 관리형 데이터 식별자, 사용자 지정 데이터 식별자 UpdateSensitivityInspectionTemplate및 허용 목록을 지정할 수 있습니다.

설정을 변경하면 Macie는 민감한 데이터 자동 검색에 대한 다음 평가 및 분석 주기가 시작될 때(일반적으로 24시간 이내) 변경 내용을 적용합니다.

S3 버킷 제외 또는 포함

기본적으로 Macie는 계정에 대해 모니터링하고 분석하는 모든 S3 범용 버킷에 대해 자동 민감 데이터 검색을 수행합니다. 사용자가 조직의 Macie 관리자인 경우, 여기에는 멤버 계정이 소유한 버킷이 포함됩니다.

범위를 좁히기 위해 분석에서 최대 1,000개의 S3 버킷을 제외할 수 있습니다. 버킷을 제외하면 Macie는 민감한 데이터 자동 검색을 수행할 때 버킷의 객체 선택 및 분석을 중단합니다. 버킷에 대한 기존의 민감한 데이터 검색 통계 및 세부 정보는 그대로 유지됩니다. 예를 들어 버킷의 현재 민감도 점수는 변경되지 않습니다. 버킷을 제외한 후, 나중에 다시 포함할 수 있습니다.

특정 S3 버킷을 제외 또는 포함하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 자동 검색 분석에서 특정 S3 버킷을 제외하거나 포함하려는 지역을 선택합니다.
3. 탐색 창의 설정에서 민감한 데이터 자동 검색을 선택합니다.

   민감한 데이터 자동 검색 페이지가 나타나고 현재 설정이 표시됩니다. 해당 페이지의 S3 버킷 섹션에는 현재 제외된 S3 버킷이 나열되거나 모든 버킷이 현재 포함되어 있음을 나타냅니다.
4. S3 버킷 섹션에서 편집을 선택합니다.
5. 다음 중 하나를 수행하십시오.

   - 하나 이상의 S3 버킷을 제외하려면 제외 목록에 버킷 추가를 선택합니다. 그런 다음 S3 버킷 테이블에서 제외하려는 각 버킷에 해당하는 확인란을 선택합니다. 표에는 현재 지역의 계정 또는 조직에 대한 모든 범용 버킷이 나열됩니다.
   - 이전에 제외한 S3 버킷을 하나 이상 포함하려면 제외 목록에서 버킷 제거를 선택합니다. 그런 다음 S3 버킷 테이블에서 포함하려는 각 버킷에 해당하는 확인란을 선택합니다. 표에는 현재 자동 검색 분석에서 제외된 모든 버킷이 나열되어 있습니다.

   특정 버킷을 더 쉽게 찾으려면 테이블 위의 검색 상자에 검색 기준을 입력합니다. 열 머리글을 선택하여 테이블을 정렬할 수 있습니다.
6. 버킷 선택을 마치면 이전 단계에서 선택한 옵션에 따라 추가 또는 제거를 선택합니다.

관리형 데이터 식별자 추가 또는 제거

관리형 데이터 식별자는 특정 유형의 민감한 데이터 (예: 특정 국가 또는 지역의 신용 카드 번호, AWS 보안 액세스 키 또는 여권 번호) 를 탐지하도록 설계된 일련의 기본 제공 기준 및 기술입니다. 기본적으로 Macie는 민감한 데이터 자동 검색에 권장되는 관리형 데이터 식별자 세트를 사용하여 S3 객체를 분석합니다. 이러한 식별자 목록을 검토하려면 을 참조하십시오. 민감한 데이터 자동 검색을 위한 기본 설정

특정 유형의 민감한 데이터에 초점을 맞추도록 분석을 조정할 수 있습니다.

- Macie가 탐지 및 보고할 민감한 데이터 유형에 대한 관리 데이터 식별자를 추가하고,
- Macie가 탐지 및 보고하지 못하게 하려는 민감한 데이터 유형의 관리형 데이터 식별자를 삭제하세요.

관리형 데이터 식별자를 제거해도 변경 사항은 S3 버킷에 대한 기존의 민감한 데이터 검색 통계 및 세부 정보에 영향을 주지 않습니다. 예를 들어, Macie가 이전에 버킷에서 해당 유형의 데이터를 감지했는데 AWS 비밀 액세스 키에 대한 관리형 데이터 식별자를 제거한 경우 Macie는 버킷에 대해 해당 탐지를 계속 보고합니다.

> **Tip**
>
> 모든 S3 버킷의 후속 분석에 영향을 미치는 관리형 데이터 식별자를 제거하는 대신 특정 버킷의 민감도 점수에서 해당 탐지를 제외할 수 있습니다. 자세한 정보는 개별 S3 버킷에 대한 민감한 데이터 자동 검색 관리을 참조하세요.

관리형 데이터 식별자를 추가하거나 제거하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 자동 검색 분석에 관리 데이터 식별자를 추가하거나 제거하려는 지역을 선택합니다.
3. 탐색 창의 설정에서 민감한 데이터 자동 검색을 선택합니다.

   민감한 데이터 자동 검색 페이지가 나타나고 현재 설정이 표시됩니다. 해당 페이지의 관리 데이터 식별자 섹션에는 현재 설정이 두 개의 탭으로 구성되어 표시됩니다.

   - 기본값으로 추가됨 — 이 탭에는 추가한 관리 데이터 식별자가 나열됩니다. Macie는 기본 세트에 있지만 제거하지 않은 식별자 외에도 이러한 식별자를 사용합니다.

- 기본값에서 제거됨 — 이 탭에는 삭제한 관리 데이터 식별자가 나열됩니다. Macie는 이러한 식별자를 사용하지 않습니다.

4. 관리형 데이터 식별자 섹션에서 편집을 선택합니다.
5. 다음을 수행합니다.

   - 관리형 데이터 식별자를 하나 이상 추가하려면 기본값에 추가됨 탭을 선택합니다. 그런 다음 표에서 추가할 각 관리 데이터 식별자의 확인란을 선택합니다. 확인란이 이미 선택되어 있으면 해당 식별자를 이미 추가한 것입니다.
   - 관리형 데이터 식별자를 하나 이상 제거하려면기본값에서 제거됨 탭을 선택합니다. 그런 다음 표에서 제거할 각 관리 데이터 식별자의 확인란을 선택합니다. 확인란이 이미 선택되어 있으면 해당 식별자가 이미 제거된 것입니다.

   각 탭의 테이블에는 Macie가 현재 제공하는 모든 관리형 데이터 식별자 목록이 표시됩니다. 표의 첫 번째 열은 각 관리 데이터 식별자의 ID를 지정합니다. ID는 식별자가 탐지하도록 설계된 민감한 데이터의 유형을 설명합니다 (예: 미국 여권 번호의 경우 USA_PASSPORT_NUMBER). 특정 관리형 데이터 식별자를 더 쉽게 찾으려면 표 위의 검색 상자에 검색 기준을 입력하세요. 열 머리글을 선택하여 테이블을 정렬할 수 있습니다. 각 식별자에 대한 자세한 내용은 관리형 데이터 식별자 사용 섹션을 참조하세요.
6. 마쳤으면 저장을 선택합니다.

사용자 지정 데이터 식별자 추가 또는 제거

사용자 지정 데이터 식별자는 민감한 데이터를 감지하기 위해 정의하는 기준 집합입니다. 기준은 일치시킬 텍스트 패턴을 정의하고 선택적으로 문자 시퀀스와 결과를 세분화하는 근접성 규칙을 정의하는 정규 표현식(regex)으로 구성됩니다. 자세한 내용은 사용자 지정 데이터 식별자 빌드(을)를 참조하세요.

기본적으로 Amazon Macie는 민감한 데이터 자동 검색을 수행할 때 사용자 지정 데이터 식별자를 사용하지 않습니다. Macie가 특정 사용자 지정 데이터 식별자를 사용하도록 하려면 해당 식별자를 분석에 추가할 수 있습니다. 그러면 Macie는 Macie에서 사용하도록 구성한 관리형 데이터 식별자 외에도 사용자 지정 데이터 식별자를 사용합니다.

사용자 지정 데이터 식별자를 추가하면 나중에 제거할 수 있습니다. 변경 사항은 S3 버킷의 기존 민감한 데이터 검색 통계 및 세부 정보에는 영향을 미치지 않습니다. 즉, 이전에 버킷에 대한 탐지를 생성한 사용자 지정 데이터 식별자를 제거해도 Macie는 버킷에 대한 탐지를 계속 보고합니다. 그러나 모든 버킷에 대한 후속 분석에 영향을 미치는 식별자를 제거하는 대신 특정 버킷의 민감도 점수에서 해당 탐지

를 제외하는 것이 좋습니다. 자세한 정보는 개별 S3 버킷에 대한 민감한 데이터 자동 검색 관리을 참조하세요.

사용자 지정 데이터 식별자를 추가하거나 제거하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 자동 검색 분석에서 사용자 지정 데이터 식별자를 추가하거나 제거할 지역을 선택합니다.
3. 탐색 창의 설정에서 민감한 데이터 자동 검색을 선택합니다.

   민감한 데이터 자동 검색 페이지가 나타나고 현재 설정이 표시됩니다. 해당 페이지에서 사용자 지정 데이터 식별자 섹션에는 추가한 사용자 지정 데이터 식별자가 나열되거나 사용자 지정 데이터 식별자를 선택하지 않았음을 나타냅니다.
4. 사용자 지정 데이터 식별자 섹션에서 편집을 선택합니다.
5. 다음을 수행합니다.

   - 사용자 지정 데이터 식별자를 하나 이상 추가하려면 추가할 각 사용자 지정 데이터 식별자의 확인란을 선택합니다. 확인란이 이미 선택되어 있으면 해당 식별자를 이미 추가한 것입니다.
   - 사용자 지정 데이터 식별자를 하나 이상 제거하려면 제거할 각 사용자 지정 데이터 식별자의 확인란을 선택 취소합니다. 확인란이 이미 선택 해제된 경우 Macie는 현재 해당 식별자를 사용하지 않습니다.

   > **Tip**
   >
   > 사용자 지정 데이터 식별자를 선택하기 전에 식별자를 검토하거나 설정을 테스트하려면 식별자 이름 옆의 링크 아이콂 ( ) 을 선택합니다. Macie는 식별자 설정을 표시하는 페이지를 엽니다. 샘플 데이터로 식별자를 테스트하려면 해당 페이지의 샘플 데이터 상자에 최대 1,000자의 텍스트를 입력합니다. 그런 다음 [Test] 를 선택합니다. Macie는 샘플 데이터를 평가하여 일치 개수를 보고합니다.
6. 마쳤으면 저장을 선택합니다.

허용 목록 추가 또는 제거

Amazon Macie에서 허용 목록은 Macie가 S3 객체에 대해 민감한 데이터를 검사할 때 무시할 특정 텍스트 또는 텍스트 패턴을 정의합니다. 텍스트가 허용 목록의 항목 또는 패턴과 일치하는 경우 Macie는 해당 텍스트를 보고하지 않습니다. 이는 텍스트가 관리형 데이터 식별자 또는 사용자 지정 데이터 식별자의 기준과 일치하는 경우에도 마찬가지입니다. 자세한 내용은 허용 목록을 사용하여 민감한 데이터 예외사항 정의(을)를 참조하세요.

기본적으로 Macie는 민감한 데이터 자동 검색을 수행할 때 허용 목록을 사용하지 않습니다. Macie가 특정 허용 목록을 사용하도록 하려면 분석에 해당 목록을 추가할 수 있습니다. 허용 목록을 추가하면 나중에 제거할 수 있습니다.

허용 목록을 추가하거나 제거하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 자동 검색 분석에서 허용 목록을 추가하거나 제거하려는 지역을 선택합니다.
3. 탐색 창의 설정에서 민감한 데이터 자동 검색을 선택합니다.

   민감한 데이터 자동 검색 페이지가 나타나고 현재 설정이 표시됩니다. 해당 페이지의 허용 목록 섹션은 이미 추가한 허용 목록을 지정하거나 허용 목록을 선택하지 않았음을 나타냅니다.
4. 허용 목록 섹션에서 편집을 선택합니다.
5. 다음을 수행합니다.

   - 하나 이상의 허용 목록을 추가하려면 추가할 각 허용 목록의 확인란을 선택합니다. 확인란이 이미 선택되어 있으면 해당 목록이 이미 추가된 것입니다.
   - 하나 이상의 허용 목록을 제거하려면 제거할 각 허용 목록의 확인란을 지우십시오. 확인란이 이미 선택 해제된 경우 Macie는 현재 해당 목록을 사용하지 않습니다.

> **Tip**
>
> 허용 목록을 추가하거나 제거하기 전에 허용 목록의 설정을 검토하려면 목록 이름 옆에 있는 링크 아이콘 ( ) 을 선택합니다. Macie는 목록 설정을 표시하는 페이지를 엽니다. 목록에 정규 표현식(regex)이 지정된 경우, 이 페이지를 사용하여 샘플 데이터로 정규 표현식을 테스트할 수

도 있습니다. 이렇게 하려면 샘플 데이터 상자에 텍스트를 1,000자까지 입력한 다음 테스트를 선택합니다. Macie는 샘플 데이터를 평가하여 일치 개수를 보고합니다.

6. 마쳤으면 저장을 선택합니다.

민감한 데이터 자동 검색 비활성화

언제든지 계정 또는 조직에 대한 민감한 데이터 자동 검색을 비활성화할 수 있습니다. 이렇게 하면 Macie는 후속 평가 및 분석 주기가 시작되기 전, 일반적으로 48시간 이내에 해당 계정 또는 조직에 대한 모든 자동 검색 활동을 중단합니다. 추가 효과는 다음과 같이 다양합니다.

- 조직의 계정에 대해 이 기능을 비활성화해도 계정에 대한 자동 검색을 수행하는 동안 Macie가 생성하고 직접 제공한 모든 통계 데이터, 인벤토리 데이터 및 기타 정보에 계속 액세스할 수 있습니다. 계정에 대한 자동 검색을 다시 활성화할 수도 있습니다. 그러면 Macie는 계정에 대한 모든 자동 검색 활동을 재개합니다.
- 조직 또는 독립형 Macie 계정에서 이 기능을 비활성화하면 조직 또는 계정에 대한 자동 검색을 수행하는 동안 Macie가 생성하고 직접 제공한 모든 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다. 예를 들어, S3 버킷 인벤토리에는 더 이상 민감도 시각화 또는 분석 통계가 포함되지 않습니다. 이후에 다시 활성화할 수 있습니다. 그러면 Macie는 조직 또는 계정에 대한 모든 자동 검색 활동을 재개합니다. 30일 이내에 다시 활성화하면 Macie가 자동 검색을 수행하는 동안 이전에 생성하여 직접 제공한 모든 데이터와 정보에 다시 액세스할 수 있습니다. 30일 이내에 다시 활성화하지 않으면 Macie는 이 데이터와 정보를 영구적으로 삭제합니다.

조직 또는 계정에 대한 민감한 데이터 자동 검색을 수행하면서 Macie가 생성한 민감한 데이터 결과에 계속 액세스할 수 있습니다. Macie는 조사 결과를 90일 동안 저장합니다. 또한 저장하거나 다른 사람에게 게시한 데이터는 그대로 AWS 서비스 유지되며 Amazon S3의 민감한 데이터 검색 결과 및 Amazon 에서의 이벤트 검색과 같이 영향을 받지 않습니다. EventBridge

민감한 데이터 자동 검색을 비활성화하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 콘솔을 사용하여 비활성화하려면 다음 단계를 따르십시오. 프로그래밍 방식으로 비활성화하려면 Amazon Macie BatchUpdateAutomatedDiscoveryAccountsAPI의 다음 작업을 사용하십시오. 조직의 경우 개별 계정의 경우, 조직의 경우 Macie 관리자 계정 UpdateAutomatedDiscoveryConfiguration또는 독립형 Macie 계정을 사용하십시오.

민감한 데이터 자동 검색을 비활성화하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.

2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 민감한 데이터 자동 검색을 비활성화하려는 지역을 선택합니다.
3. 탐색 창의 설정에서 민감한 데이터 자동 검색을 선택합니다.
4. 조직의 Macie 관리자인 경우 상태 섹션에서 옵션을 선택하여 다음에 대한 민감한 데이터 자동 검색을 비활성화할 계정을 지정합니다.

   - 특정 구성원 계정에 대해서만 이 기능을 비활성화하려면 계정 관리를 선택합니다. 그런 다음 계정 페이지의 표에서 비활성화하려는 각 계정의 확인란을 선택합니다. 작업을 마치면 작업 메뉴에서 민감한 데이터 자동 검색 비활성화를 선택합니다.
   - Macie 관리자 계정에 대해서만 비활성화하려면 [비활성화] 를 선택합니다. 나타나는 대화 상자에서 [내 계정] 을 선택한 다음 [비활성화] 를 선택합니다.
   - 조직 및 조직 전체의 모든 계정에 대해 이 기능을 비활성화하려면 비활성화를 선택합니다. 표시되는 대화 상자에서 내 조직을 선택한 다음 비활성화를 선택합니다.
5. 독립형 Macie 계정이 있는 경우 상태 섹션에서 비활성화를 선택합니다.

개별 S3 버킷에 대한 민감한 데이터 자동 검색 관리

자동화된 민감한 데이터 검색 통계 및 결과를 검토 및 평가하면서 개별 Amazon Simple Storage Service (Amazon S3) 버킷의 민감도 점수 및 기타 설정을 조정할 수 있습니다. 이러한 설정을 조정하면, Amazon S3 데이터 자산 전체 및 해당 데이터 자산 내의 특정 버킷에 대한 민감도 평가를 미세 조정할 수 있습니다. 또한 특정 버킷에 대해 수행한 조사 결과를 캡처할 수 있습니다.

다음과 같은 방법으로 S3 버킷의 민감한 데이터 자동 검색 설정을 조정할 수 있습니다.

민감도 점수 할당

기본적으로 Amazon Macie는 버킷의 민감도 점수를 자동으로 계산합니다. 점수는 주로 Macie가 버킷에서 발견한 민감한 데이터의 양과 Macie가 버킷에서 분석한 데이터의 양을 기반으로 합니다. 자세한 정보는 S3 버킷의 민감도 점수을 참조하세요.

버킷의 계산된 점수를 재정의하고 최대 점수(100)를 수동으로 할당할 수 있습니다. 이렇게 하면 버킷에도 민감함 레이블이 적용됩니다. 이렇게 하면 Macie는 버킷에 대한 자동 검색을 계속 수행합니다. 하지만 후속 분석은 버킷 점수에 영향을 주지 않습니다. 점수를 자동으로 다시 계산하려면 설정을 다시 변경하세요.

민감도 점수에서 특정 민감 데이터 유형 제외 또는 포함

자동으로 계산되는 경우 버킷의 민감도 점수는 Macie가 버킷에서 발견한 민감한 데이터의 양을 부분적으로 기반으로 합니다. 이는 주로 Macie가 버킷에서 찾은 민감한 데이터 유형의 특성과 수, 각

유형의 발생 횟수에서 비롯됩니다. 기본적으로 Macie는 버킷의 민감도 점수를 계산할 때 모든 유형의 민감한 데이터가 발생한 경우를 포함합니다.

버킷 점수에서 특정 유형의 민감한 데이터를 제외하거나 포함하여 계산을 조정할 수 있습니다. 예를 들어 Macie가 버킷에서 우편 주소를 감지했는데 이 주소가 허용된다고 판단한 경우 버킷 점수에서 모든 우편 주소를 제외할 수 있습니다. 민감한 데이터 유형을 제외하면 Macie는 계속해서 버킷을 검사하여 해당 유형의 데이터가 있는지 확인하고 발견된 데이터를 보고합니다. 하지만 이러한 상황은 버킷의 계산된 점수에는 영향을 미치지 않습니다. 민감한 데이터 유형을 계산된 저장소에 다시 포함하려면 설정을 다시 변경하세요.

후속 분석에서 버킷을 제외 또는 포함

기본적으로 Macie는 계정에 대해 모니터링하고 분석하는 모든 범용 버킷에 대해 자동 검색을 수행합니다. 조직의 Macie 관리자인 경우 기본 설정에는 구성원 계정이 소유한 버킷이 포함됩니다. 분석에서 특정 버킷을 제외할 수 있습니다. 예를 들어, 이벤트 로그와 같이 AWS CloudTrail 일반적으로 AWS 로깅 데이터를 저장하는 버킷을 제외할 수 있습니다.

버킷을 제외하면 기존의 민감한 데이터 검색 통계 및 버킷 세부 정보가 유지됩니다. 예를 들어 버킷의 현재 민감도 점수는 변경되지 않습니다. 하지만 Macie는 자동 검색을 수행할 때 버킷의 객체 분석을 중단합니다. 버킷을 제외한 후, 나중에 다시 포함할 수 있습니다.

S3 버킷의 민감도 점수에 영향을 미치는 설정을 변경하면 Macie는 Amazon S3 데이터에 대해 제공하는 관련 통계 및 정보를 즉시 재계산하고 업데이트하기 시작합니다. 예를 들어, 버킷에 최대 점수를 할당하면 Macie는 계정 또는 조직의 집계 통계에서 민감한 버킷의 수를 증가시킵니다.

Amazon Macie 콘솔을 사용하여 설정을 변경하려면 다음 단계를 따르세요. 프로그래밍 방식으로 설정을 변경하려면 Amazon Macie UpdateResourceProfileAPI의 다음 작업을 사용하여 버킷에 민감도 점수를 할당하고, 민감한 데이터 유형을 버킷 UpdateResourceProfileDetections점수에서 제외하거나 이후에 포함시키고 UpdateClassificationScope, 후속 분석에서 버킷을 제외하거나 포함시킬 수 있습니다.

S3 버킷에 대한 민감한 데이터 자동 검색 설정을 변경하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 S3 버킷을 선택합니다. S3 버킷 페이지에는 버킷 인벤토리가 표시됩니다.

   기본적으로 페이지에는 현재 분석에서 제외된 버킷에 대한 데이터가 표시되지 않습니다. 조직의 Macie 관리자인 경우 현재 민감한 데이터 자동 검색이 비활성화된 계정의 데이터도 표시되지 않습니다. 이 데이터를 표시하려면 필터 상자 아래에 있는 자동 검색으로 모니터링됨 필터 토큰에서 X를 선택합니다.

3. 설정을 변경하려는 S3 버킷을 선택합니다. 테이블 보기
()
또는 대화형 맵
()
을 사용하여 버킷을 선택할 수 있습니다.
4. 세부 정보 패널에서 다음 작업 중 하나를 수행합니다.

   - 계산된 점수를 재정의하고 민감도 점수를 버킷에 수동으로 할당하려면 최대 점수 할당()을 켜세요. 이렇게 하면 버킷 점수가 100으로 변경되고 버킷에 민감함 레이블이 적용됩니다.

     Macie가 자동으로 계산하는 점수를 할당하려면 최대 점수 할당()을 끕니다.
   - 후속 분석에서 버킷을 제외하려면 자동 검색에서 제외()를 켜세요.

     이전에 버킷을 분석에서 제외한 경우 자동 검색에서 제외()를 해제하여 버킷을 다시 포함하세요.
   - 버킷의 민감도 점수에서 특정 유형의 민감한 데이터를 제외하거나 포함하려면 민감도 탭을 선택합니다. 탐지 표에서 제외하거나 포함할 수 있는 민감한 데이터 유형의 선택 상자를 선택합니다. 그런 다음 작업 메뉴에서 점수에서 제외를 선택하여 유형을 제외하거나 점수에 포함을 선택하여 유형을 포함합니다.

     표에서 민감한 데이터 유형 필드는 데이터를 탐지한 관리형 데이터 식별자의 고유 식별자(ID) 또는 데이터를 탐지한 사용자 지정 데이터 식별자의 이름을 지정합니다. 관리형 데이터 식별자의 ID는 식별자가 탐지하도록 설계된 민감한 데이터의 유형을 설명합니다(예: 미국 여권 번호의 경우, USA_PASSPORT_NUMBER). 각 관리형 데이터 식별자에 대한 자세한 내용은 관리형 데이터 식별자 사용 섹션을 참조하세요.

S3 버킷의 민감도 점수에 영향을 미치는 설정을 변경한 경우 Macie는 즉시 관련 민감한 데이터 검색 통계 및 버킷에 대한 기타 정보를 다시 계산하고 업데이트하기 시작합니다.

민감한 데이터 자동 검색 범위 평가

계정 또는 조직의 민감한 데이터 자동 검색이 진행됨에 따라 Amazon Macie는 Amazon Simple Storage Service (Amazon S3) 데이터 자산의 적용 범위를 평가하고 모니터링하는 데 도움이 되는 통계 및 세부 정보를 제공합니다. 이 데이터를 사용하여 전체 데이터 자산과 버킷 인벤토리의 개별 S3 버킷에 대한 민감한 데이터 자동 검색의 상태를 확인할 수 있습니다. 또한 Macie가 특정 버킷의 객체를 분석하지 못하게 하는 문제를 식별할 수 있습니다. 문제를 해결하면 후속 분석 주기 동안 Amazon S3 데이터의 적용 범위를 늘릴 수 있습니다.

커버리지 데이터는 현재 S3 범용 버킷에 대한 자동 민감 데이터 검색의 현재 상태에 대한 스냅샷을 제공합니다. AWS 리전사용자가 조직의 Macie 관리자인 경우, 여기에는 멤버 계정이 소유한 버킷이 포함됩니다. 각 버킷의 데이터는 Macie가 버킷의 객체를 분석하려고 할 때 문제가 발생했는지 여부를 나타냅니다. 문제가 발생한 경우 데이터는 각 문제의 특성과 경우에 따라 발생 횟수를 나타냅니다. 민감한 데이터 자동 검색이 매일 진행됨에 따라 데이터가 업데이트됩니다. Macie가 일일 분석 주기 동안 버킷에 있는 하나 이상의 객체를 분석하거나 분석을 시도하는 경우, Macie는 적용 범위 데이터 및 기타 데이터를 업데이트하여 결과를 반영합니다.

특정 유형의 문제의 경우 모든 S3 범용 버킷의 데이터를 집계하여 검토하고 선택적으로 드릴다운하여 각 버킷에 대한 추가 세부 정보를 확인할 수 있습니다. 예를 들어 적용 범위 데이터를 사용하면 Macie가 계정에서 액세스할 수 없는 모든 버킷을 빠르게 식별할 수 있습니다. 적용 범위 데이터는 발생한 객체 수준의 문제도 보고합니다. 분류 오류라고 하는 이러한 문제로 인해 Macie는 버킷의 특정 객체를 분석하지 못했습니다. 예를 들어 더 이상 사용할 수 없는 AWS Key Management Service (AWS KMS) 키로 객체가 암호화되므로 Macie가 버킷에서 분석하지 못한 객체 수를 확인할 수 있습니다.

Amazon Macie 콘솔을 사용하여 적용 범위 데이터를 검토하는 경우, 데이터 보기에는 각 유형의 문제를 해결하기 위한 지침이 포함됩니다. 이 섹션의 후속 주제에서는 각 유형에 대한 수정 지침도 제공합니다.

주제

민감한 데이터 자동 검색 범위 데이터 검토

자동화된 민감한 데이터 검색 범위를 검토 및 평가하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 콘솔과 API는 모두 현재 Amazon Simple Storage Service (Amazon S3) 범용 버킷에 대한 분석의 현재 상태를 나타내는 데이터를 제공합니다. AWS 리전데이터에는 분석에서 격차를 야기하는 문제에 대한 정보가 포함됩니다.

- Macie가 액세스할 수 없는 버킷. 버킷의 권한 설정으로 인해 Macie가 버킷과 버킷의 객체에 액세스할 수 없기 때문에 Macie는 이러한 버킷의 객체를 분석할 수 없습니다.
- 분류 가능한 객체를 저장하지 않는 버킷. 모든 객체가 Macie가 지원하지 않는 Amazon S3 스토리지 클래스를 사용하거나 Macie가 지원하지 않는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가지고 있기 때문에 Macie는 이러한 버킷의 객체를 분석할 수 없습니다.
- 객체 수준 분류 오류로 인해 Macie가 아직 분석하지 못한 버킷입니다. Macie는 이러한 버킷에 있는 하나 이상의 객체를 분석하려고 시도했습니다. 하지만 Macie는 객체 수준 권한 설정, 객체 콘텐츠 또는 할당량 관련 문제로 인해 객체를 분석할 수 없었습니다.

커버리지 데이터는 민감한 데이터 자동 검색이 매일 진행됨에 따라 업데이트됩니다. 조직의 Macie 관리자인 경우 데이터에는 멤버 계정이 소유한 S3 버킷에 대한 정보가 포함됩니다.

> **Note**
>
> 적용 범위 데이터에는 생성 및 실행한 민감한 데이터 검색 작업의 결과가 명시적으로 포함되지 않습니다. 하지만 민감한 데이터 자동 검색 결과에 영향을 미치는 적용 범위 문제를 해결하면 이후에 실행하는 민감한 데이터 검색 작업의 적용 범위도 늘어날 수 있습니다. 작업의 적용 범위를 평가하려면 해당 작업의 통계 및 결과를 검토하세요. 작업의 로그 이벤트 또는 기타 결과가 적용 범위 문제를 나타내는 경우, 이 섹션 뒷부분에 나오는 수정 지침을 통해 일부 문제를 해결할 수 있습니다.

민감한 데이터 자동 검색 범위 데이터를 검토하려면

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 계정 또는 조직의 적용 범위 데이터를 검토할 수 있습니다. 콘솔에서는 각 버킷에서 최근에 발생한 문제의 롤업을 포함하여 모든 S3 범용 버킷의 커버리지 데이터를 한 페이지에 통합하여 볼 수 있습니다. 이 페이지에는 문제 유형별로 데이터 그룹을 검토할 수 있는 옵션도 제공됩니다. 특정 버킷에 대한 결과를 추적하려면 페이지의 데이터를 쉼표로 구분된 값(CSV) 파일로 내보내면 됩니다.

Console

Amazon Macie 콘솔을 사용하여 민감한 데이터 자동 검색 범위 데이터를 검토하려면 다음 단계를 따르세요.

적용 범위 데이터를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 리소스 적용 범위을 선택합니다.
3. 리소스 적용 범위 페이지에서 검토하려는 적용 범위 데이터 유형의 탭을 선택합니다.

   - 전체 - Macie가 사용자 계정에 대해 모니터링하고 분석하는 모든 버킷을 나열합니다.

     각 버킷의 문제 필드에는 Macie가 문제로 인해 버킷의 객체를 분석하지 못했는지에 대한 여부가 표시됩니다. 이 필드의 값이 없음이면 Macie가 버킷의 객체 중 하나 이상을 분석했거나 Macie가 아직 버킷의 객체 분석을 시도하지 않은 것입니다. 문제가 있는 경우 이 필드에는 문제의 성격과 문제 해결 방법이 표시됩니다. 객체 수준 분류 오류의 경우 오류 발생 횟수를 괄호 안에 표시할 수도 있습니다.
   - 액세스 거부 - Macie가 액세스할 수 없는 버킷을 나열합니다. 이러한 버킷의 권한 설정으로 인해 Macie는 버킷과 버킷의 객체에 액세스할 수 없습니다. 따라서 Macie는 이러한 버킷의 객체를 분석할 수 없습니다.
   - 분류 오류 - 객체 수준 권한 설정, 객체 콘텐츠 또는 할당량 관련 문제 등 객체 수준 분류 오류로 인해 Macie가 아직 분석하지 않은 버킷을 나열합니다.

     각 버킷의 문제 필드에는 발생하여 Macie가 버킷의 객체를 분석하지 못하게 한 각 오류 유형의 특성이 표시됩니다. 또한 각 유형의 오류를 해결하는 방법도 안내합니다. 오류에 따라 오류 발생 횟수를 괄호 안에 표시할 수도 있습니다.
   - 분류 불가 - Macie가 분류 가능한 객체를 저장하지 않아 분석할 수 없는 버킷을 나열합니다. 이러한 버킷의 모든 객체는 지원되지 않는 Amazon S3 스토리지 클래스를 사용하거나 지원되지 않는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 사용합니다. 따라서 Macie는 이러한 버킷의 객체를 분석할 수 없습니다.
4. 버킷에 대한 지원 데이터를 자세히 살펴보고 검토하려면 버킷 이름을 선택하십시오. 그런 다음 버킷 세부 정보 패널에서 버킷에 대한 통계 및 기타 정보를 참조하세요.
5. 테이블을 CSV 파일로 내보내려면 페이지 상단에서 CSV로 내보내기를 선택합니다. 결과 CSV 파일에는 테이블의 각 버킷에 대한 메타데이터 하위 집합이 포함되며, 최대 50,000개의 버킷이 포함됩니다. 이 파일에는 적용 범위 문제 필드가 포함되어 있습니다. 이 필드의 값은 Macie가

문제로 인해 버킷의 객체를 분석하지 못했는지 여부와 분석할 수 없는 경우 해당 문제의 특성을 나타냅니다.

API

커버리지 데이터를 프로그래밍 방식으로 검토하려면 Amazon Macie API DescribeBuckets작업을 사용하여 제출하는 쿼리에 필터 기준을 지정하십시오. 이 작업은 객체의 배열을 반환합니다. 각 객체에는 필터 기준과 일치하는 S3 범용 버킷에 대한 통계 데이터 및 기타 정보가 들어 있습니다.

필터 기준에 검토하려는 적용 범위 데이터 유형에 대한 조건을 포함시킵니다.

- 버킷의 권한 설정으로 인해 Macie가 액세스할 수 없는 버킷을 식별하려면 `errorCode` 필드 값이 `ACCESS_DENIED`와(과) 같은 조건을 포함시킵니다.
- Macie가 액세스할 수있지만 아직 분석하지 않은 버킷을 식별하려면 `sensitivityScore` 필드 값이 `50`와(과) 같고 `errorCode` 필드 값은 `ACCESS_DENIED`와(과) 같지 않은 조건을 포함시킵니다.
- 모든 버킷의 객체가 지원되지 않는 스토리지 클래스나 형식을 사용하기 때문에 Macie가 분석할 수 없는 버킷을 식별하려면 `classifiableSizeInBytes` 필드 값이 `0`와(과) 같고 `sizeInBytes` 필드 값이 `0`보다 큰 조건을 포함시킵니다.
- Macie가 하나 이상의 객체를 분석한 버킷을 식별하려면 `sensitivityScore` 필드 값이 1~99 범위에 속하지만 `50`와(과) 같지 않은 조건을 포함시킵니다. 수동으로 최대 점수를 할당한 버킷도 포함하려면 해당 범위는 1~100이어야 합니다.
- 객체 수준 분류 오류로 인해 Macie가 아직 분석하지 않은 버킷을 식별하려면 `sensitivityScore` 필드 값이 `-1`와(과) 같은 조건을 포함시킵니다. 그런 다음 특정 버킷에서 발생한 오류 유형 및 수에 대한 분석을 검토하려면 GetResourceProfile작업을 사용하십시오.

AWS Command Line Interface (AWS CLI)를 사용하는 경우 describe-buckets 명령을 실행하여 제출하는 쿼리의 필터 기준을 지정합니다. 특정 S3 버킷에서 발생한 오류 유형 및 수를 분류하여 검토하려면 (있는 경우) get-resource-profile명령을 실행하십시오.

예를 들어 다음 AWS CLI 명령은 필터 기준을 사용하여 버킷의 권한 설정으로 인해 Macie가 액세스할 수 없는 모든 S3 버킷의 세부 정보를 검색합니다.

이 예제는 Linux, macOS 또는 Unix용 형식으로 표시됩니다.

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

이 예제는 Microsoft Windows에 맞게 포맷되어 있습니다.

```
C:\> aws macie2 describe-buckets --criteria={\"errorCode\":{\"eq\":[\"ACCESS_DENIED\"]}}
```

요청이 성공하면 Macie는 buckets 배열을 반환합니다. 배열에는 현재 상태이고 필터 AWS 리전 기준과 일치하는 각 S3 버킷의 객체가 포함됩니다.

필터 기준과 일치하는 S3 버킷이 없는 경우 Macie는 빈 buckets 배열을 반환합니다.

```
{
    "buckets": []
}
```

일반적인 기준의 예를 포함하여 쿼리에 필터 기준을 지정하는 방법에 대한 자세한 내용은 S3 버킷 인벤토리 필터링 섹션을 참조하세요.

민감한 데이터 자동 검색에 대한 적용 범위 문제 해결

Amazon Macie는 Amazon Simple Storage Service(S3) 데이터의 민감한 데이터 자동 검색 범위를 제한하는 여러 유형의 문제를 보고합니다. 다음 정보는 이러한 문제를 조사하고 해결하는 데 도움이 될 수 있습니다.

문제 유형 및 세부 정보

- 액세스 거부됨
- 분류 오류: 잘못된 콘텐츠
- 분류 오류: 잘못된 암호화
- 분류 오류: 잘못된 KMS 키
- 분류 오류: 권한이 거부됨
- 분류 불가

> **Tip**
>
> S3 버킷의 객체 수준 분류 오류를 조사하려면 먼저 버킷의 객체 샘플 목록을 검토합니다. 이 목록은 Macie가 버킷에서 분석하거나 분석을 시도한 객체(최대 100개 객체)를 나타냅니다. Amazon Macie 콘솔에서 목록을 검토하려면 S3 버킷 페이지에서 버킷을 선택한 다음 버킷 세부 정보 패널에서 객체 샘플 탭을 선택합니다. 목록을 프로그래밍 방식으로 검토하려면

Amazon ListResourceProfileArtifactsMacie API의 작업을 사용하십시오. 객체의 분석 상태가 건너뜀(SKIPPED)인 경우 객체로 인해 오류가 발생했을 수 있습니다.

액세스 거부됨

이 문제는 S3 버킷의 권한 설정으로 인해 Macie가 버킷과 버킷의 객체에 액세스할 수 없음을 나타냅니다. Macie는 버킷의 모든 객체를 검색하고 분석할 수 없습니다.

세부 정보

이러한 유형의 문제가 발생하는 가장 일반적인 원인은 제한적인 버킷 정책입니다. 버킷 정책은 보안 주체 AWS Identity and Access Management (사용자, 계정, 서비스 또는 기타 엔티티) 가 S3 버킷에서 수행할 수 있는 작업과 보안 주체가 해당 작업을 수행할 수 있는 조건을 지정하는 리소스 기반 (IAM) 정책입니다. 제한적인 버킷 정책은 특정 조건에 따라 버킷 데이터에 대한 액세스를 허용하거나 제한하는 명시적 `Allow` 또는 `Deny` 명령문을 사용합니다. 예를 들어 버킷에 액세스하는데 특정 소스 IP 주소를 사용하지 않는 한, 버킷 정책에는 버킷에 대한 액세스를 거부하는 `Allow` 또는 `Deny` 명령문이 포함될 수 있습니다.

S3 버킷의 버킷 정책에 하나 이상의 조건이 포함된 명시적인 `Deny` 명령문이 포함된 경우, Macie가 민감한 데이터를 탐지하기 위해 버킷의 객체를 검색 및 분석하는 것이 허용되지 않을 수 있습니다. Macie는 버킷 이름, 생성 날짜 등 버킷에 대한 일부 정보만 제공할 수 있습니다.

수정 지침

이 문제를 해결하려면 S3 버킷의 버킷 정책을 업데이트합니다. 정책에서 Macie가 버킷과 버킷의 객체에 액세스할 수 있도록 허용하는지 확인하세요. 이 액세스를 허용하려면 Macie 서비스 연결 역할(`AWSServiceRoleForAmazonMacie`)에 대한 조건을 정책에 추가합니다. 조건은 Macie 서비스 연결 역할이 정책의 `Deny` 제한과 일치하지 않도록 해야 합니다. `aws:PrincipalArn` 전역 조건 컨텍스트 키와 계정에 대한 Macie 서비스 연결 역할의 Amazon 리소스 이름(ARN)을 사용하여 이 작업을 수행할 수 있습니다.

버킷 정책을 업데이트하여 Macie가 S3 버킷에 대한 액세스 권한을 얻으면 Macie가 변경 사항을 감지합니다. 이 경우 Macie는 Amazon S3 데이터에 대해 제공하는 통계, 인벤토리 데이터 및 기타 정보를 업데이트합니다. 또한 후속 분석 주기에서는 버킷의 객체가 분석에서 우선 순위가 높아지게 됩니다.

추가 참조

Macie가 버킷에 액세스할 수 있도록 S3 버킷 정책을 업데이트하는 방법에 대한 자세한 내용은 Amazon Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용 섹션을 참조하세요. 버킷에 대한 액

세스를 제어하기 위한 버킷 정책 사용에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서 의 킷 정책 및 사용자 정책과 Amazon S3가 요청을 승인하는 방법을 참조하세요.

분류 오류: 잘못된 콘텐츠

이 유형의 분류 오류는 Macie가 S3 버킷의 객체를 분석하려고 하는데 객체의 형식이 잘못되었거나 객체에 민감한 데이터 검색 할당량을 초과하는 콘텐츠가 포함된 경우 발생합니다. Macie는 객체를 분석할 수 없습니다.

세부 정보

이 오류는 일반적으로 S3 객체가 형식이 잘못되었거나 손상된 파일이기 때문에 발생합니다. 따라서 Macie는 파일의 모든 데이터를 파싱하고 분석할 수 없습니다.

이 오류는 S3 객체 분석이 개별 파일의 민감한 데이터 검색 할당량을 초과하는 경우에도 발생할 수 있습니다. 예를 들어, 객체의 스토리지 크기가 해당 유형의 파일에 대한 크기 할당량을 초과하는 경우가 있습니다.

어느 경우든 Macie는 S3 객체에 대한 분석을 완료할 수 없으며, 객체의 분석 상태는 건너뜀(SKIPPED)입니다.

수정 지침

이 오류를 조사하려면 S3 객체를 다운로드하고 파일의 형식과 내용을 확인하세요. 또한 민감한 데이터 검색을 위해 Macie 할당량을 기준으로 파일 내용을 평가하세요.

이 오류를 수정하지 않으면 Macie는 S3 버킷의 다른 객체를 분석하려고 시도합니다. Macie가 다른 객체를 성공적으로 분석하면 Macie는 버킷에 대해 제공하는 적용 범위 데이터 및 기타 정보를 업데이트합니다.

추가 참조

특정 유형의 파일에 대한 할당량을 비롯한 민감한 데이터 검색 할당량 목록은 Amazon Macie 할당량 섹션을 참조하세요. Macie가 민감도 점수를 업데이트하는 방법가 S3 버킷에 대해 제공하는 기타 정보에 대한 자세한 내용은 민감한 데이터 자동 검색의 작동 방식 섹션을 참조하세요.

분류 오류: 잘못된 암호화

이 유형의 분류 오류는 Macie가 S3 버킷의 객체를 분석하려고 시도하고 객체가 고객 제공 키로 암호화되는 경우 발생합니다. 객체는 SSE-C 암호화를 사용하므로 Macie는 객체를 검색하고 분석할 수 없습니다.

세부 정보

Amazon S3는 S3 객체에 대한 여러 암호화 옵션을 지원합니다. 대부분의 경우 Macie는 계정의 Macie 서비스 연결 역할을 사용하여 객체의 암호를 해독할 수 있습니다. 하지만, 이는 사용된 암호화 유형에 따라 달라질 수 있습니다.

Macie가 S3 객체의 암호를 해독하려면 해당 객체는 Macie가 액세스할 수 있고 사용할 수 있는 키로 암호화되어 있어야 합니다. 객체가 고객 제공 키로 암호화된 경우 Macie는 Amazon S3에서 객체를 검색하는 데 필요한 키 자료를 제공할 수 없습니다. 따라서 Macie는 객체를 분석할 수 없고 객체에 대한 분석 상태는 건너뜀(SKIPPED)입니다.

수정 지침

이 오류를 해결하려면 Amazon S3 관리 키 또는 AWS Key Management Service (AWS KMS) 키로 S3 객체를 암호화하십시오. AWS KMS 키를 사용하려는 경우 키는 AWS 관리형 KMS 키 또는 Macie가 사용할 수 있는 고객 관리형 KMS 키일 수 있습니다.

Macie가 액세스하여 사용할 수 있는 키로 기존 S3 객체를 암호화하려면 객체의 암호화 설정을 변경하면 됩니다. Macie가 액세스하여 사용할 수 있는 키로 새 객체를 암호화하려면 S3 버킷의 기본 암호화 설정을 변경합니다. 또한 버킷 정책에 따라 고객 제공 키로 새 객체를 암호화해야는지 확인하세요.

이 오류를 수정하지 않으면 Macie는 S3 버킷의 다른 객체를 분석하려고 시도합니다. Macie가 다른 객체를 성공적으로 분석하면 Macie는 버킷에 대해 제공하는 적용 범위 데이터 및 기타 정보를 업데이트합니다.

추가 참조

Macie를 사용하여 암호화된 S3 객체를 분석하기 위한 요구 사항 및 옵션에 대한 자세한 내용은 Amazon Macie를 사용한 암호화된 Amazon S3 객체 분석 섹션을 참조하세요. S3 버킷의 암호화 옵션 및 설정에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 암호화로 데이터 보호 및 S3 버킷에 대한 기본 서버 측 암호화 동작 설정 섹션을 참조하세요.

분류 오류: 잘못된 KMS 키

이 유형의 분류 오류는 Macie가 S3 버킷의 객체를 분석하려고 할 때 더 이상 사용할 수 없는 AWS Key Management Service (AWS KMS) 키로 객체를 암호화하는 경우 발생합니다. Macie는 객체를 검색하고 분석할 수 없습니다.

세부 정보

AWS KMS 고객 관리를 비활성화 및 삭제할 수 있는 옵션을 제공합니다. AWS KMS keys S3 객체가 비활성화된 KMS 키로 암호화되었거나, 삭제 예정이거나, 삭제된 경우, Macie는 객체를 검색하고 암호를 해독할 수 없습니다. 따라서 Macie는 객체를 분석할 수 없고 객체에 대한 분석 상태는 건너뜀(SKIPPED)입니다. Macie가 암호화된 객체를 분석하려면 해당 객체는 Macie가 액세스할 수 있고 사용할 수 있는 키로 암호화되어 있어야 합니다.

수정 지침

이 오류를 해결하려면 키의 현재 상태에 따라 해당 AWS KMS key의 예정된 삭제를 다시 활성화하거나 취소하세요. 해당 키가 이미 삭제된 경우 이 오류를 수정할 수 없습니다.

어느 것이 S3 객체를 암호화하는 데 AWS KMS key 사용되었는지 확인하려면 먼저 Macie를 사용하여 S3 버킷의 서버 측 암호화 설정을 검토할 수 있습니다. 버킷의 기본 암호화 설정이 KMS 키를 사용하도록 구성된 경우, 버킷의 세부 정보에 사용되는 키가 표시됩니다. 그리고 해당 키의 상태를 확인할 수 있습니다. 또는 Amazon S3를 사용하여 버킷과 버킷의 개별 객체에 대한 암호화 설정을 검토할 수 있습니다.

이 오류를 수정하지 않으면 Macie는 S3 버킷의 다른 객체를 분석하려고 시도합니다. Macie가 다른 객체를 성공적으로 분석하면 Macie는 버킷에 대해 제공하는 적용 범위 데이터 및 기타 정보를 업데이트합니다.

추가 참조

Macie를 사용하여 S3 버킷의 서버 측 암호화 설정을 검토하는 방법에 대한 자세한 내용은 S3 버킷의 세부 정보 검토 섹션을 참조하세요. 예약된 삭제를 다시 활성화하거나 취소하는 방법에 대한 자세한 내용은 개발자 안내서의 키 활성화 및 비활성화 AWS KMS key, 키 삭제 예약 및 취소를 참조하십시오.AWS Key Management Service

분류 오류: 권한이 거부됨

이 유형의 분류 오류는 Macie가 S3 버킷의 객체를 분석하려고 하는데 객체에 대한 권한 설정 또는 객체 암호화에 사용된 키의 권한 설정으로 인해 Macie가 객체를 검색하거나 해독할 수 없는 경우에 발생합니다. Macie는 객체를 검색하고 분석할 수 없습니다.

세부 정보

이 오류는 일반적으로 S3 객체가 Macie가 사용할 수 없는 고객 관리형 AWS Key Management Service (AWS KMS) 키로 암호화되어 있기 때문에 발생합니다. 고객이 관리하는 AWS KMS key방

식으로 객체를 암호화하는 경우 키 정책에 따라 Macie가 키를 사용하여 데이터를 해독할 수 있도록 허용해야 합니다.

Amazon S3 권한 설정으로 인해 Macie가 S3 객체를 검색하지 못하는 경우에도 이 오류가 발생할 수 있습니다. S3 버킷의 버킷 정책은 특정 버킷 객체에 대한 액세스를 제한하거나 특정 주체(사용자, 계정, 서비스 또는 기타 엔터티)만 객체에 액세스하도록 허용할 수 있습니다. 또는 객체의 액세스 제어 목록(ACL)이 객체에 대한 액세스를 제한할 수 있습니다. 따라서 Macie는 객체에 액세스하지 못할 수 있습니다.

위의 모든 경우 Macie는 객체를 검색 및 분석할 수 없으며, 객체의 분석 상태는 건너뜀(SKIPPED)입니다.

수정 지침

이 오류를 해결하려면 S3 객체가 고객 관리형 AWS KMS key(으)로 암호화되어 있는지 확인하세요. 그렇다면 키의 정책에서 Macie 서비스 연결 역할(AWSServiceRoleForAmazonMacie)이 키로 데이터를 해독하도록 허용하는지 확인하세요. 이 액세스를 허용하는 방법은 를 소유한 계정이 객체를 저장하는 S3 AWS KMS key 버킷도 소유하고 있는지 여부에 따라 달라집니다. 동일한 계정이 KMS 키와 버킷을 소유한 경우, 해당 계정의 사용자가 키 정책을 업데이트해야 합니다. 한 계정이 KMS 키를 소유하고 다른 계정이 버킷을 소유하는 경우, 키를 소유한 계정의 사용자는 키에 대한 크로스 계정 액세스를 허용해야 합니다.

> **Tip**
>
> Macie가 계정의 S3 버킷에 AWS KMS keys 있는 객체를 분석하기 위해 액세스해야 하는 모든 고객 관리 대상 목록을 자동으로 생성할 수 있습니다. 이렇게 하려면 Amazon Macie Scripts 리포지토리에서 사용할 수 있는 AWS KMS 권한 분석기 스크립트를 실행하십시오. GitHub 스크립트는 AWS Command Line Interface (AWS CLI) 명령의 추가 스크립트를 생성할 수도 있습니다. 선택적으로 이러한 명령을 실행하여 지정한 KMS 키의 필수 구성 설정 및 정책을 업데이트할 수 있습니다.

Macie가 이미 해당 객체를 사용할 수 있도록 AWS KMS key 허용되었거나 S3 객체가 고객 관리형 KMS 키로 암호화되지 않은 경우, 버킷 정책에서 Macie가 객체에 액세스할 수 있도록 허용하는지 확인하십시오. 또한 객체의 ACL이 Macie가 객체의 데이터 및 메타데이터를 읽을 수 있도록 허용하는지도 확인합니다.

버킷 정책의 경우 Macie 서비스 연결 역할에 대한 조건을 정책에 추가하여 이러한 액세스를 허용할 수 있습니다. 조건은 Macie 서비스 연결 역할이 정책의 Deny 제한과 일치하지 않도록 해야 합니다.

`aws:PrincipalArn` 전역 조건 컨텍스트 키와 계정에 대한 Macie 서비스 연결 역할의 Amazon 리소스 이름(ARN)을 사용하여 이 작업을 수행할 수 있습니다.

객체 ACL의 경우 객체 소유자와 협의해 객체에 대한 권한이 있는 AWS 계정 수혜자로 추가함으로써 이러한 액세스를 허용할 수 있습니다. `READ` 그러면 Macie는 계정의 서비스 연결 역할을 사용하여 객체를 검색하고 분석할 수 있습니다. 또한 버킷의 객체 소유권 설정을 변경하는 것도 고려해 보세요. 이러한 설정을 사용하여 버킷의 모든 객체에 대한 ACL을 비활성화하고 버킷을 소유한 계정에 소유권 권한을 부여할 수 있습니다.

이 오류를 수정하지 않으면 Macie는 S3 버킷의 다른 객체를 분석하려고 시도합니다. Macie가 다른 객체를 성공적으로 분석하면 Macie는 버킷에 대해 제공하는 적용 범위 데이터 및 기타 정보를 업데이트합니다.

추가 참조

Macie가 고객 관리형 AWS KMS key을(를) 사용하여 데이터를 해독하도록 허용하는 방법에 대한 자세한 내용은 Amazon Macie가 고객 관리형 앱을 사용할 수 있도록 허용 AWS KMS key 섹션을 참조하세요. Macie가 버킷에 액세스할 수 있도록 S3 버킷 정책을 업데이트하는 방법에 대한 자세한 내용은 Amazon Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용 섹션을 참조하세요.

키 정책 업데이트에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 변경을 참조하세요. 고객 관리형 AWS KMS keys S3 객체 암호화에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 AWS KMS 키를 사용한 서버 측 암호화 사용을 참조하십시오.

S3 버킷에 대한 액세스를 제어하기 위한 버킷 정책 사용에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서 의 버킷 정책 및 사용자 정책과 Amazon S3가 요청을 승인하는 방법을 참조하세요. ACL 또는 객체 소유권 설정을 사용하여 S3 객체에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 ACL을 통한 액세스 관리 및 객체 소유권 제어 및 버킷에 대해 ACL 사용 중지 섹션을 참조하세요.

분류 불가

이 문제는 S3 버킷의 모든 객체가 지원되지 않는 Amazon S3 스토리지 클래스 또는 지원되지 않는 파일 또는 스토리지 형식을 사용하여 저장되었음을 나타냅니다. Macie이 버킷에 있는 모든 객체를 분석할 수 없습니다.

세부 정보

선택 및 분석에 적합하려면 S3 객체가 Macie가 지원하는 Amazon S3 스토리지 클래스를 사용해야 합니다. 또한 객체에는 Macie가 지원하는 파일 또는 스토리지 형식의 파일 이름 확장자가 있어야

합니다. 객체가 이러한 기준을 충족하지 않는 경우 해당 객체는 분류할 수 없는 객체로 취급됩니다. Macie는 분류할 수 없는 객체의 데이터를 검색하거나 분석하려고 시도하지 않습니다.

S3 버킷의 모든 객체가 분류할 수 없는 객체인 경우 전체 버킷은 분류할 수 없는 버킷입니다. Macie는 버킷에 대해 민감한 데이터 자동 검색을 수행할 수 없습니다.

수정 지침

이 문제를 해결하려면 S3 버킷에 객체를 저장하는 데 사용되는 스토리지 클래스를 결정하는 수명 주기 구성 규칙 및 기타 설정을 검토하세요. Macie가 지원하는 스토리지 클래스를 사용하도록 이러한 설정을 조정하는 것을 고려해 보세요. 버킷에 있는 기존 객체의 스토리지 클래스를 변경할 수도 있습니다.

또한 S3 버킷에 있는 기존 객체의 파일 및 스토리지 형식을 평가합니다. 객체를 분석하려면 지원되는 형식을 사용하는 새 객체로 데이터를 일시적 또는 영구적으로 이식하는 것을 고려해 보세요.

객체가 S3 버킷에 추가되고 지원되는 스토리지 클래스와 형식을 사용하는 경우, Macie는 다음에 버킷 인벤토리를 평가할 때 객체를 감지합니다. 이 경우 Macie는 Amazon S3 데이터에 대해 제공하는 통계, 적용 범위 데이터 및 기타 정보에서 버킷을 분류할 수 없음으로 보고하는 것을 중단합니다. 또한 후속 분석 주기에서는 새로운 객체가 분석에서 우선 순위가 높아지게 됩니다.

추가 참조

Amazon S3 스토리지 클래스와 Macie가 지원하는 파일 및 스토리지 형식에 대한 자세한 내용은 Amazon Macie에서 지원하는 스토리지 클래스 및 형식 섹션을 참조하세요. 수명 주기 구성 규칙 및 Amazon S3에서 제공하는 스토리지 클래스 옵션에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 스토리지 수명 주기 관리 및 Amazon S3 스토리지 클래스 사용 섹션을 참조하세요.

민감한 데이터 자동 검색 통계 및 결과 검토

민감한 데이터 자동 검색이 활성화된 경우 Amazon Macie는 Amazon Simple Storage Service (Amazon S3) 범용 버킷에 대한 추가 인벤토리 데이터, 통계 및 기타 정보를 자동으로 생성하고 유지 관리하며, 이 버킷은 계정에 대해 모니터링하고 분석합니다. 조직의 Macie 관리자인 경우 기본적으로 여기에는 구성원 계정이 소유한 S3 버킷이 포함됩니다.

추가 정보는 Macie가 지금까지 수행한 자동화된 민감한 데이터 검색 활동의 결과를 캡처합니다. 또한 개별 S3 버킷에 대한 퍼블릭 액세스 및 암호화 설정과 같이, Macie가 Amazon S3 데이터에 대해 제공하는 기타 정보를 보완합니다. 메타데이터 및 통계 외에도 Macie는 발견한 민감한 데이터와 해당 데이터가 수행하는 분석 (민감한 데이터 검색 결과 및 민감한 데이터 검색 결과) 에 대한 기록을 생성합니다.

민감한 데이터 자동 검색이 매일 진행됨에 따라 다음 기능 및 데이터를 사용하여 결과를 검토하고 평가할 수 있습니다.

- 요약 대시보드 - Amazon S3 데이터 자산에 대한 집계 통계를 제공합니다. 통계에는 Macie가 민감한 데이터를 찾은 총 버킷 수, 퍼블릭 액세스가 가능한 버킷 수와 같은 주요 지표에 대한 데이터가 포함됩니다. 또한 Amazon S3 데이터 범위에 영향을 미치는 문제도 보고합니다.
- S3 버킷 히트 맵 - 데이터 자산 전반의 데이터 민감도를 대화형 방식으로 시각적으로 표현하며, AWS 계정별로 그룹화됩니다. 각 계정의 맵에는 집계된 민감도 통계가 포함되어 있으며, 색상을 사용하여 계정이 소유한 각 버킷의 현재 민감도 점수를 나타냅니다. 또한 맵에서는 기호를 사용하여 공개적으로 액세스할 수 있는 버킷과 Macie가 분석할 수 없는 버킷 등을 식별하는 데 도움을 줍니다.
- S3 버킷 테이블 - 인벤토리의 각 S3 버킷에 대한 요약 정보를 제공합니다. 각 버킷에 대해 테이블에는 버킷의 현재 민감도 점수, Macie가 버킷에서 분석할 수 있는 객체 수, 버킷의 객체를 정기적으로 분석하도록 민감한 데이터 검색 작업을 구성했는지 여부 등의 데이터가 포함됩니다. 테이블의 데이터를 CSV (쉼표로 구분된 값) 파일로 내보낼 수 있습니다.
- 세부 정보 패널 - 히트 맵 또는 테이블에서 선택한 S3 버킷에 대한 세부 정보 및 통계를 제공합니다. 세부 정보에는 Macie가 버킷에서 분석한 객체 목록과 Macie가 버킷에서 발견한 민감한 데이터의 유형 및 발생 횟수에 대한 분석이 포함됩니다. 패널을 사용하여 버킷의 자동 검색 설정을 관리할 수도 있습니다.
- 민감한 데이터 조사 결과 - Macie가 개별 S3 객체에서 발견한 민감한 데이터에 대한 자세한 보고서를 제공합니다. 세부 정보에는 Macie가 발견한 민감한 데이터의 유형 및 발생 횟수가 포함됩니다. 세부 정보에는 버킷의 퍼블릭 액세스 설정, 객체가 가장 최근에 변경된 시기 등 영향을 받는 S3 버킷 및 객체에 대한 정보도 포함됩니다.
- 민감한 데이터 검색 결과 - Macie가 개별 S3 객체에 대해 수행한 분석 기록을 제공합니다. 여기에는 Macie가 민감한 데이터를 찾지 못한 객체 및 문제나 오류로 인해 Macie가 분석할 수 없는 객체가 포함됩니다. Macie가 개체에서 민감한 데이터를 발견한 경우 중요한 데이터 검색 결과에는 Macie가 찾은 민감한 데이터에 대한 정보가 제공됩니다.

이 데이터를 사용하여 Amazon S3 데이터 자산 전반의 데이터 민감도를 평가하고 개별 S3 버킷과 객체를 자세히 평가하고 조사할 수 있습니다. Macie가 Amazon S3 데이터의 보안 및 개인 정보 보호에 대해 제공하는 정보를 결합하여 즉각적인 수정이 필요한 경우도 식별할 수 있습니다(예: Macie가 민감한 데이터를 발견한 공개적으로 액세스할 수 있는 버킷).

추가 데이터는 Amazon S3 데이터 자산의 적용 범위를 평가하고 모니터링하는 데 도움이 될 수 있습니다. 적용 범위 데이터를 사용하면 전체 데이터 자산과 버킷 인벤토리의 개별 S3 버킷에 대한 분석 상태를 확인할 수 있습니다. 또한 Macie가 특정 버킷의 객체를 분석하지 못하게 하는 문제를 식별할 수 있

습니다. 문제를 해결하면 후속 분석 주기 동안 Amazon S3 데이터의 적용 범위를 늘릴 수 있습니다. 자세한 정보는 민감한 데이터 자동 검색 범위 평가을 참조하세요.

주제

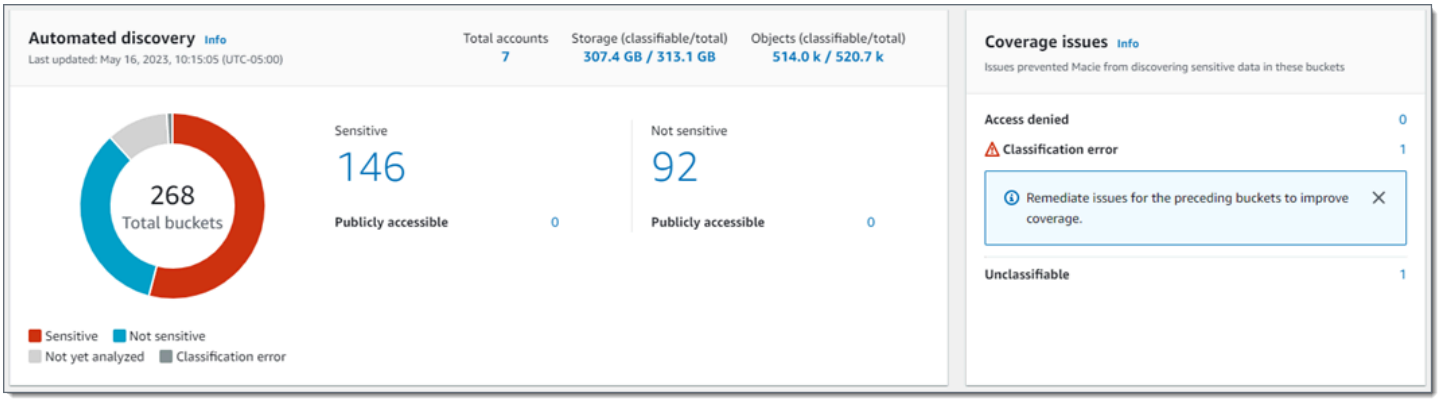
- 요약 대시보드에서 집계된 데이터 민감도 통계 검토
- S3 버킷 맵을 사용한 데이터 민감도 시각화
- S3 버킷 테이블을 사용한 데이터 민감도 평가
- 개별 S3 버킷의 데이터 민감도 세부 정보 검토
- 자동 검색으로 생성된 민감한 데이터 분석 조사 결과 분석
- 자동 검색으로 생성된 민감한 데이터 검색 결과에 액세스

요약 대시보드에서 집계된 데이터 민감도 통계 검토

Amazon Macie 콘솔의 요약 대시보드는 현재 AWS 리전의 Amazon Simple Storage Service(S3) 데이터에 대한 집계된 통계 및 조사 결과 데이터의 스냅샷을 제공합니다. Amazon S3 데이터의 전반적인 보안 상태를 평가하는 데 도움이 되도록 설계되었습니다.

대시보드 통계에는 공개적으로 액세스할 수 있거나 다른 사람과 공유되는 S3 범용 버킷 수와 같은 주요 보안 지표에 대한 데이터가 포함됩니다. AWS 계정또한 대시보드에는 계정에 대해 집계된 결과 데이터 그룹 (예: 지난 7일 동안 가장 많은 검색 결과를 생성한 버킷) 이 표시됩니다. 조직의 Macie 관리자인 경우, 대시보드는 조직 내 모든 계정에 대한 집계된 통계 및 데이터를 제공합니다. 필요에 따라 계정별로 데이터를 필터링할 수 있습니다.

민감한 데이터 자동 검색이 활성화된 경우 요약 대시보드에는 자동 검색 통계가 포함됩니다. 통계는 Macie가 Amazon S3 데이터에 대해 지금까지 수행한 민감한 데이터 자동 검색 활동의 상태 및 결과를 수집합니다. 예:



자동 검색 섹션의 통계는 자동화된 민감한 데이터 검색 활동의 현재 상태 및 결과에 대한 스냅샷을 제공합니다. 만들고 실행한 민감한 데이터 검색 작업의 결과는 데이터에 포함되지 않습니다.

적용 범위 문제 섹션의 통계는 Macie가 문제로 인해 개별 S3 버킷의 객체를 분석하지 못하는지 여부를 나타냅니다. 이러한 통계에는 사용자가 만들고 실행한 민감한 데이터 검색 작업에 대한 데이터가 명시적으로 포함되지 않습니다. 하지만 자동화된 민감한 데이터 검색 결과에 영향을 미치는 적용 범위 문제를 해결하면 이후에 실행하는 작업의 적용 범위도 늘어날 수 있습니다.

주제

- 요약 대시보드 표시
- 요약 대시보드의 민감한 데이터 자동 검색 통계 이해

요약 대시보드 표시

다음 단계에 따라 Amazon Macie 콘솔에 요약 대시보드를 표시할 수 있습니다. 프로그래밍 방식으로 통계를 쿼리하려는 경우 Amazon Macie API의 GetBucketStatistics작업을 사용할 수 있습니다.

요약 대시보드를 표시하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다. Macie는 요약 대시보드를 표시합니다.
3. 대시보드의 항목에 대한 지원 데이터를 자세히 살펴보고 검토하려면 해당 항목을 선택합니다.

조직의 Macie 관리자인 경우, 대시보드는 사용자의 계정 및 조직의 멤버 계정에 대한 집계된 통계 및 데이터를 표시합니다. 대시보드를 필터링하고 특정 계정에 대한 데이터만 표시하려면 계정 상자에 계정 ID를 입력합니다.

요약 대시보드의 민감한 데이터 자동 검색 통계 이해

Amazon Macie 콘솔의 요약 대시보드에는 Amazon S3 데이터에 대한 자동 민감한 데이터 검색을 모니터링하는 데 도움이 되는 집계된 통계가 포함되어 있습니다. 현재 Amazon S3 데이터의 현재 상태 및 분석 결과에 대한 스냅샷을 제공합니다. AWS 리전

예를 들어 대시보드 통계를 사용하여 Amazon Macie가 민감한 데이터를 발견한 S3 버킷의 수와 이러한 버킷 중 공개적으로 액세스할 수 있는 버킷의 수를 신속하게 파악할 수 있습니다. 또한 Amazon S3 데이터의 적용 범위를 평가하고 Macie가 개별 S3 버킷의 객체를 분석하지 못하게 하는 문제를 식별할 수 있습니다.

대시보드에는 민감한 데이터 자동 검색 통계가 주로 다음 섹션으로 구성되어 있습니다.

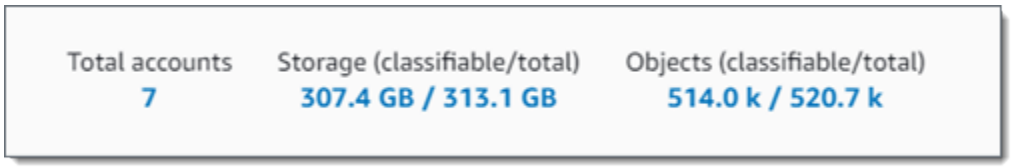
- 스토리지 및 민감한 데이터 검색
- 자동 검색
- 적용 범위 문제

각 섹션을 검토할 때는 선택적으로 드릴다운할 항목을 선택하여 지원 데이터를 검토할 수 있습니다. 또한 대시보드에는 S3 디렉터리 버킷에 대한 데이터는 포함되지 않고 범용 버킷만 포함됩니다. Macie는 디렉터리 버킷을 모니터링하거나 분석하지 않습니다.

각 섹션의 개별 통계는 다음과 같습니다. 요약 대시보드의 다른 섹션에 있는 통계에 대한 자세한 내용은 요약 대시보드의 구성 요소 이해 섹션을 참조하세요.

스토리지 및 민감한 데이터 검색

자동 검색 섹션 상단에는 Amazon S3에 저장하는 데이터의 양과 Macie가 민감한 데이터를 탐지하기 위해 분석할 수 있는 데이터의 양을 나타내는 통계가 있습니다. 예:



이 섹션:

- 전체 계정 — 버킷 인벤토리에 AWS 계정 있는 자체 버킷의 총 수입니다. 조직의 Macie 관리자인 경우, 이 수는 조직을 위해 관리하는 Macie 계정의 총 개수입니다. 독립형 Macie 계정이 있는 경우, 이 값은 1입니다.
- 스토리지 - 이 지표는 버킷 인벤토리에 있는 객체의 스토리지 크기에 대한 정보를 제공합니다.
  - 분류 가능 - Macie가 버킷에서 분석할 수 있는 모든 객체의 총 스토리지 크기입니다.
  - 합계 - Macie가 분석할 수 없는 객체를 포함하여 버킷에 있는 모든 객체의 총 스토리지 크기입니다.

  객체가 압축된 파일인 경우, 이러한 값은 압축을 푼 후의 해당 파일의 실제 크기를 반영하지 않습니다. 모든 버킷에 버전 관리가 활성화된 경우, 이 값은 해당 버킷에 있는 각 객체의 최신 버전 스토리지 크기를 기반으로 합니다.
- 객체- 이 지표는 버킷 인벤토리의 객체 수에 대한 정보를 제공합니다.
  - 분류 가능 - Macie가 버킷에서 분석할 수 있는 총 객체 수입니다.

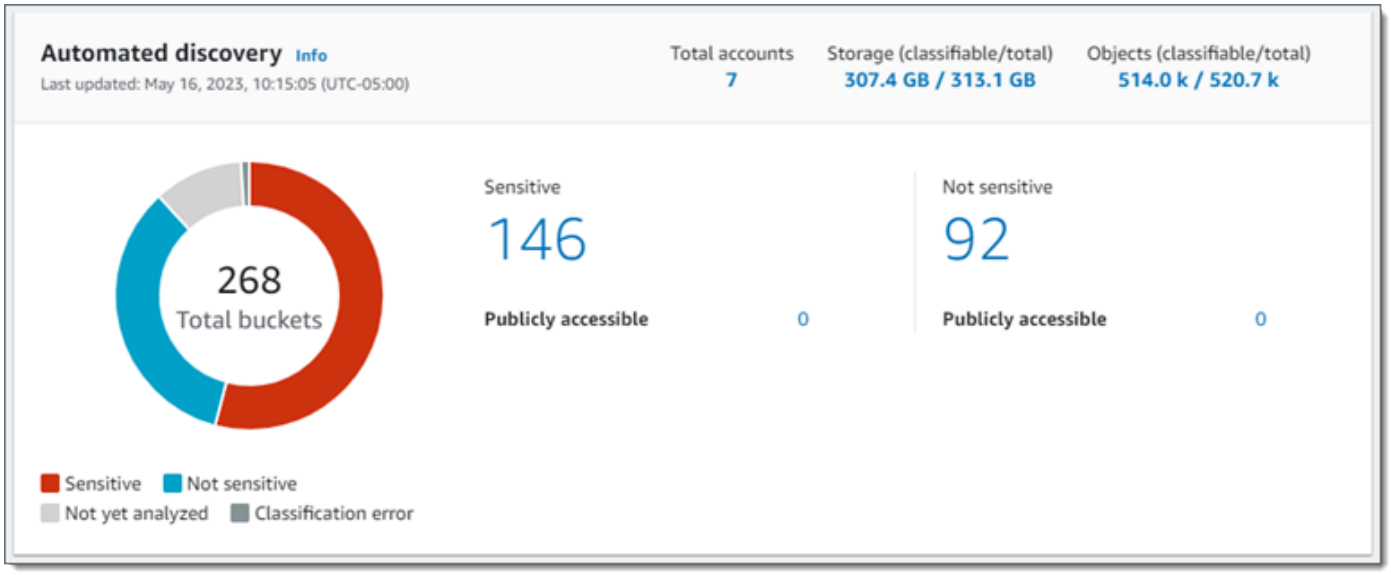
- 합계 - Macie가 분석할 수 없는 객체를 포함하여 버킷에 있는 총 객체 수입니다.

위 통계에서 데이터와 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자가 있는 경우, 분류 가능합니다. Macie를 사용하여 객체에서 민감한 데이터를 탐지할 수 있습니다. 자세한 내용은 지원하는 스토리지 클래스 및 형식 섹션을 참조하세요.

참고로 스토리지 및 객체 통계에는 Macie가 액세스할 수 없는 버킷의 객체에 대한 데이터는 포함되지 않습니다. 이런 경우가 있는 버킷을 식별하려면 대시보드의 적용 범위 문제 섹션에서 액세스 거부 통계를 선택하세요.

자동 검색

이러한 통계는 주로 Macie가 Amazon S3 데이터에 대해 지금까지 수행한 민감한 데이터 자동 검색 활동의 상태와 결과를 수집합니다. 예:



이 섹션의 개별 통계는 다음과 같습니다.

총 버킷

도넛형 차트는 버킷 인벤토리의 총 버킷 수를 나타냅니다. 차트는 각 버킷의 현재 민감도 점수를 기준으로 버킷을 범주별로 그룹화합니다.

- 민감도(빨간색) - 민감도 점수 범위가 51~100인 버킷의 총 수입니다.
- 민감하지 않음(파란색) - 민감도 점수 범위가 1~49인 버킷의 총 수입니다.
- 아직 분석되지 않음(밝은 회색) - 민감도 점수가 50인 버킷의 총 수입니다.
- 분류 오류(짙은 회색)- 민감도 점수가 -1인 버킷의 총 수입니다.

Macie가 정의하는 민감도 점수 및 레이블의 범위에 대한 자세한 내용은 S3 버킷의 민감도 점수 섹션을 참조하세요.

그룹에 대한 추가 통계를 검토하려면 그룹 위로 마우스를 가져갑니다.

- 버킷 – 버킷의 총수
- 퍼블릭 액세스 가능 - 일반 대중이 버킷에 대한 읽기 또는 쓰기 액세스 권한을 가질 수 있는 버킷의 총 수입니다.
- 분류 가능한 바이트는 가 버킷에서 분석할 수 있는 모든 객체의 총 스토리지 크기입니다. 이러한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하며 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가집니다. 자세한 정보는 지원하는 스토리지 클래스 및 형식을 참조하세요.
- 총 바이트 - 모든 버킷의 총 스토리지 크기입니다.

위 통계에서 스토리지 크기 값은 버킷에 있는 각 객체의 최신 버전 스토리지 크기를 기반으로 합니다. 객체가 압축된 파일인 경우, 이러한 값은 압축을 푼 후의 해당 파일의 실제 크기를 반영하지 않습니다.

민감함

이 영역은 현재 민감도 점수가 51~100 범위인 버킷의 총 수를 나타냅니다. 이 그룹 내에서 퍼블릭 액세스 가능은 일반 사용자도 버킷에 대한 읽기 또는 쓰기 액세스 권한을 가질 수 있는 버킷의 총 수를 나타냅니다.

민감하지 않음

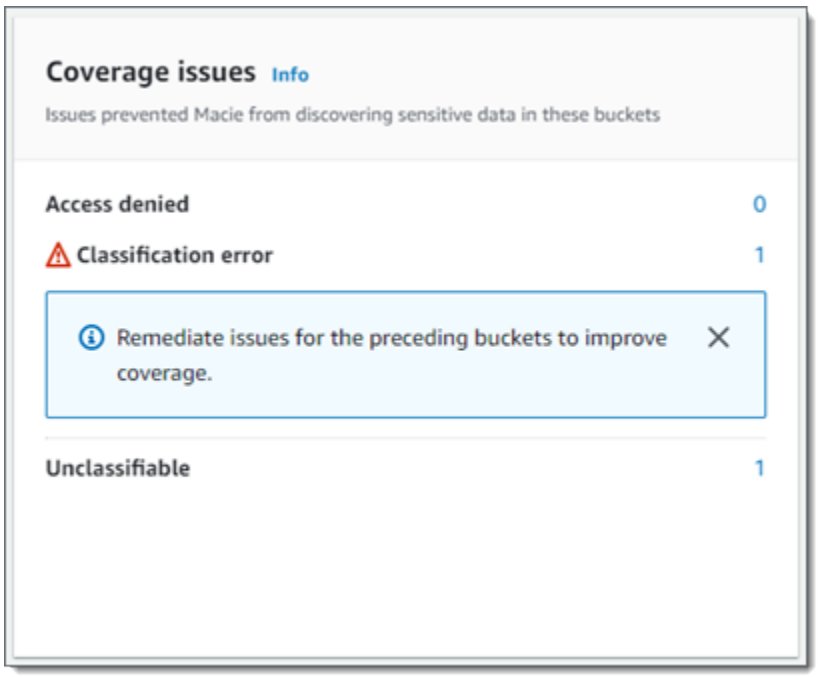
이 영역은 현재 민감도 점수가 1~49인 버킷의 총 수를 나타냅니다. 이 그룹 내에서 퍼블릭 액세스 가능은 일반 사용자도 버킷에 대한 읽기 또는 쓰기 액세스 권한을 가질 수 있는 버킷의 총 수를 나타냅니다.

퍼블릭 액세스 가능한 통계의 값을 결정하고 계산하기 위해 Macie는 계정과 버킷의 퍼블릭 액세스 차단 설정, 버킷의 버킷 정책 등 각 버킷에 대한 계정 및 버킷 수준 설정의 조합을 분석합니다. 자세한 정보는 Macie가 Amazon S3 데이터 보안을 모니터링하는 방법을 참조하세요.

단, 자동 검색 섹션의 통계에는 사용자가 만들고 실행한 민감한 데이터 검색 작업의 결과가 포함되지 않습니다.

적용 범위 문제

이 통계는 특정 유형의 문제로 인해 Macie가 개별 S3 버킷의 객체를 분석하지 못하는지 여부를 나타냅니다. 예:



이 섹션:

- 액세스 거부됨 - Macie가 액세스할 수 없는 버킷의 총 개수입니다. Macie는 이러한 버킷의 객체를 분석할 수 없습니다. 버킷의 권한 설정으로 인해 Macie는 버킷과 버킷의 객체에 액세스할 수 없습니다.
- 분류 오류 - 객체 수준 분류 오류로 인해 Macie가 아직 분석하지 않은 버킷의 총 수입니다. Macie는 이러한 버킷에 있는 하나 이상의 객체를 분석하려고 했습니다. 하지만 Macie는 객체 수준 권한 설정, 객체 콘텐츠 또는 할당량 관련 문제로 인해 객체를 분석할 수 없었습니다.
- 분류 불가 - 분류 가능한 객체를 저장하지 않는 버킷의 총 수입니다. Macie는 이러한 버킷의 객체를 분석할 수 없습니다. 모든 객체가 Macie가 지원하지 않는 Amazon S3 스토리지 클래스를 사용하거나 Macie가 지원하지 않는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가지고 있습니다.

통계 값을 선택하면 추가 세부 정보가 표시되고, 해당하는 경우, 수정 지침이 표시됩니다. 액세스 문제 및 분류 오류를 수정하면 후속 분석 주기 동안 Amazon S3 데이터의 적용 범위를 늘릴 수 있습니다. 자세한 정보는 민감한 데이터 자동 검색 범위 평가을 참조하세요.

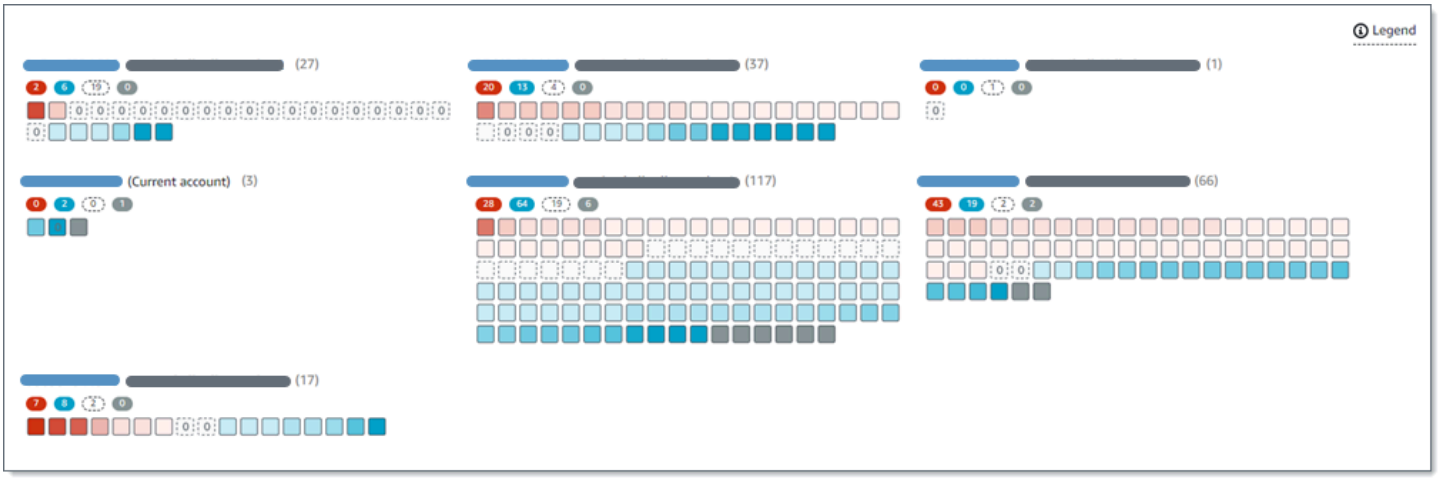
참고로 커버리지 이슈 섹션의 통계에는 사용자가 만들고 실행한 민감한 데이터 검색 작업에 대한 데이터가 명시적으로 포함되지 않습니다. 하지만 자동화된 민감한 데이터 검색 결과에 영향을 미치는 적용 범위 문제를 해결하면 이후에 실행하는 작업의 적용 범위도 늘어날 수 있습니다.

요약 대시보드의 다른 섹션에 대한 자세한 내용은 요약 대시보드의 구성 요소 이해 섹션을 참조하세요.

S3 버킷 맵을 사용한 데이터 민감도 시각화

Amazon Macie 콘솔의 S3 버킷 히트 맵은 Amazon Simple Storage Service (Amazon S3) 데이터 자산 전체의 데이터 민감도를 대화형 방식으로 시각적으로 보여줍니다. Macie가 현재 AWS 리전 Amazon S3 데이터에 대해 지금까지 수행한 자동화된 민감한 데이터 검색 활동의 결과를 캡처합니다.

조직의 Macie 관리자인 경우 구성원 계정이 소유한 S3 버킷의 결과가 맵에 포함됩니다. 데이터는 계정 ID별로 AWS 계정 그룹화되고 정렬됩니다. 예:



맵의 각 페이지에는 조직 또는 Amazon S3 데이터 자산의 규모에 따라 최대 99개의 계정 또는 1,000개의 버킷에 대한 데이터가 표시됩니다.

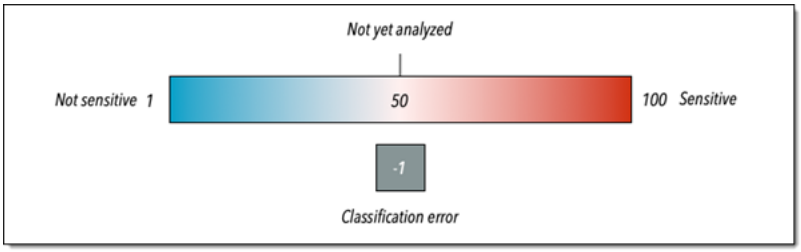
맵을 표시하려면 콘솔의 탐색 창에서 S3 버킷을 선택합니다. 페이지 상단에서 맵 ( ) 을 선택합니다. 맵은 현재 계정 또는 조직에서 민감한 데이터 자동 검색이 활성화된 경우에만 사용할 수 있습니다. 사용자가 만들고 실행한 민감한 데이터 검색 작업의 결과는 포함되지 않습니다.

주제

- S3 버킷 맵의 데이터 해석
- S3 버킷 맵과 상호 작용

S3 버킷 맵의 데이터 해석

S3 버킷 맵에서 각 사각형은 버킷 인벤토리에 있는 S3 범용 버킷을 나타냅니다. 사각형의 색상은 버킷의 현재 민감도 점수를 나타내며, 이 점수는 두 가지 기본 차원, 즉 Macie가 버킷에서 발견한 민감한 데이터의 양과 Macie가 버킷에서 분석한 데이터의 양의 교차점을 측정합니다. 색상의 강도는 다음 이미지와 같이 데이터 민감도 값 범위에서 버킷의 점수가 어디에 속하는지를 나타냅니다.



일반적으로 색상과 색상의 강도는 다음과 같이 해석할 수 있습니다.

- 파란색 - 버킷의 현재 민감도 점수 범위가 1~49인 경우, 버킷의 사각형은 파란색이고 버킷의 민감도 레이블은 민감하지 않음입니다. 파란색의 강도는 Macie가 버킷에 있는 고유한 객체의 총 개수를 기준으로 버킷에서 분석한 고유한 객체의 수를 반영합니다. 색상이 어두울수록 낮은 민감도 점수를 나타냅니다.
- 색상 없음 - 버킷의 현재 민감도 점수가 50인 경우, 버킷의 사각형에는 색상이 지정되지 않으며 버킷의 민감도 레이블은 아직 분석되지 않음입니다. 또한 사각형에는 점선 테두리가 있습니다.
- 빨간색 - 버킷의 현재 민감도 점수 범위가 51~100인 경우, 버킷의 사각형은 빨간색이고 버킷의 민감도 레이블은 민감함입니다. 빨간색의 강도는 Macie가 버킷에서 발견한 민감한 데이터의 양을 반영합니다. 색상이 어두울수록 민감도 점수가 높음을 나타냅니다.
- 회색 - 버킷의 현재 민감도 점수가 -1이면 버킷의 사각형 색상은 짙은 회색이고 버킷의 민감도 레이블은 분류 오류입니다. 색상의 강도는 다양하지 않습니다.

Macie가 정의하는 민감도 점수 및 레이블의 범위에 대한 자세한 내용은 S3 버킷의 민감도 점수 섹션을 참조하세요.

맵에서 S3 버킷의 사각형에는 기호도 포함될 수 있습니다. 기호는 버킷의 민감도 평가에 영향을 미칠 수 있는 오류, 문제 또는 기타 고려 사항 유형을 나타냅니다. 기호는 버킷 보안과 관련된 잠재적 문제를 나타낼 수도 있습니다(예: 버킷에 공개적으로 액세스할 수 있음). 다음 테이블에는 Macie가 이러한 경우를 알리기 위해 사용하는 기호가 나열되어 있습니다.

Symbol	정의	설명
!	액세스 거부됨	Macie는 버킷 또는 버킷의 객체에 액세스할 수 없습니다. 따라서 Macie는 버킷의 어떤 객체도 분석할 수 없습니다. 이 문제는 일반적으로 버킷에 제한적인 버킷 정책이 있기 때

Symbol	정의	설명
		문에 발생합니다. 이 문제를 해결하는 방법에 대한 자세한 내용은 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을(를) 참조하세요.
	공개적으로 액세스할 수 있음(Publicly accessible)	일반 사용자가 버킷에 대한 읽기 또는 쓰기 액세스 권한을 가집니다. 이를 결정하기 위해 Macie는 계정과 버킷의 퍼블릭 액세스 차단 설정, 버킷의 버킷 정책 등 각 버킷에 대한 계정 및 버킷 수준 설정의 조합을 분석합니다. 자세한 정보는 Macie가 Amazon S3 데이터 보안을 모니터링하는 방법을 참조하세요.

Symbol	정의	설명
?	분류 불가	Macie이 버킷에 있는 모든 객체를 분석할 수 없습니다. 모든 버킷의 객체가 Macie가 지원하지 않는 Amazon S3 스토리지 클래스를 사용하거나 Macie가 지원하지 않는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가지고 있습니다. Macie가 객체를 분석하려면 객체가 지원되는 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가져야 합니다. 자세한 정보는 지원하는 스토리지 클래스 및 형식을 참조하세요.
0	0바이트	버킷에는 Macie가 분석할 객체가 저장되지 않습니다. 버킷이 비어 있거나 버킷의 모든 객체에 0바이트의 데이터가 포함되어 있습니다.

S3 버킷 맵과 상호 작용

S3 버킷 맵을 검토하면서 다양한 방식으로 상호 작용하여 개별 계정 및 버킷에 대한 추가 데이터와 세부 정보를 확인하고 평가할 수 있습니다. 다음 단계에 따라 Amazon Macie 콘솔에 맵을 표시하고 맵에서 제공하는 다양한 기능을 사용하십시오.

S3 버킷 맵과 상호 작용하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 S3 버킷을 선택합니다. S3 버킷 페이지에는 버킷 인벤토리 맵이 표시됩니다. 페이지에 인벤토리가 테이블 형식으로 대신 표시되는 경우, 페이지 상단에서 맵

()
을 선택합니다.

기본적으로 현재 자동화된 민감한 데이터 검색에서 제외된 버킷의 데이터는 맵에 표시되지 않습니다. 조직의 Macie 관리자인 경우 현재 민감한 데이터 자동 검색이 비활성화된 계정의 데이터도 표시되지 않습니다. 이 데이터를 표시하려면 필터 상자 아래에 있는 자동 검색으로 모니터링됨 필터 토큰에서 X를 선택합니다.

3. 필요에 따라 페이지 상단에서 새로 고침
()
을 선택하여 Amazon S3에서 최신 버킷 메타데이터를 검색할 수 있습니다.
4. S3 버킷 맵에서 다음 중 하나를 수행합니다.
   - 특정 민감도 레이블이 있는 버킷 수를 확인하려면 ID 바로 아래에 있는 AWS 계정 컬러 배지를 참조하십시오. 배지에는 집계된 버킷 수가 민감도 레이블별로 분류되어 표시됩니다.

     예를 들어, 빨간색 배지는 해당 계정이 소유하고 민감함 레이블이 지정된 버킷의 총 수를 보고합니다. 이러한 버킷의 민감도 점수 범위는 51~100입니다. 파란색 배지는 해당 계정이 소유하고 민감하지 않음이라는 레이블이 지정된 버킷의 총 수를 나타냅니다. 이러한 버킷의 민감도 점수 범위는 1~49입니다.
   - 버킷에 대한 정보의 하위 집합을 검토하려면 버킷의 사각형 위로 마우스를 가져갑니다. 팝오버에 버킷 이름과 현재 민감도 점수가 표시됩니다.

     팝오버에는 Macie가 버킷에서 분석할 수 있는 총 개체 수와 해당 개체의 최신 버전의 총 스토리지 크기도 표시됩니다. 이러한 객체는 분류 가능합니다. 이러한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하며 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가집니다. 자세한 정보는 지원하는 스토리지 클래스 및 형식을 참조하세요.
   - 맵을 필터링하고 필드에 특정 값이 있는 버킷만 표시하려면 필터 상자에 커서를 놓고 필드에 필터 조건을 추가합니다. Macie는 조건의 기준을 적용하고 필터 상자 아래에 조건을 표시합니다. 결과를 더 세분화하려면 추가 필드에 필터 조건을 추가합니다. 자세한 정보는 S3 버킷 인벤토리 필터링을 참조하세요.
   - 특정 계정이 소유한 버킷만 자세히 살펴보고 표시하려면 해당 계정의 계정 ID를 선택합니다. Macie는 해당 계정의 데이터만 필터링하고 표시하는 새 탭을 엽니다.
5. 특정 버킷에 대한 모든 민감한 데이터 검색 통계 및 기타 정보를 검토하려면 버킷의 사각형을 선택한 다음 세부 정보 패널을 참조하십시오. 이러한 세부 정보에 대한 자세한 내용은 개별 S3 버킷의 데이터 민감도 세부 정보 검토 섹션을 참조하세요.

> **Tip**
>
> 패널의 버킷 세부 정보 탭에서 여러 필드를 피벗하고 드릴다운
> 할 수 있습니다. 필드 값이 동일한 버킷을 표시하려면 필드에서
>  를
> 선택합니다. 필드에 다른 값이 있는 버킷을 표시하려면 필드에서
>  를
> 선택합니다.

S3 버킷 테이블을 사용한 데이터 민감도 평가

Amazon Macie 콘솔의 S3 버킷 테이블에는 현재 사용 중인 Amazon Simple Storage Service (Amazon S3) 범용 버킷 각각에 대한 요약 정보가 표시됩니다. AWS 리전조직의 Macie 관리자인 경우 여기에는 멤버 계정이 소유한 버킷에 대한 정보가 포함됩니다. 프로그래밍 방식으로 데이터에 액세스하려는 경우 Amazon Macie API의 DescribeBuckets작업을 사용할 수 있습니다.

콘솔에서 테이블을 정렬하고 필터링하여 보기를 사용자 지정할 수 있습니다. 또한 테이블의 데이터를 쉼표로 구분된 값(CSV)파일로 내보낼 수 있습니다. 테이블에서 S3 버킷을 선택하면 세부 정보 패널에 해당 버킷에 대한 추가 정보가 표시됩니다. 여기에는 설정 및 메트릭에 대한 세부 정보 및 통계가 포함되어 버킷 데이터의 보안 및 개인정보 보호에 대한 인사이트를 제공받을 수 있습니다. 민감한 데이터 자동 검색이 활성화된 경우 Macie가 지금까지 버킷에 대해 수행한 자동 검색 활동의 결과를 캡처하는 데이터도 포함됩니다. 이러한 세부 정보를 검토하는 것 외에도 패널을 사용하여 버킷의 자동 검색 설정을 조정할 수 있습니다. 자세한 방법은 개별 S3 버킷에 대한 민감한 데이터 자동 검색 관리(을)를 참조하세요.

S3 버킷 테이블을 사용하여 데이터 민감도를 평가하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 S3 버킷을 선택합니다. S3 버킷 페이지에는 버킷 인벤토리가 표시됩니다.

   기본적으로 이 페이지에는 현재 민감한 데이터 자동 검색에서 제외된 버킷의 데이터가 표시되지 않습니다. 조직의 Macie 관리자인 경우 현재 민감한 데이터 자동 검색이 비활성화된 계정의 데이터도 표시되지 않습니다. 이 데이터를 표시하려면 필터 상자 아래에 있는 자동 검색으로 모니터링됨 필터 토큰에서 X를 선택합니다.

3. 페이지 상단에서 table
()
을 선택합니다. Macie는 인벤토리의 버킷 수와 버킷 테이블을 표시합니다.
4. Amazon S3에서 최신 버킷 메타데이터를 검색하려면 페이지 상단에서 refresh
()
를 선택합니다.

   버킷 이름 옆에 정보 아이콘
()
이 표시되면 이렇게 하는 것이 좋습니다. 정보 아이콘은 지난 24시간 동안 버킷이 생성되었음을 의미합니다. 아마도 Macie가 일일 새로 고침 주기의 일부로 Amazon S3에서 버킷과 객체 메타데이터를 마지막으로 검색한 이후일 것입니다.
5. S3 버킷 테이블에서 인벤토리의 각 버킷에 대한 다음 요약 정보를 검토하세요.

   - 민감도 - 버킷의 현재 민감도 점수. Macie가 정의하는 민감도 점수 범위에 대한 자세한 내용은 S3 버킷의 민감도 점수 섹션을 참조하세요.
   - 버킷 - 버킷의 이름
   - 계정 — 버킷을 AWS 계정 소유한 사람의 계정 ID입니다.
   - 분류 가능한 객체는 Macie가 버킷에서 민감한 데이터를 탐지하기 위해 분석할 수 있는 총 객체 수입니다.
   - 분류 가능한 크기는 Macie가 버킷에서 민감한 데이터를 탐지하기 위해 분석할 수 있는 모든 객체의 총 스토리지 크기입니다.

     이 값은 압축 해제된 후 압축된 객체의 실제 크기를 반영하지 않습니다. 버킷에 버전 관리가 활성화된 경우, 이 값은 버킷에 있는 각 객체의 최신 버전의 스토리지 크기를 기준으로 합니다.
   - 작업별 모니터링 - 민감한 데이터 검색 작업이 버킷의 객체를 일별, 주별 또는 월별로 주기적으로 분석하도록 구성되어 있는지 여부를 나타냅니다.

     이 필드의 값이 예이면 해당 버킷이 명시적으로 정기적인 작업에 포함되어 있거나 버킷이 지난 24시간 이내에 정기적인 작업 기준과 일치한 경우입니다. 또한 이러한 작업 중 하나 이상의 상태는 취소되지 않습니다. Macie는 이 데이터를 매일 업데이트합니다.
   - 최근 작업 실행 - 버킷의 객체를 분석하도록 일회성 또는 주기적인 민감한 데이터 검색 작업을 구성한 경우 이 필드에는 해당 작업 중 하나가 실행되기 시작한 가장 최근 날짜 및 시간이 표시됩니다. 그렇지 않으면 이 필드에 대시 (-) 가 표시됩니다.

앞의 데이터에서, 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식의 파일 이름 확장자를 가진 경우 분류할 수 있습니다. Macie를 사용하여 객체에서 민감한 데이터를 탐지할 수 있습니다. 자세한 정보는 지원하는 스토리지 클래스 및 형식을 참조하세요.

6. 표를 사용하여 인벤토리를 분석하려면, 다음 작업 중 하나를 수행합니다.

   - 특정 필드를 기준으로 테이블을 정렬하려면 해당 필드의 열 제목을 선택합니다. 정렬 순서를 변경하려면 열 제목을 다시 선택합니다.
   - 테이블을 필터링하고 필드에 특정 값이 있는 버킷만 표시하려면 필터 상자에 커서를 놓고 필드에 필터 조건을 추가합니다. Macie는 조건의 기준을 적용하고 필터 상자 아래에 조건을 표시합니다. 결과를 더 세분화하려면 추가 필드에 필터 조건을 추가합니다. 자세한 정보는 S3 버킷 인벤토리 필터링을 참조하세요.
   - 특정 버킷에 대한 민감한 데이터 검색 통계 및 기타 정보를 검토하려면 표에서 버킷 이름을 선택한 다음 세부 정보 패널을 참조하십시오. 이러한 세부 정보에 대한 자세한 내용은 S3 버킷 세부 정보 검토 섹션을 참조하세요.

   > **Tip**
   >
   > 패널의 버킷 세부 정보 탭에서 여러 필드를 피벗하고 드릴다운할 수 있습니다. 필드 값이 동일한 버킷을 표시하려면 필드에서  를 선택합니다. 필드에 다른 값이 있는 버킷을 표시하려면 필드에서  를 선택합니다.

7. 테이블의 데이터를 CSV 파일로 내보내려면 내보내려는 각 행의 확인란을 선택하거나 선택 항목의 열 제목의 확인란을 선택하여 모든 행을 선택합니다. 그런 다음 페이지 상단에서 CSV로 내보내기를 선택합니다. 테이블에서 최대 50,000개의 행을 내보낼 수 있습니다.
8. 하나 이상의 버킷에 있는 객체를 더 심층적이고 즉각적으로 분석하려면 각 버킷의 확인란을 선택한 다음 작업 생성을 선택합니다. 자세한 정보는 민감한 데이터 검색 작업 생성을 참조하세요.

개별 S3 버킷의 데이터 민감도 세부 정보 검토

Amazon Macie 콘솔에서는 S3 버킷 페이지의 세부 정보 패널을 사용하여 Macie가 사용자 계정에 대해 모니터링하고 분석하는 각 Amazon Simple Storage Service (Amazon S3) 범용 버킷에 대한 통계 및

기타 정보를 검토할 수 있습니다. 사용자가 조직의 Macie 관리자인 경우, 여기에는 멤버 계정이 소유한 버킷이 포함됩니다.

통계 및 정보에는 S3 버킷 데이터의 보안 및 개인 정보 보호에 대한 통찰력을 제공하는 세부 정보가 포함됩니다. 민감한 데이터 자동 검색이 활성화되면 Macie가 지금까지 버킷에 대해 수행한 자동 검색 활동의 결과도 캡처됩니다. 예를 들어 Macie가 버킷에서 분석한 객체 목록과 Macie가 버킷에서 발견한 민감한 데이터의 유형 및 발생 횟수에 대한 분석을 찾을 수 있습니다. 단, 사용자가 만들고 실행한 민감한 데이터 검색 작업의 결과는 데이터에 포함되지 않습니다.

Macie는 민감한 데이터 자동 검색을 수행하는 동안 이러한 통계 및 세부 정보를 자동으로 재계산하고 업데이트합니다. 예:

- Macie가 S3 객체에서 민감한 데이터를 찾지 못하면 Macie는 버킷의 민감도 점수를 낮추고 필요에 따라 버킷의 민감도 레이블을 업데이트합니다. 또한 Macie는 버킷에서 분석된 객체 목록에 객체를 추가합니다.
- Macie가 S3 객체에서 민감한 데이터를 발견하면 Macie가 해당 데이터를 Macie가 버킷에서 찾은 민감한 데이터 유형의 분류에 추가합니다. 또한 Macie는 버킷의 민감도 점수를 높이고 필요에 따라 버킷의 민감도 레이블을 업데이트합니다. 또한 Macie는 버킷에서 분석되는 객체 목록에 객체를 추가합니다. 이러한 태스크는 객체에 대한 민감한 데이터 조사 결과를 생성하는 작업과 함께 수행됩니다.
- Macie가 S3 객체에서 이후에 변경되거나 삭제된 민감한 데이터를 발견하면 Macie는 버킷의 민감한 데이터 유형 분석에서 해당 객체에 발생한 민감한 데이터를 제거합니다. 또한 Macie는 버킷의 민감도 점수를 낮추고 필요에 따라 버킷의 민감도 레이블을 업데이트합니다. 또한 Macie는 버킷에서 분석된 객체 목록에서 객체를 제거합니다.
- Macie가 S3 객체를 분석하려고 시도했지만 문제나 오류로 인해 Macie가 분석을 수행할 수 없는 경우, Macie는 해당 객체를 버킷에서 분석된 객체 목록에 추가하고 객체를 분석하지 못했음을 알립니다.

통계 및 세부 정보를 검토하는 것 외에도 패널을 사용하여 S3 버킷의 민감한 데이터 자동 검색 설정을 조정할 수 있습니다. 예를 들어 버킷 점수에서 특정 유형의 민감한 데이터를 포함하거나 제외할 수 있습니다. 자세한 정보는 개별 S3 버킷에 대한 자동화된 데이터 검색 관리을 참조하세요.

S3 버킷에 대한 데이터 민감도 세부 정보를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 S3 버킷을 선택합니다. S3 버킷 페이지에는 버킷 인벤토리의 대화형 맵이 표시됩니다. 선택적으로 페이지 상단의 테이블

( )
를 선택하여 인벤토리를 테이블 형식으로 대신 표시할 수도 있습니다.

기본적으로 이 페이지에는 현재 자동화된 민감한 데이터 검색에서 제외된 버킷의 데이터가 표시되지 않습니다. 조직의 Macie 관리자인 경우 현재 민감한 데이터 자동 검색이 비활성화된 계정의 데이터도 표시되지 않습니다. 이 데이터를 표시하려면 필터 상자 아래에 있는 자동 검색으로 모니터링됨 필터 토큰에서 X를 선택합니다.

3. S3 버킷 맵 또는 테이블에서 세부 정보를 검토하려는 S3 버킷을 선택합니다. 세부 정보 패널에는 버킷에 대한 통계 및 기타 정보가 표시됩니다.

패널 상단에는 버킷에 대한 일반 정보 (버킷 이름, 버킷을 소유한 계정 ID) AWS 계정 가 표시됩니다. 또한 버킷의 특정 민감한 데이터 자동 검색 설정을 변경할 수 있는 옵션도 제공합니다. 버킷에 대한 추가 설정 및 정보는 다음 탭으로 구성되어 있습니다.

- 민감도
- 버킷 세부 정보
- 객체 샘플
- 민감한 데이터 검색

각 탭의 개별 설정과 정보는 다음과 같습니다.

민감도

이 탭에는 버킷의 현재 민감도 점수가 -1에서 100 사이로 표시됩니다. Macie가 정의하는 민감도 점수 범위에 대한 자세한 내용은 S3 버킷의 민감도 점수 섹션을 참조하세요.

또한 이 탭에는 Macie가 버킷 객체에서 발견한 민감한 데이터의 유형과 각 유형의 발생 횟수에 대한 분석도 제공합니다.

- 민감한 데이터 유형 - 데이터를 탐지한 관리형 데이터 식별자의 고유 식별자(ID) 또는 데이터를 탐지한 사용자 지정 데이터 식별자의 이름.

  관리형 데이터 식별자의 ID는 식별자가 탐지하도록 설계된 민감한 데이터의 유형을 설명합니다 (예: 미국 여권 번호의 경우, USA_PASSPORT_NUMBER). 각 관리형 데이터 식별자에 대한 자세한 내용은 관리형 데이터 식별자 사용 섹션을 참조하세요.
- 개수 - 관리형 또는 사용자 지정 데이터 식별자가 탐지한 총 데이터 발생 횟수입니다.
- 채점 상태 - 데이터 발생 횟수를 버킷의 민감도 점수에 포함할지 아니면 제외할지를 지정합니다.

버킷 점수를 자동으로 계산하도록 Macie를 구성한 경우, 버킷 점수에서 특정 유형의 민감한 데이터를 포함하거나 제외하여 계산을 조정할 수 있습니다. 포함하거나 제외하려는 데이터 식별자의 확인란을 선택한 다음 작업 메뉴에서 원하는 옵션을 선택합니다. 자세한 정보는 개별 S3 버킷에 대한 자동화된 데이터 검색 관리을 참조하세요.

Macie가 현재 버킷에 저장되어 있는 객체에서 민감한 데이터를 찾지 못한 경우, 이 섹션에는 탐지되지 않음 메시지가 표시됩니다.

참고로 Macie가 분석하고 이후에 변경 또는 삭제된 객체에 대한 데이터는 민감도 탭에 포함되지 않습니다. Macie가 객체를 분석한 후 객체가 변경되거나 버킷에서 삭제되면 Macie는 적절한 통계와 데이터를 자동으로 다시 계산하고 업데이트하여 해당 객체를 제외합니다.

버킷 세부 정보

이 탭은 데이터 보안 및 개인 정보 설정을 포함하여 버킷 설정에 대한 세부 정보를 제공합니다. 예를 들어, 버킷의 퍼블릭 액세스 설정의 세부 분석을 검토하고 버킷이 객체를 복제하는지 아니면 다른 AWS 계정과 공유되는지 여부를 결정할 수 있습니다.

특히 최종 업데이트 필드에는 Macie가 Amazon S3에서 가장 최근에 버킷 또는 버킷 객체에 대한 메타데이터를 검색한 시기가 표시됩니다. 최신 자동 검색 실행 필드는 Macie가 자동 검색을 수행하면서 가장 최근에 버킷의 객체를 분석한 시기를 나타냅니다. 이 분석이 수행되지 않은 경우 이 필드에 대시 (-) 가 표시됩니다.

또한 이 탭에는 Macie가 버킷에서 분석할 수 있는 데이터의 양을 평가하는 데 도움이 되는 객체 수준 통계도 제공됩니다. 또한 민감한 데이터 검색 작업이 버킷의 객체를 분석하도록 구성되어 있는지 여부도 나타냅니다. 있는 경우, 가장 최근에 실행된 작업에 대한 세부 정보에 액세스한 다음 해당 작업에서 생성된 조사 결과를 선택적으로 표시할 수 있습니다.

이 탭의 정보에 대한 추가 세부 정보는 S3 버킷의 세부 정보 검토 섹션을 참조하세요.

객체 샘플

이 탭에는 Macie가 버킷에 대한 민감한 데이터 자동 검색을 수행하는 동안 분석을 위해 선택한 객체가 나열됩니다. 선택적으로 객체 이름을 선택하여 Amazon S3 콘솔을 열고 객체의 속성을 표시합니다.

목록에는 최대 100개의 객체에 대한 데이터가 포함됩니다. 목록은 다음 객체 민감도 필드 값을 기준으로 채워집니다. 민감함 다음에 민감하지 않음, 그 다음에 Macie가 분석하지 못한 객체 순으로 채워집니다.

목록에서 객체 민감도 필드는 Macie가 객체에서 민감한 데이터를 찾았는지 여부를 나타냅니다.

- 민감함 - Macie가 객체에서 하나 이상의 민감한 데이터를 발견했습니다.
- 민감하지 않음 - Macie가 객체에서 민감한 데이터를 찾지 못했습니다.
- –(대시) – Macie가 문제 또는 오류로 인해 개체 분석을 완료하지 못했습니다.

분류 결과 필드는 Macie가 객체를 분석할 수 있었는지 여부를 나타냅니다.

- 완료 - Macie가 객체 분석을 완료했습니다.
- 부분적 - Macie가 문제나 오류로 인해 개체의 일부 데이터만 분석했습니다. 예를 들어, 객체는 지원되지 않는 형식의 파일을 포함하는 아카이브 파일입니다.
- 건너뜀 - Macie가 문제나 오류로 인해 객체의 데이터를 분석할 수 없었습니다. 예를 들어 객체가 Macie가 사용할 수 없는 키로 암호화되었습니다.

Macie가 분석 또는 분석을 시도한 후 변경되거나 삭제된 객체는 목록에 포함되지 않습니다. 객체가 이후에 변경되거나 삭제되는 경우, Macie 목록에서 해당 객체를 자동으로 제거합니다.

민감한 데이터 검색

이 탭은 버킷에 대한 민감한 데이터 자동 검색 통계를 집계하여 제공합니다.

- 분석된 바이트 - Macie가 버킷에서 분석한 총 데이터 양(바이트)입니다.
- 분류 가능한 바이트는 Macie가 버킷에서 분석할 수 있는 모든 객체의 총 스토리지 크기입니다. 이러한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하며 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가집니다. 자세한 정보는 지원하는 스토리지 클래스 및 형식을 참조하세요.
- 총 탐지 수 - Macie가 버킷에서 발견한 민감한 데이터의 총 발생 횟수입니다. 여기에는 버킷의 민감도 점수 설정에 의해 현재 억제된 발생 건수도 포함됩니다.

분석된 객체 차트는 Macie가 버킷에서 분석한 총 객체 수를 나타냅니다. 또한 Macie가 민감한 데이터를 찾았거나 찾지 못한 객체의 수를 시각적으로 보여줍니다. 차트 아래의 범례에는 이러한 결과를 분석한 내용이 나와 있습니다.

- 민감한 객체(빨간색) - Macie가 하나 이상의 민감한 데이터를 발견한 총 객체 수입니다.
- 민감하지 않은 객체(파란색) - Macie가 민감한 데이터를 찾지 못한 총 객체 수입니다.
- 건너뛴 객체(짙은 회색) - 문제나 오류로 인해 Macie가 분석하지 못한 총 객체 수입니다.

차트 범례 아래 영역에는 특정 유형의 권한 문제나 암호화 오류가 발생하여 Macie가 객체를 분석하지 못한 사례를 분류하여 보여줍니다.

- 생략: 잘못된 암호화 — 고객 제공 키로 암호화된 총 객체 수입니다. Macie는 이러한 키에 액세스할 수 없습니다.

- 건너뛰기: 잘못된 KMS — 더 이상 사용할 수 없는 AWS Key Management Service (AWS KMS) 키로 암호화된 총 개체 수입니다. 이러한 객체는 비활성화되었거나, 삭제 AWS KMS keys 일정이 잡혔거나, 삭제된 객체로 암호화됩니다. Macie는 이 키를 사용할 수 없습니다.
- 건너뛰기: 권한 거부됨 - 객체에 대한 권한 설정 또는 객체를 암호화하는 데 사용된 키의 권한 설정으로 인해 Macie가 액세스할 수 없는 총 개체 수입니다.

이러한 문제 및 발생할 수 있는 다른 유형의 문제 및 오류에 대한 자세한 내용은 을 참조하십시오. 민감한 데이터 자동 검색에 대한 적용 범위 문제 해결 문제와 오류를 수정하면 후속 분석 주기 동안 버킷 데이터의 적용 범위를 늘릴 수 있습니다.

민감한 데이터 검색 탭의 통계에는 Macie가 분석하거나 또는 분석을 시도한 후 변경되거나 삭제된 객체에 대한 데이터는 포함되지 않습니다. Macie가 객체를 분석하거나 분석을 시도한 후 객체가 변경되거나 버킷에서 삭제되면 Macie는 이러한 통계를 자동으로 다시 계산하여 객체를 제외합니다.

자동 검색으로 생성된 민감한 데이터 분석 조사 결과 분석

Amazon Macie는 민감한 데이터를 자동으로 검색하는 동안 민감한 데이터를 검색하는 각 Amazon Simple Storage Service (Amazon S3) 객체에 대해 민감한 데이터 검색 기능을 생성합니다. 민감한 데이터 조사 결과는 Macie가 S3 객체에서 발견한 민감한 데이터에 대한 상세 보고서입니다. 각 민감한 데이터 조사 결과는 심각도 등급과 다음과 같은 세부 정보를 제공합니다.

- Macie가 민감한 데이터를 발견한 날짜 및 시간.
- Macie가 발견한 민감한 데이터의 범주 및 유형.
- Macie가 발견한 각 유형의 민감한 데이터 발생 횟수.
- Macie가 민감한 데이터를 발견한 방법, 민감한 데이터 자동 검색 또는 민감한 데이터 검색 작업.
- 영향을 받는 S3 버킷 및 객체에 대한 이름, 퍼블릭 액세스 설정, 암호화 유형 및 기타 정보.

영향을 받는 S3 객체의 파일 유형이나 스토리지 형식에 따라 세부 정보에는 Macie가 발견한 최대 15개의 민감한 데이터 위치가 포함될 수 있습니다. 민감한 데이터 조사 결과에는 Macie가 발견한 민감한 데이터는 포함되지 않습니다. 대신 필요에 따라 추가 조사 및 수정에 사용할 수 있는 정보를 제공합니다.

Macie는 사용자의 민감한 데이터 조사 결과를 90일 동안 저장합니다. Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 이러한 결과에 액세스할 수 있습니다. 또한 다른 애플리케이션, 서비스 및 시스템을 사용하여 조사 결과를 모니터링하고 처리할 수 있습니다. 자세한 정보는 조사 결과 분석을 참조하세요.

민감한 데이터 자동 검색을 통해 생성된 조사 결과를 분석하려면

Macie가 민감한 데이터 자동 검색을 수행하는 동안 생성한 결과를 식별하고 분석하기 위해 결과를 필터링할 수 있습니다. 필터를 사용하면 조사 결과의 특정 속성을 사용하여 조사 결과에 대한 사용자 지정 보기 및 쿼리를 만들 수 있습니다. Amazon Macie 콘솔을 사용하여 조사 결과를 필터링하거나 Amazon Macie API를 사용하여 프로그래밍 방식으로 쿼리를 제출할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 조사 결과를 식별하고 분석하려면 다음 단계를 따르세요.

자동 검색으로 생성된 조사 결과를 분석하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. (선택 사항) 억제 규칙에 의해 제외된 조사 결과를 표시하려면 조사 결과 상태 설정을 변경합니다. 억제된 조사 결과와 억제되지 않은 조사 결과를 모두 표시하려면 모두를 선택하고, 억제된 조사 결과만 표시하려면 보관됨을 선택합니다. 그런 다음 억제된 조사 결과를 다시 숨기려면 현재를 선택합니다.
4. 필터 기준 상자에 커서를 놓습니다. 나타나는 필드 목록에서 오리진 유형을 선택합니다.

   이 필드는 Macie가 조사 결과, 민감한 데이터 자동 검색 또는 민감한 데이터 검색 작업을 생성하는 민감한 데이터를 찾은 방법을 지정합니다. 필터 필드 목록에서 이 필드를 찾으려면 전체 목록을 찾아보거나 필드 이름의 일부를 입력하여 필드 목록의 범위를 좁힐 수 있습니다.
5. 필드 값으로 AUTOMATED_SENSITIVE_DATA_DISCOVERY를 선택한 다음 적용을 선택합니다. Macie는 필터 기준을 적용하고 필터 기준 상자의 필터 토큰에 조건을 추가합니다.
6. (선택 사항) 조사 결과를 세분화하려면 추가 필드에 대한 필터 조건을 추가합니다. 예를 들어 조사 결과가 생성된 시간 범위의 경우는 생성 날짜, 영향을 받는 버킷 이름의 경우, S3 버킷 이름, 탐지되어 조사 결과를 생성한 민감한 유형의 경우, 민감한 데이터 탐지 유형을 추가합니다. 자세한 정보는 조사 결과 필터링을 참조하세요.

이후에 이 조건 세트를 다시 사용하려면 필터 규칙으로 저장하면 됩니다. 이렇게 하려면 필터 기준 상자에서 규칙 저장을 선택합니다. 규칙의 이름을 입력하고, 선택적으로 설명을 입력합니다. 마쳤으면 저장을 선택합니다.

API

결과를 프로그래밍 방식으로 식별하고 분석하려면 Amazon Macie API의 ListFindings또는 GetFindingStatistics연산을 사용하여 제출하는 쿼리에 필터 기준을 지정하십시오. 이 ListFindings작업은 필터 기준과 일치하는 각 조사 결과에 대해 하나의 ID씩 조사 결과 ID 배열을

반환합니다. 그런 다음 해당 ID를 사용하여 각 조사 결과의 세부 정보를 검색할 수 있습니다. 이 GetFindingStatistics 작업은 필터 기준과 일치하는 모든 조사 결과에 대한 집계된 통계 데이터를 요청에서 지정한 필드별로 그룹화하여 반환합니다. 결과를 프로그래밍 방식으로 필터링하는 방법에 대한 자세한 내용은 을 참조하십시오. 조사 결과 필터링

필터 기준에 `originType` 필드에 대한 조건을 포함시킵니다. 이 필드는 Macie가 조사 결과, 민감한 데이터 자동 검색 또는 민감한 데이터 검색 작업을 생성하는 민감한 데이터를 찾은 방법을 지정합니다. 자동 검색을 수행하는 동안 조사 결과가 생성된 경우, 이 필드의 값은 `AUTOMATED_SENSITIVE_DATA_DISCOVERY`입니다.

AWS Command Line Interface (AWS CLI) 를 사용하여 결과를 식별하고 분석하려면 list-findings 또는 명령을 실행합니다. get-finding-statistics 다음 예에서는 list-findings 명령을 사용하여 현재 AWS 리전에서 민감한 데이터 자동 검색으로 생성된 심각도가 높은 모든 조사 결과에 대한 검색 ID를 검색합니다.

Linux, macOS 또는 Unix의 경우, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

Microsoft Windows의 경우 캐럿(^) 줄 연속 문자를 사용하여 가독성을 개선합니다.

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"classificationDetails.originType\":{\"eq
\":[\"AUTOMATED_SENSITIVE_DATA_DISCOVERY\"]},\"severity.description\":{\"eq\":
[\"High\"]}}}
```

위치:

- `classificationDetails.originType`은 오리진 유형 필드의 JSON 이름을 지정합니다.
  - `eq`는 equals 연산자를 지정합니다.
  - `AUTOMATED_SENSITIVE_DATA_DISCOVERY`는 필드의 열거형 값입니다.
- *`severity.description`*은 심각도 필드의 JSON 이름을 지정합니다.
  - *`eq`*는 equals 연산자를 지정합니다.
  - *`High`*는 필드의 열거형 값입니다.

이 명령이 성공적으로 실행되면 Macie는 `findingIds` 배열을 반환합니다. 배열에는 다음 예시와 같이 필터 기준과 일치하는 각 조사 결과의 고유 식별자가 표시됩니다.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

필터 기준과 일치하는 조사 결과가 없는 경우 Macie는 빈 `findingIds` 배열을 반환합니다.

```
{
    "findingIds": []
}
```

자동 검색으로 생성된 민감한 데이터 검색 결과에 액세스

Amazon Macie는 자동화된 민감한 데이터 검색을 수행하는 동안 분석을 위해 선택한 각 Amazon Simple Storage Service (Amazon S3) 객체에 대한 분석 레코드를 생성합니다. 민감한 데이터 검색 결과라고 하는 이러한 레코드는 Macie가 개별 S3 객체에 대해 수행하는 분석에 대한 세부 정보를 기록합니다. 여기에는 Macie가 민감한 데이터를 찾지 못한 객체와 권한 설정이나 지원되지 않는 파일 또는 스토리지 형식의 사용과 같은 오류나 문제로 인해 Macie가 분석할 수 없는 객체가 포함됩니다.

Macie가 S3 객체에서 민감한 데이터를 찾은 경우, 민감한 데이터 검색 결과에는 Macie가 발견한 민감한 데이터에 대한 정보가 제공됩니다. 이 정보에는 민감한 데이터 검색 결과에서 제공하는 것과 동일한 유형의 세부 정보가 포함됩니다. 또한 Macie가 발견한 각 유형의 민감한 데이터가 1,000건 이상 발생한 위치와 같은 추가 정보도 제공합니다. 예:

- Microsoft Excel 통합 문서, CSV 파일 또는 TSV 파일에 있는 셀 또는 필드의 열 및 행 번호
- JSON 또는 JSON 라인 파일에 있는 필드 또는 배열의 경로
- CSV, JSON, JSON 라인 또는 TSV 파일이 아닌 비이진 텍스트 파일(예: HTML, TXT 또는 XML 파일)의 줄 번호
- Adobe PDF(휴대용 문서 형식) 파일에 있는 페이지의 페이지 번호

- Apache Avro 객체 컨테이너 또는 Apache Parquet 파일에 있는 레코드 인덱스 및 레코드 내 필드 경로

영향을 받는 S3 객체가 아카이브 파일 (예: .tar 또는.zip 파일) 인 경우 중요한 데이터 검색 결과에는 Macie가 아카이브에서 추출한 개별 파일의 민감한 데이터 발생에 대한 자세한 위치 데이터도 제공됩니다. Macie는 아카이브 파일에 대한 민감한 데이터 조사 결과에 이 정보를 포함시키지 않습니다. 위치 데이터를 보고하기 위해 민감한 데이터 검색 결과는 표준화된 JSON 스키마를 사용합니다.

민감한 데이터 검색 결과에는 Macie가 발견한 민감한 데이터는 포함되지 않습니다. 대신 데이터 프라이버시 및 보호 감사 또는 조사에 도움이 될 수 있는 분석 기록을 제공합니다.

Macie는 민감한 데이터 검색 결과를 90일 동안 저장합니다. Amazon Macie 콘솔이나 Amazon Macie API에서는 바로 액세스할 수 없습니다. 대신 Macie를 구성하여 S3 버킷에 저장할 수 있습니다. 버킷은 모든 민감한 데이터 검색 결과를 위한 확정적이고 장기적인 리포지토리 역할을 할 수 있습니다. 그런 다음, 필요에 따라 해당 리포지토리에 있는 결과에 액세스하고 쿼리할 수 있습니다.

계정의 이 리포지토리가 어디에 있는지 확인하려면 Amazon Macie 콘솔의 탐색 창에서 검색 결과를 선택합니다. 프로그래밍 방식으로 이 작업을 수행하려면 Amazon GetClassificationExportConfigurationMacie API의 작업을 사용하십시오. 계정에 대해 이 리포지토리를 구성하지 않은 경우, 방법을 알아보려면 민감한 데이터 검색 결과 저장 및 유지 섹션을 참조하세요.

민감한 데이터 검색 결과를 S3 버킷에 저장하도록 Macie를 구성한 후 Macie는 결과를 JSON Lines(.jsonl) 파일에 기록하고 해당 파일을 암호화하여 GNU Zip(.gz) 파일로 버킷에 추가합니다. 민감한 데이터를 자동으로 검색하기 위해 Macie는 파일을 버킷에 이름이 지정된 `automated-sensitive-data-discovery` 폴더에 추가합니다.

민감한 데이터 조사 결과의 경우와 마찬가지로 민감한 데이터 조사 결과도 표준화된 스키마를 따릅니다. 이렇게 하면 다른 애플리케이션, 서비스 및 시스템을 사용하여 선택적으로 쿼리, 모니터링 및 처리하는 데 도움이 될 수 있습니다.

> **Tip**
>
> 민감한 데이터 검색 결과를 쿼리하고 사용하여 잠재적 데이터 보안 위험을 분석하고 보고하는 방법에 대한 자세한 지침 예제는 보안 QuickSight 블로그의 Amazon Athena와 Amazon을 사용하여 Macie의 민감한 데이터 검색 결과를 쿼리하고 시각화하는 방법 블로그 게시물을 참조하십시오.AWS
>
> 민감한 데이터 검색 결과를 분석하는 데 사용할 수 있는 Athena 쿼리 샘플을 보려면 의 Amazon Macie 결과 분석 리포지토리를 방문하십시오. GitHub 또한 이 리포지토리는 결과를

검색하고 해독할 수 있게 Athena를 구성하는 지침과 결과에 대한 테이블을 생성하는 스크립트도 제공합니다.

S3 버킷의 민감도 점수

민감한 데이터 자동 검색이 활성화된 경우 Amazon Macie는 계정 또는 조직을 모니터링하고 분석하는 각 Amazon Simple Storage Service (Amazon S3) 범용 버킷에 민감도 점수를 자동으로 계산하여 할당합니다. 민감도 점수는 S3 버킷에 포함될 수 있는 민감한 데이터의 양을 정량적으로 나타낸 것입니다. 또한 Macie는 이 점수를 기반으로 각 버킷에 민감도 레이블을 할당합니다. 민감도 레이블은 버킷의 민감도 점수를 정성적으로 표현한 것입니다. 이러한 값은 민감한 데이터가 Amazon S3 데이터 자산에 위치할 수 있는 위치를 결정하고 해당 데이터에 대한 잠재적 보안 위험을 식별 및 모니터링하기 위한 기준점이 될 수 있습니다.

기본적으로 S3 버킷의 민감도 점수 및 레이블은 Macie가 지금까지 해당 버킷에 대해 수행한 자동화된 민감한 데이터 검색 활동의 결과를 반영합니다. 생성 및 실행한 민감한 데이터 검색 작업의 결과는 반영되지 않습니다. 또한 점수나 레이블은 버킷 또는 버킷 객체가 조직에 미칠 수 있는 중요도나 중요성을 암시하거나 나타내지 않습니다. 하지만 버킷에 최고 점수(100)를 수동으로 할당하여 버킷의 계산된 점수를 재정의할 수 있으며, 이때 민감 레이블도 버킷에 할당됩니다.

주제

민감도 점수, 치수 및 범위

Amazon Macie에서 계산하는 경우 S3 버킷의 민감도 점수는 두 기본 차원의 교차점을 정량적으로 측정한 값입니다.

- Macie가 버킷에서 발견한 민감한 데이터의 양을 반영합니다. 이는 주로 Macie가 버킷에서 찾은 민감한 데이터 유형의 특성과 수, 각 유형의 발생 횟수에서 비롯됩니다.
- Macie가 버킷에서 분석한 데이터의 양. 이는 주로 버킷에 있는 총 고유한 객체의 총 개수와 비교하여 Macie가 버킷에서 분석한 고유 개체 수에서 파생됩니다.

S3 버킷의 민감도 점수에 따라 Macie가 버킷에 할당하는 민감도 레이블도 결정됩니다. 민감도 레이블은 점수를 정성적으로 표현한 것입니다(예: 민감 또는 민감하지 않음). Amazon Macie 콘솔에서는 다음

이미지와 같이 버킷의 민감도 점수에 따라 데이터 시각화에서 Macie가 버킷을 나타내는 데 사용하는 색상도 결정됩니다.

민감도 점수의 범위는 다음 표에 설명된 대로 -1에서 100까지입니다. S3 버킷 점수에 대한 입력을 평가하려면 Macie가 해당 버킷에 대해 제공하는 민감한 데이터 검색 통계 및 기타 세부 정보를 참조할 수 있습니다.

민감도 점수	민감도 레이블	추가 정보
-1	분류 오류	Macie는 개체 수준 분류 오류(개체 수준 권한 설정, 개체 콘텐츠 또는 할당량 문제)로 인해 아직 버킷의 개체를 성공적으로 분석하지 못했습니다. Macie가 버킷에 있는 하나 이상의 객체를 분석하려고 시도했을 때 오류가 발생했습니다. 예를 들어 객체가 잘못된 파일이거나, 객체가 Macie가 액세스할 수 없거나 사용할 수 없는 키로 암호화된 경우를 들 수 있습니다. 버킷의 커버리지 데이터는 오류를 조사하고 해결하는 데 도움이 될 수 있습니다. 자세한 정보는 민감한 데이터 자동 검색 범위 평가을 참조하세요. Macie는 계속해서 버킷의 객체를 분석하려고 노력할 것입니다. Macie가 물체를 성공적으

민감도 점수	민감도 레이블	추가 정보
		로 분석하면 Macie는 분석 결과를 반영하도록 버킷의 민감도 점수와 레이블을 업데이트합니다.
1-49	민감하지 않음	이 범위에서 점수(예: 49)가 높으면 Macie가 버킷에 있는 비교적 적은 수의 객체를 분석했음을 나타냅니다. 점수가 1과 같이 낮으면 Macie가 버킷에 있는 많은 객체(예: 버킷의 총 객체의 개수 기준)를 분석했으며 해당 객체에서 민감한 데이터의 유형 및 발생 횟수가 상대적으로 적다는 것을 나타냅니다. 또한 점수가 1이면 버킷에 어떤 객체도 저장되어 있지 않거나 버킷의 모든 객체에 0바이트의 데이터가 포함되어 있음을 의미할 수 있습니다. 버킷 세부 정보에 있는 객체 통계를 보면 해당 여부를 판단하는 데 도움이 될 수 있습니다. 자세한 정보는 S3 버킷 세부 정보 검토을 참조하세요.

민감도 점수	민감도 레이블	추가 정보
50	아직 분석되지 않음	Macie는 아직 버킷의 객체를 분석하거나 분석하려고 시도하지 않았습니다. Macie는 처음에 자동 검색을 활성화하거나 계정의 버킷 인벤토리에 버킷을 추가하면 이 점수를 자동으로 할당합니다. 조직에서 버킷을 소유한 계정에 대해 자동 검색을 활성화한 적이 없는 경우에도 버킷에 이 점수가 부여될 수 있습니다. 점수가 50이면 버킷의 권한 설정으로 인해 Macie가 버킷이나 버킷의 객체에 액세스하지 못함을 나타낼 수도 있습니다. 이는 일반적으로 제한적인 버킷 정책 때문입니다. Macie는 버킷에 대한 정보의 일부만 제공할 수 있기 때문에 버킷의 세부 정보를 통해 해당 여부를 판단할 수 있습니다. 이 문제를 해결하는 방법에 대한 자세한 내용은 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을(를) 참조하세요.

민감도 점수	민감도 레이블	추가 정보
51-99	민감함	이 범위에서 점수(예: 99)가 높으면 Macie가 버킷에 있는 많은 객체를 분석하고(버킷에 있는 총 객체의 개수를 기준으로) 해당 객체에서 민감한 데이터의 유형과 발생을 여러 번 감지했음을 나타냅니다. 51과 같이 점수가 낮으면 Macie가 버킷에 있는 적당한 수의 객체(예: 버킷의 총 객체의 개수 기준)를 분석하여 해당 객체에서 몇 가지 이상의 민감한 데이터 유형과 발생을 감지했음을 나타냅니다.
100	민감함	점수를 수동으로 버킷에 할당하여 계산된 점수를 재정의했습니다. Macie는 이 점수를 버킷에 할당하지 않습니다.

민감도 점수 모니터링

계정에 대해 민감한 데이터 자동 검색을 처음 활성화하면 Amazon Macie는 계정이 소유한 각 S3 버킷에 민감도 점수 50점을 자동으로 할당합니다. 또한 Macie는 계정의 버킷 인벤토리에 버킷을 추가할 때 이 점수를 버킷에 할당합니다. 이 점수를 기준으로 각 버킷의 민감도 레이블은 아직 분석되지 않음이 할당됩니다. 단, 빈 버킷은 객체를 저장하지 않거나 버킷의 모든 객체에 0바이트의 데이터가 포함된 버킷입니다. 버킷이 이 경우에 해당하면 Macie는 버킷에 점수 1을 할당하고 버킷의 민감도 레이블은 민감하지 않음으로 설정합니다.

민감한 데이터 자동 검색이 매일 진행됨에 따라 Macie는 S3 버킷의 민감도 점수와 레이블을 업데이트하여 분석 결과를 반영합니다. 예:

- Macie가 객체에서 민감한 데이터를 찾지 못하면 Macie는 버킷의 민감도 점수를 낮추고 필요에 따라 버킷의 민감도 레이블을 업데이트합니다.

- Macie가 객체에서 민감한 데이터를 발견하면 Macie는 버킷의 민감도 점수를 높이고 필요에 따라 버킷의 민감도 레이블을 업데이트합니다.
- Macie가 이후에 변경된 객체에서 민감한 데이터를 발견하면 Macie는 해당 객체에 대한 민감한 데이터 감지를 버킷의 민감도 점수에서 제거하고, 필요에 따라 버킷의 민감도 레이블을 업데이트합니다.
- Macie가 이후에 삭제된 객체에서 민감한 데이터를 발견하면 해당 객체에 대한 민감한 데이터 감지를 버킷의 민감도 점수에서 제거하고, 필요에 따라 버킷의 민감도 레이블을 업데이트합니다.
- 이전에 비어 있던 버킷에 객체가 추가되고 Macie가 객체에서 민감한 데이터를 발견한 경우 Macie는 버킷의 민감도 점수를 높이고 필요에 따라 버킷의 민감도 레이블을 업데이트합니다.
- 버킷의 권한 설정으로 인해 Macie가 버킷 또는 버킷의 객체에 대한 정보를 검색하거나 액세스할 수 없는 경우 Macie는 버킷의 민감도 점수를 50으로 변경하고 버킷의 민감도 레이블을 아직 분석되지 않음으로 변경합니다.

계정에 대한 민감한 데이터 자동 검색을 활성화한 후 48시간 이내에 분석 결과가 나타나기 시작할 수 있습니다.

조직의 Macie 관리자이거나 독립형 Macie 계정을 보유한 경우 조직 또는 계정의 민감도 점수 설정을 조정할 수 있습니다.

- 모든 S3 버킷의 후속 분석에 대한 설정을 조정하려면 계정의 자동 민감 데이터 검색 설정을 변경하십시오. 특정 관리형 데이터 식별자, 사용자 지정 데이터 식별자 또는 허용 목록을 포함하거나 제외하기 시작할 수 있습니다. 특정 버킷을 제외할 수도 있습니다. 자세한 정보는 자동 검색 구성을 참조하세요.
- 개별 S3 버킷의 설정을 조정하려면 각 버킷의 자동 민감 데이터 검색 설정을 변경하십시오. 버킷 점수에서 특정 유형의 민감한 데이터를 포함하거나 제외할 수 있습니다. 자동 계산된 점수를 버킷에 할당할지 여부도 지정할 수 있습니다. 자세한 정보는 개별 S3 버킷에 대한 자동화된 데이터 검색 관리을 참조하세요.

민감한 데이터 자동 검색을 비활성화하면 기존 민감도 점수 및 레이블에 미치는 영향이 달라집니다. 조직의 구성원 계정에 대해 이 기능을 비활성화하면 해당 계정이 소유한 S3 버킷에 대해 기존 점수와 레이블이 그대로 유지됩니다. 조직 전체 또는 독립형 Macie 계정에서 이 기능을 비활성화하면 기존 점수와 레이블이 30일 동안만 유지됩니다. 30일이 지나면 Macie는 조직 또는 계정이 소유한 모든 버킷의 점수와 레이블을 재설정합니다. 버킷에 객체가 저장되어 있는 경우 Macie는 점수를 50점으로 변경하고 해당 버킷에 아직 분석되지 않음 레이블을 할당합니다. 버킷이 비어 있는 경우 Macie는 점수를 1로 변경하고 버킷에 민감하지 않음 레이블을 할당합니다. 이렇게 재설정하면 조직이나 계정에 대한 민감한 데이터 자동 검색을 다시 활성화하지 않는 한 Macie는 버킷의 민감도 점수 및 레이블 업데이트를 중단합니다.

민감한 데이터 자동 검색을 위한 기본 설정

민감한 데이터 자동 검색이 활성화된 경우 Amazon Macie는 계정에 대해 모니터링하고 분석하는 모든 Amazon Simple Storage Service (Amazon S3) 범용 버킷에서 샘플 객체를 자동으로 선택하고 분석합니다. 조직의 Macie 관리자인 경우 기본적으로 여기에는 구성원 계정이 소유한 S3 버킷이 포함됩니다.

분석 범위를 좁히기 위해 자동화된 민감한 데이터 검색에서 특정 S3 버킷을 제외할 수 있습니다. 계정의 설정을 변경하는 방법과 개별 버킷의 설정을 변경하는 두 가지 방법으로 이 작업을 수행할 수 있습니다. Macie 관리자인 경우 조직의 개별 계정에 대해 민감한 데이터 자동 검색을 활성화하거나 비활성화할 수도 있습니다. 자세한 정보는 민감한 데이터 자동 검색 구성을 참조하세요.

기본적으로 Macie는 민감한 데이터 자동 검색에 권장되는 관리형 데이터 식별자 세트만 사용하여 S3 객체를 분석합니다. Macie는 사용자가 정의한 사용자 지정 데이터 식별자나 허용 목록을 사용하지 않습니다. 분석을 사용자 지정하려면 Macie가 특정 관리형 데이터 식별자, 사용자 지정 데이터 식별자, 허용 목록을 사용하도록 구성할 수 있습니다. 계정의 설정을 변경하여 이 작업을 수행할 수 있습니다. 자세한 정보는 민감한 데이터 자동 검색 구성을 참조하세요.

주제

민감한 데이터 자동 검색을 위한 기본 관리형 데이터 식별자

기본적으로 Amazon Macie는 민감한 데이터 자동 검색에 권장되는 관리형 데이터 식별자 세트만 사용하여 S3 객체를 분석합니다. 이 기본 관리형 데이터 식별자 세트는 민감한 데이터의 일반적인 범주와 유형을 감지하도록 설계되었습니다. 연구 결과에 따르면 민감한 데이터의 일반적인 범주와 유형을 감지하는 동시에 노이즈를 줄여 자동 검색 결과를 최적화할 수 있습니다.

기본 세트는 동적입니다. 새로운 관리형 데이터 식별자를 출시하면서 민감한 데이터 자동 검색 결과를 더욱 최적화할 가능성이 있는 경우, 기본 세트에 추가합니다. 시간이 지나면서 세트에 기존 관리형 데이터 식별자를 추가하거나 제거할 수도 있습니다. 관리형 데이터 식별자를 제거해도 S3 버킷의 기존 민감한 데이터 검색 통계 및 세부 정보에는 영향을 미치지 않습니다. 예를 들어 Macie가 이전에 버킷에서 감지한 민감한 데이터 유형에 대한 관리형 데이터 식별자를 제거해도 Macie는 해당 버킷에 대해 해당 감지를 계속 보고합니다. 기본 세트에서 관리형 데이터 식별자를 추가하거나 제거하면 이 페이지를 업데이트하여 변경의 특성과 시기를 표시합니다. 이러한 변경 사항에 대한 자동 알림을 받으려면 Macie 문서 기록 페이지에서 RSS 피드를 구독하세요.

다음 주제에서는 현재 기본 세트에 있는 관리형 데이터 식별자를 민감한 데이터 범주 및 유형별로 정리하여 나열합니다. 세트의 각 관리형 데이터 식별자에 대해 고유 식별자(ID)를 지정합니다. 이 ID는 관리형 데이터 식별자가 감지하도록 설계된 민감한 데이터의 유형을 설명합니다(예: PGP 개인 키는 PGP_PRIVATE_KEY. 미국 여권 번호는 USA_PASSPORT_NUMBER). 계정의 민감한 데이터 자동 검색 설정을 변경하는 경우, 이 ID를 사용하여 후속 분석에서 관리형 데이터 식별자를 명시적으로 제외할 수 있습니다.

주제

- 보안 인증
- 금융 정보
- 개인 식별 정보(PII)

특정 관리형 데이터 식별자 또는 Macie가 현재 제공하는 모든 관리형 데이터 식별자의 전체 목록에 대한 자세한 내용은 관리형 데이터 식별자 사용 섹션을 참조하세요.

보안 인증

S3 객체에서 보안 인증 정보 데이터의 발생을 감지하기 위해 Macie는 기본적으로 다음과 같은 관리형 데이터 식별자를 사용합니다.

민감한 데이터 유형	관리형 데이터 식별자 ID
AWS 비밀 액세스 키	AWS_CREDENTIALS
HTTP Basic Authorization 헤더	HTTP_BASIC_AUTH_HEADER
OpenSSH 프라이빗 키	OPENSSH_PRIVATE_KEY
PGP 프라이빗 키	PGP_PRIVATE_KEY
퍼블릭 키 암호화 표준(PKCS) 프라이빗 키	PKCS
PuTTY 프라이빗 키	PUTTY_PRIVATE_KEY

금융 정보

S3 객체에서 발생하는 금융 정보를 감지하기 위해 Macie는 기본적으로 다음과 같은 관리형 데이터 식별자를 사용합니다.

민감한 데이터 유형	관리형 데이터 식별자 ID
신용 카드 마그네틱 스트립 데이터	CREDIT_CARD_MAGNETIC_STRIPE
신용 카드 번호	CREDIT_CARD_NUMBER (키워드 근처에 있는 신용 카드 번호의 경우)

개인 식별 정보(PII)

Macie는 S3 객체에서 개인 식별 정보(PII) 발생을 감지하기 위해 기본적으로 다음과 같은 관리형 데이터 식별자를 사용합니다.

민감한 데이터 유형	관리형 데이터 식별자 ID
운전면허증 식별 번호	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (미국의 경우), UK_DRIVERS_LICENSE
선거인단 번호	UK_ELECTORAL_ROLL_NUMBER
국적 식별 번호	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
National Insurance Number(NINO)	UK_NATIONAL_INSURANCE_NUMBER
여권 번호	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Social Insurance Number(SIN)	CANADA_SOCIAL_INSURANCE_NUMBER

민감한 데이터 유형	관리형 데이터 식별자 ID
사회 보장 번호	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
납세자 식별 번호 또는 참조 번호	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

민감한 데이터 자동 검색을 위한 기본 설정 업데이트

다음 테이블에서는 Amazon Macie가 민감한 데이터 자동 검색을 위해 기본적으로 사용하는 설정의 변경 사항을 설명합니다. Macie 문서 기록페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
새롭고 동적인 기본 관리형 데이터 식별자 세트를 구현했습니다.	새로운 자동 민감 데이터 검색 구성은 이제 관리형 데이터 식별자의 동적 기본 세트를 기반으로 합니다. 이 날짜 또는 그 이후에 처음으로 민감한 데이터 자동 검색을 활성화하는 경우, 구성은 동적 세트를 기반으로 합니다. 이 날짜 이전에 처음으로 민감한 데이터 자동 검색을 활성화한 경우, , 구성은 다른 관리형 데이터 식별자 세트를 기반으로 합니다. 자세한 내용은 이 테	2023년 8월 2일

변경 사항	설명	날짜
	이블 뒤에 있는 정보를 참조하세요.	
정식 출시	민감한 데이터 자동 검색 최초 릴리스.	2022년 11월 28일

2023년 8월 2일 이전에 민감한 데이터 자동 검색을 처음 활성화한 경우, 구성은 동적 기본 관리 데이터 식별자 세트를 기반으로 하지 않습니다. 대신 아래 표에 나와 있는 것처럼 자동 민감 데이터 검색의 초기 릴리스를 위해 정의한 정적 관리 데이터 식별자 세트를 기반으로 합니다.

민감한 데이터 자동 검색을 처음 활성화한 시기를 확인하려면 Amazon Macie 콘솔의 탐색 창에서 자동 민감 데이터 검색을 선택한 다음 상태 섹션에서 활성화된 날짜를 참조하십시오. 프로그래밍 방식으로 이 GetAutomatedDiscoveryConfiguration작업을 수행하려면 Amazon Macie API의 작업을 사용하고 필드 값을 참조하십시오`firstEnabledAt`. 날짜가 2023년 8월 2일 이전이고 동적 기본 관리 데이터 식별자 세트를 사용하기 시작하려는 경우 지원을 요청하십시오. AWS Support

다음 테이블은 정적 세트에 있는 모든 관리형 데이터 식별자를 나열합니다. 테이블은 먼저 민감한 데이터 범주별로 정렬된 다음 민감한 데이터 유형별로 정렬됩니다. 특정 관리형 데이터 식별자에 대한 자세한 내용은 관리형 데이터 식별자 사용 섹션을 참조하세요.

민감한 데이터 범주	민감한 데이터 유형	관리형 데이터 식별자 ID
보안 인증 정보	AWS 비밀 액세스 키	`AWS_CREDENTIALS`
보안 인증 정보	HTTP Basic Authorization 헤더	`HTTP_BASIC_AUTH_HEADER`
보안 인증 정보	OpenSSH 프라이빗 키	`OPENSSH_PRIVATE_KEY`
보안 인증 정보	PGP 프라이빗 키	`PGP_PRIVATE_KEY`
보안 인증 정보	퍼블릭 키 암호화 표준(PKCS) 프라이빗 키	`PKCS`
보안 인증 정보	PuTTY 프라이빗 키	`PUTTY_PRIVATE_KEY`

민감한 데이터 범주	민감한 데이터 유형	관리형 데이터 식별자 ID
금융 정보	은행 계좌 번호	BANK_ACCOUNT_NUMBER (캐나다 및 미국 은행 계좌 번호의 경우), FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
금융 정보	신용 카드 유효 기간	CREDIT_CARD_EXPIRATION
금융 정보	신용 카드 마그네틱 스트립 데이터	CREDIT_CARD_MAGNETIC_STRIPE
금융 정보	신용 카드 번호	CREDIT_CARD_NUMBER (키워드 근처에 있는 신용 카드 번호의 경우)
금융 정보	신용 카드 인증 코드	CREDIT_CARD_SECURITY_CODE
개인 정보: 개인 건강 정보(PHI)	마약단속국(DEA) 등록 번호	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
개인 정보: PHI	건강 보험 청구 번호(HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER

민감한 데이터 범주	민감한 데이터 유형	관리형 데이터 식별자 ID
개인 정보: PHI	건강 보험 또는 의료 식별 번호	`CANADA_HEALTH_NUMBER`, `EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER`, `FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER`, `FRANCE_HEALTH_INSURANCE_NUMBER`, `UK_NHS_NUMBER`, `USA_MEDICARE_BENEFICIARY_IDENTIFIER`
개인 정보: PHI	Healthcare Common Procedure Coding System(HCPCS) 코드	`USA_HEALTHCARE_PROCEDURE_CODE`
개인 정보: PHI	국가 의약품 코드(NDC)	`USA_NATIONAL_DRUG_CODE`
개인 정보: PHI	국가 공급자 식별자(NPI)	`USA_NATIONAL_PROVIDER_IDENTIFIER`
개인 정보: PHI	고유 디바이스 식별자(UDI)	`MEDICAL_DEVICE_UDI`
개인 정보: 개인 식별 정보(PII)	생년월일	`DATE_OF_BIRTH`

민감한 데이터 범주	민감한 데이터 유형	관리형 데이터 식별자 ID
개인 정보: PII	운전면허증 식별 번호	AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (미국의 경우), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVER

민감한 데이터 범주	민감한 데이터 유형	관리형 데이터 식별자 ID
		S_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
개인 정보: PII	선거인단 번호	UK_ELECTORAL_ROLL_NUMBER
개인 정보: PII	전체 이름	NAME
개인 정보: PII	위성 항법 시스템(GPS) 좌표	LATITUDE_LONGITUDE
개인 정보: PII	우편 주소	ADDRESS, BRAZIL_CEP_CODE
개인 정보: PII	국적 식별 번호	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
개인 정보: PII	National Insurance Number(NINO)	UK_NATIONAL_INSURANCE_NUMBER

민감한 데이터 범주	민감한 데이터 유형	관리형 데이터 식별자 ID
개인 정보: PII	여권 번호	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
개인 정보: PII	영주권 번호	CANADA_NATIONAL_IDENTIFICATION_NUMBER
개인 정보: PII	전화번호	BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (캐나다 및 미국의 경우), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
개인 정보: PII	Social Insurance Number(SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
개인 정보: PII	사회 보장 번호	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

민감한 데이터 범주	민감한 데이터 유형	관리형 데이터 식별자 ID
개인 정보: PII	납세자 식별 번호 또는 참조 번호	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER
개인 정보: PII	차량 식별 번호(VIN)	VEHICLE_IDENTIFICATION_NUMBER

Amazon Macie에서 민감한 데이터 검색 작업 실행

Amazon Macie를 사용하면 민감한 데이터 검색 작업을 생성하고 실행하여 Amazon Simple Storage Service (Amazon S3) 범용 버킷에서 민감한 데이터의 검색, 로깅 및 보고를 자동화할 수 있습니다. 민감한 데이터 검색 작업은 Amazon S3 객체에서 민감한 데이터를 감지하고 보고하기 위해 Macie가 수행하는 일련의 자동화된 처리 및 분석 작업입니다. 각 작업은 Macie가 찾은 민감한 데이터와 Macie가 수행하는 분석에 대한 상세한 보고서를 제공합니다. 작업을 생성하고 실행하면 조직이 Amazon S3에 저장하는 데이터와 해당 데이터에 대한 보안 또는 규정 준수 위험을 포괄적으로 파악하고 유지할 수 있습니다.

데이터 보안 및 개인정보 보호 요구 사항을 충족하고 규정 준수를 유지할 수 있도록 Macie에서는 작업 일정을 수립하고 범위를 정할 수 있는 몇 가지 옵션을 제공합니다. 온디맨드 분석 및 평가의 경우 한 번만 실행하도록 작업을 구성하거나 정기적인 분석, 평가 및 모니터링의 경우 반복적으로 실행하도록 구성할 수 있습니다. 또한 선택한 특정 S3 버킷 또는 특정 기준과 일치하는 버킷 등 작업 분석의 범위와

깊이를 정의합니다. 추가 옵션을 선택하여 해당 분석의 범위를 선택적으로 세분화할 수 있습니다. 옵션에는 태그, 접두사, 객체 최종 수정 날짜 등 S3 객체의 속성에서 파생되는 사용자 지정 포함 및 제외 기준 등이 있습니다.

각 작업에 대해 Macie가 감지하고 보고할 민감한 데이터의 유형도 지정할 수 있습니다. Macie에서 제공하는 관리형 데이터 식별자, 사용자가 정의한 사용자 지정 데이터 식별자 또는 이 두 가지를 조합하여 사용하도록 작업을 구성할 수 있습니다. 작업에 대한 특정 관리형 데이터 식별자와 사용자 지정 데이터 식별자를 선택하여 특정 유형의 민감한 데이터에 초점을 맞추도록 분석을 조정할 수 있습니다. 분석을 세밀하게 조정하기 위해 사용자가 정의한 허용 목록을 사용하도록 작업을 구성할 수도 있습니다. 허용 목록은 Macie에서 무시할 텍스트 및 텍스트 패턴을 지정합니다. 일반적으로 조직 고유의 시나리오 또는 환경에 대한 민감한 데이터 예외입니다.

각 작업은 Macie가 찾은 민감한 데이터와 Macie가 수행한 분석, 즉 민감한 데이터 결과 및 민감한 데이터 검색 결과에 대한 기록을 생성합니다. 민감한 데이터 조사 결과는 Macie가 S3 객체에서 발견한 민감한 데이터에 대한 상세 보고서입니다. 민감한 데이터 검색 결과는 S3 객체 분석에 대한 세부 정보를 기록하는 레코드입니다. Macie는 각 객체에 대해 민감한 데이터 검색 결과를 생성하여 분석할 작업을 구성합니다. 민감한 데이터를 찾지 못해서 민감한 데이터 결과가 생성되지 않는 객체와 오류 또는 문제로 인해 Macie가 분석할 수 없는 객체도 포함됩니다. 각 레코드 유형은 표준화된 스키마를 준수하므로 보안 및 규정 준수 요구 사항을 충족하기 위해 레코드를 쿼리, 모니터링 및 처리하는 데 도움이 될 수 있습니다.

주제

민감한 데이터 검색 작업의 범위 옵션

민감한 데이터 검색 작업을 통해 Amazon Macie가 민감한 데이터를 감지하고 보고하기 위해 분석하는 Amazon Simple Storage Service(S3) 데이터 범위를 정의합니다. 이를 위해 Macie는 작업을 생성하고 구성할 때 선택할 수 있는 몇 가지 작업별 옵션을 제공합니다.

범위 옵션

- S3 버킷
- 초기 실행: 기존 S3 객체
- 샘플링 깊이
- S3 객체 기준

S3 버킷

민감한 데이터 검색 작업을 생성할 때는 작업이 실행될 때 Macie가 분석할 객체를 저장할 S3 버킷을 지정합니다. 두 가지 방법으로 이 작업을 수행할 수 있습니다. 하나는 버킷 인벤토리에서 특정 S3 버킷을 선택하거나 S3 버킷의 속성에서 파생되는 사용자 지정 기준을 지정하는 것입니다.

특정 S3 버킷을 선택합니다.

이 옵션을 사용하면 분석할 각 S3 버킷을 명시적으로 선택합니다. 그런 다음, 작업이 실행되면 선택한 버킷의 객체만 분석합니다. 일별, 주별 또는 월별로 주기적으로 실행되도록 작업을 구성하면 작업이 실행될 때마다 동일한 버킷의 객체를 분석합니다.

이 구성은 특정 데이터 세트에 대한 표적 분석을 수행하려는 경우에 유용합니다. 작업에서 분석하는 버킷을 정확하고 예측 가능한 방식으로 제어할 수 있습니다.

S3 버킷 기준을 지정하십시오.

이 옵션을 사용하면 분석할 S3 버킷을 결정하는 런타임 기준을 정의합니다. 기준은 퍼블릭 액세스 설정 및 태그와 같은 버킷 속성에서 파생되는 하나 이상의 조건으로 구성됩니다. 작업이 실행되면 기준과 일치하는 버킷을 식별한 다음 해당 버킷에 있는 객체를 분석합니다. 작업을 주기적으로 실행하도록 구성하면 작업이 실행될 때마다 이 작업이 수행됩니다. 따라서 버킷 인벤토리의 변경 사항과 정의한 기준에 따라 실행될 때마다 다른 버킷의 객체를 분석할 수 있습니다.

이 구성은 버킷 인벤토리의 변화에 따라 분석 범위를 동적으로 조정하려는 경우에 유용합니다. 버킷 기준을 사용하고 주기적으로 실행하도록 작업을 구성하면 해당 기준과 일치하는 새로운 버킷을 자동으로 식별하고 민감한 데이터가 있는지 검사합니다.

이 섹션에서는 각 옵션에 대한 자세한 내용을 설명합니다.

주제

- 특정 S3 버킷 선택
- S3 버킷 기준 지정

특정 S3 버킷 선택

작업에서 분석하려는 각 S3 버킷을 명시적으로 선택하면 Macie는 현재 범용 버킷의 전체 인벤토리를 제공합니다. AWS 리전그런 다음 인벤토리를 검토하고 원하는 버킷을 선택할 수 있습니다. Macie가 이 인벤토리를 생성하고 관리하는 방법은 Macie가 Amazon S3 데이터 보안을 모니터링하는 방법을 참조하십시오.

조직의 Macie 관리자인 경우 인벤토리에는 구성원 계정이 소유한 버킷이 포함됩니다. 최대 1,000개의 계정에서 이러한 버킷을 1,000개까지 선택할 수 있습니다.

인벤토리는 버킷을 선택하는 데 도움이 되도록 각 버킷에 대한 세부 정보와 통계를 제공합니다. 여기에는 작업에서 각 버킷에서 분석할 수 있는 데이터의 양이 포함됩니다. 분류 가능한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식의 파일 이름 확장명을 가진 객체입니다. 또한 인벤토리는 버킷에 있는 객체를 분석하도록 구성된 기존 작업이 있는지 여부도 표시합니다. 이러한 세부 정보를 통해 작업의 범위를 추정하고 버킷 선택을 구체화할 수 있습니다.

인벤토리 표에서:

- 민감도 — 민감한 데이터 자동 검색이 활성화된 경우 버킷의 현재 민감도 점수를 나타냅니다.
- 분류 가능한 객체는 작업이 버킷에서 분석할 수 있는 총 객체 수입니다.
- 분류 가능한 크기는 작업이 버킷에서 분석할 수 있는 모든 객체의 총 스토리지 크기입니다.

  버킷에 압축된 객체가 저장되어 있는 경우 이 값은 압축을 푼 후의 해당 객체의 실제 크기를 반영하지 않습니다. 버킷에 버전 관리가 활성화된 경우 이 값은 버킷에 있는 각 객체의 최신 버전의 스토리지 크기를 기준으로 합니다.
- 작업별 모니터링 - 기존 작업이 버킷의 객체를 매일, 매주 또는 매월 정기적으로 분석하도록 구성되어 있는지 여부를 나타냅니다.

  이 필드의 값이 예이면 해당 버킷이 명시적으로 정기적인 작업에 포함되어 있거나 버킷이 지난 24시간 이내에 정기적인 작업 기준과 일치한 경우입니다. 또한 이러한 작업 중 하나 이상의 상태는 취소되지 않습니다. Macie는 이 데이터를 매일 업데이트합니다.
- 최신 작업 실행 - 기존 정기 또는 일회성 작업이 버킷의 객체를 분석하도록 구성된 경우 이 필드에는 해당 작업 중 하나가 실행되기 시작한 가장 최근 날짜 및 시간이 표시됩니다. 그렇지 않으면 이 필드에 대시 (-) 가 표시됩니다.

표의 버킷 이름 옆에 정보 아이콘
( )
이 표시된 경우 Amazon S3에서 최신 버킷 메타데이터를 검색하는 것이 좋습니다. 이렇게 하려면 표

위에서 새로 고침
()
을 선택합니다. 정보 아이콘은 지난 24시간 동안 버킷이 생성되었음을 의미합니다. 아마도 Macie가 일일 새로 고침 주기 의 일부로 Amazon S3에서 버킷과 객체 메타데이터를 마지막으로 검색한 이후일 것입니다. 자세한 정보는 데이터 새로 고침을 참조하세요.

표에서 버킷 이름 옆에 경고 아이콘
(⚠)
이 표시되면 Macie는 해당 버킷 또는 버킷의 객체에 액세스할 수 없습니다. 즉, 작업 시 버킷에 있는 객체를 분석할 수 없습니다. 문제를 조사하려면 Amazon S3의 버킷 정책 및 권한 설정을 검토하십시오. 예를 들어 버킷에 제한적인 버킷 정책이 있을 수 있습니다. 자세한 정보는 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을 참조하세요.

인벤토리 보기를 사용자 지정하고 특정 버킷을 더 쉽게 찾으려면 필터 상자에 필터 기준을 입력하여 표를 필터링할 수 있습니다. 다음 표에 몇 가지 예가 나와 있습니다.

다음에 해당되는 모든 버킷을 표시하려면...	이 필터 적용...
특정 계정이 소유하고 있음	계정 ID = *## ### 12## ID*
공개적으로 액세스할 수 있음	유효 권한 = 공개
정기적인 작업에 포함되지 않음	작업을 통해 적극적으로 모니터링됨 = 거짓
일회성 작업에 포함되지 않음	작업에 정의됨 = 거짓
특정 태그 키 보유*	태그 키 = *the tag key*
특정 태그 값 보유*	태그 값 = *## #*
암호화되지 않은 개체 (또는 클라이언트 측 암호화를 사용하는 개체) 를 저장합니다.	암호화에 따른 객체 수는 암호화 안함이고 From = 1

* 태그 키와 값은 대/소문자를 구분합니다. 또한 필터에서 이러한 필드에 대해 완전하고 유효한 값을 지정해야 합니다. 부분 값을 지정하거나 와일드카드 문자를 사용할 수 없습니다.

버킷의 세부 정보를 표시하려면 버킷의 이름을 선택하고 세부 정보 패널을 참조하세요. 다음을 수행할 수도 있습니다.

- 필드에 돋보기를 선택하여 특정 필드를 피벗하고 드릴다운할 수 있습니다. 같은 값을 가진 버킷을 표시하려면 를 선택하고, 다른 값을 가진 버킷을 표시하려면 를 선택합니다.
- 버킷에 있는 객체에 대한 최신 메타데이터를 검색합니다. 최근에 버킷을 만들었거나 지난 24시간 동안 버킷의 객체를 상당 부분 변경한 경우에 유용할 수 있습니다. 데이터를 검색하려면 패널의 개체 통계 섹션에서 새로고침 ()을 선택합니다. 이 옵션은 30,000개 이하의 객체를 저장하는 버킷에 사용할 수 있습니다.

S3 버킷 기준 지정

작업에 대한 버킷 기준을 지정하면 Macie는 해당 기준을 정의하고 테스트할 수 있는 옵션을 제공합니다. 이는 분석할 객체를 저장하는 S3 버킷을 결정하는 런타임 기준입니다. 작업이 실행될 때마다 기준과 일치하는 범용 버킷을 식별한 다음 적절한 버킷의 객체를 분석합니다. 조직의 Macie 관리자인 경우 여기에는 구성원 계정이 소유한 버킷이 포함됩니다.

버킷 기준 정의

버킷 기준은 S3 버킷의 속성에서 파생된 하나 이상의 조건으로 구성됩니다. 각 조건은 기준이라고도 하며 다음과 같이 구성됩니다.

- 계정 ID 또는 유효 권한과 같은 속성 기반 필드
- 연산자는 equals(eq) 또는 not equals(neq)입니다.
- 하나 이상의 값입니다.
- 조건에 맞는 버킷을 분석 (포함) 할지 아니면 건너뛰지 (제외) 할지를 나타내는 포함 또는 제외 명령문입니다.

필드에 두 개 이상의 값을 지정하는 경우 Macie는 OR 논리를 사용하여 값을 결합합니다. 조건에 두 개 이상의 조건을 지정하는 경우 Macie는 AND 논리를 사용하여 조건을 결합합니다. 또한 제외 조건은 포함 조건보다 우선합니다. 예를 들어, 공개적으로 액세스할 수 있는 버킷을 포함하고 특정 태그가 있는 버킷은 제외하는 경우, 작업은 버킷에 지정된 태그 중 하나가 없는 한 공개적으로 액세스할 수 있는 모든 버킷의 객체를 분석합니다.

S3 버킷에 대해 다음 속성 기반 필드 중 하나에서 파생되는 조건을 정의할 수 있습니다.

계정 ID

버킷을 AWS 계정 소유한 사람의 고유 식별자 (ID). 이 필드에 여러 값을 지정하려면 각 계정의 ID를 입력하고 각 항목을 쉼표로 구분합니다.

Macie는 이 필드에 와일드카드 문자나 부분값 사용을 지원하지 않습니다.

Bucket name

버킷의 이름입니다. 이 필드는 Amazon S3의 Amazon 리소스 이름(ARN) 필드가 아닌 이름와 관련이 있습니다. 이 필드에 여러 값을 지정하려면 각 버킷의 이름을 입력하고 각 항목을 쉼표로 구분합니다.

와 는 대소문자를 구분합니다. 또한, Macie는 이 필드에 와일드카드 문자나 부분값 사용을 지원하지 않습니다.

유효한 권한

버킷을 공개적으로 액세스할 수 있는지 지정합니다. 이 필드에 대해 다음 값 중 하나 이상을 선택할 수 있습니다.

- 비공개 - 일반 사용자는 버킷에 대한 읽기 또는 쓰기 액세스 권한이 없습니다.
- 공개 - 일반 사용자는 버킷에 대한 읽기 또는 쓰기 액세스 권한이 없습니다.
- 알 수 없음 - Macie는 버킷의 퍼블릭 액세스 설정을 평가할 수 없었습니다.

버킷의 이 값을 결정하기 위해 Macie는 계정의 공개 액세스 차단 설정, 버킷의 공개 액세스 차단 설정, 버킷의 버킷 정책, 버킷의 액세스 제어 목록(ACL) 등 버킷에 대한 계정 및 버킷 수준 설정의 조합을 분석합니다.

공유 액세스

버킷을 다른 사람과 공유할지 AWS 계정, Amazon CloudFront 원본 액세스 ID (OAI) 또는 CloudFront 원본 액세스 제어 (OAC) 와 공유할지를 지정합니다. 이 필드에 대해 다음 값 중 하나 이상을 선택할 수 있습니다.

- 외부 — 버킷은 CloudFront OAI, CloudFront OAC 또는 조직 외부 (소속이 아닌) 계정 중 하나 이상 또는 이들의 조합과 공유됩니다.
- 내부 - 버킷은 조직 내부(일부)에 있는 하나 이상의 계정과 공유됩니다. CloudFront OAI 또는 OAC와는 공유되지 않습니다.
- 공유되지 않음 — 버킷은 다른 계정, CloudFront OAI 또는 OAC와 공유되지 않습니다. CloudFront

- 알 수 없음 - Macie가 버킷의 공유된 접속 설정을 평가할 수 없었습니다.

버킷을 다른 AWS 계정사람과 공유하는지 여부를 확인하기 위해 Macie는 해당 버킷의 버킷 정책 및 ACL을 분석합니다. 또한 조직은 Macie 초대를 통해 AWS Organizations 또는 Macie 초대를 통해 관련 계정 그룹으로 중앙에서 관리되는 Macie 계정 집합으로 정의됩니다. 버킷 공유에 대한 Amazon S3 옵션에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3의 ID 및 액세스 관리를 참조하세요.

Macie는 버킷을 CloudFront OAI 또는 OAC와 공유할지 여부를 확인하기 위해 버킷의 버킷 정책을 분석합니다. CloudFront OAI 또는 OAC를 사용하면 사용자가 하나 이상의 지정된 배포를 통해 버킷의 객체에 액세스할 수 있습니다. CloudFront CloudFront OAI 및 OAC에 대한 자세한 내용은 Amazon 개발자 안내서의 Amazon S3 오리진에 대한 액세스 제한을 참조하십시오. CloudFront

태그

버킷과 관련된 태그입니다. 태그는 S3 버킷을 비롯한 특정 유형의 AWS 리소스에 정의하여 할당할 수 있는 레이블입니다. 각 태그는 필수 태그 키 및 선택적 태그 값으로 구성됩니다. S3 버킷 태그에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 S3 버킷 태그 비용 분담 사용을 참조하십시오.

민감한 데이터 검색 작업의 경우, 이러한 유형의 조건을 사용하여 특정 태그 키, 특정 태그 값 또는 특정 태그 키와 태그 값(쌍으로)이 있는 버킷을 포함하거나 제외할 수 있습니다. 예:

- 태그 키로 **`Project`**를 지정하고 조건에 대한 태그 값을 지정하지 않으면 해당 태그 키와 연결된 태그 값에 관계없이 프로젝트 태그 키가 있는 모든 버킷이 조건의 기준과 일치합니다.
- 태그 키로 **`Development`**과 **`Test`**를 지정하고 조건에 대한 태그 값을 지정하지 않으면 해당 태그 키와 연결된 **`Development`** 또는 **`Test`** 태그 값에 관계없이 프로젝트 태그 키가 있는 모든 버킷이 조건의 기준과 일치합니다.

조건에 여러 개의 태그 키를 지정하려면 키 필드에 각 태그 키를 입력하고 각 항목을 쉼표로 구분합니다. 조건에 여러 개의 태그 키를 지정하려면 값 필드에 각 태그 키를 입력하고 각 항목을 쉼표로 구분합니다.

태그 키와 값은 대/소문자를 구분합니다. 또한, Macie는 태그 조건에 와일드카드 문자나 부분값 사용을 지원하지 않습니다.

버킷 기준 테스트

버킷 기준을 정의하는 동안 결과를 미리 보면서 기준을 테스트하고 개선할 수 있습니다. 이렇게 하려면 콘솔에서 기준 아래에 표시되는 기준 결과 미리 보기 섹션을 펼칩니다. 이 섹션에는 현재 기준과 일치하는 S3 범용 버킷 표가 표시됩니다.

이 표에는 작업이 각 버킷에서 분석할 수 있는 데이터의 양도 포함됩니다. 분류 가능한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식의 파일 이름 확장자를 가진 객체입니다. 또한 이 표에는 버킷에 있는 객체를 주기적으로 분석하도록 구성된 기존 작업이 있는지 여부도 표시합니다.

테이블에서

- 민감도 — 민감한 데이터 자동 검색이 활성화된 경우 버킷의 현재 민감도 점수를 나타냅니다.
- 분류 가능한 객체는 작업이 버킷에서 분석할 수 있는 총 객체 수입니다.
- 분류 가능한 크기는 작업이 버킷에서 분석할 수 있는 모든 객체의 총 스토리지 크기입니다.

  버킷에 압축된 객체가 저장되어 있는 경우 이 값은 압축을 푼 후의 해당 객체의 실제 크기를 반영하지 않습니다. 버킷에 버전 관리가 활성화된 경우 이 값은 버킷에 있는 각 객체의 최신 버전의 스토리지 크기를 기준으로 합니다.
- 작업별 모니터링 - 기존 작업이 버킷의 객체를 매일, 매주 또는 매월 정기적으로 분석하도록 구성되어 있는지 여부를 나타냅니다.

  이 필드의 값이 예이면 해당 버킷이 명시적으로 정기적인 작업에 포함되어 있거나 버킷이 지난 24시간 이내에 정기적인 작업 기준과 일치한 경우입니다. 또한 이러한 작업 중 하나 이상의 상태는 취소되지 않습니다. Macie는 이 데이터를 매일 업데이트합니다.

표에서 버킷 이름 옆에 경고 아이콘
(⚠)
이 표시되면 Macie는 해당 버킷 또는 버킷의 객체에 액세스할 수 없습니다. 즉, 작업 시 버킷에 있는 객체를 분석할 수 없습니다. 문제를 조사하려면 Amazon S3의 버킷 정책 및 권한 설정을 검토하십시오. 예를 들어 버킷에 제한적인 버킷 정책이 있을 수 있습니다. 자세한 정보는 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을 참조하세요.

작업의 버킷 기준을 세분화하려면 필터 옵션을 사용하여 기준에서 조건을 추가, 변경 또는 제거합니다. 그러면 Macie가 표를 업데이트하여 변경 내용을 반영합니다.

초기 실행: 기존 S3 객체

민감한 데이터 검색 작업을 사용하여 S3 버킷에 있는 객체를 지속적으로 증분 분석할 수 있습니다. 작업을 주기적으로 실행하도록 구성하면 Macie가 자동으로 이 작업을 수행합니다. 즉, 각 실행은 이전 실행 이후에 생성되거나 변경된 객체만 분석합니다. 기존 객체 포함 옵션을 사용하여 첫 번째 증분의 시작점을 선택합니다.

- 작업을 생성한 후 즉시 기존의 적격 객체를 모두 분석하려면 이 체크박스를 선택합니다.

- 작업을 생성한 후에 첫 번째 실행 전에 대기한 다음 생성되거나 변경된 객체만 분석하려면 이 옵션의 체크박스를 선택 취소합니다.

  이미 데이터를 분석한 후 주기적으로 해당 내용을 계속 분석하려는 경우에 이 확인란의 선택을 취소하면 유용합니다. 예를 들어, 이전에 다른 서비스나 응용 프로그램을 사용하여 데이터를 분류했고 최근에 Macie를 사용하기 시작한 경우, 이 옵션을 사용하면 불필요한 비용이 발생하거나 분류 데이터를 복제하지 않고도 데이터를 계속 검색하고 분류할 수 있습니다.

이후에 정기적으로 작업을 실행할 때는 이전 실행 후에 생성되거나 변경된 객체만 분석됩니다.

정기 작업과 일회성 작업 모두 특정 시간 전후 또는 특정 기간 동안에 생성되거나 변경된 객체만 분석하도록 작업을 구성할 수도 있습니다. 이렇게 하려면 객체의 마지막 수정 날짜를 사용하는 객체 기준을 추가합니다.

샘플링 깊이

이 옵션을 사용하면 민감한 데이터 검색 작업에서 분석할 적격 S3 객체의 비율을 지정합니다. 적합한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하고, 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자를 가지며, 작업에 지정된 다른 기준과 일치하는 객체입니다.

이 값이 100%보다 작으면 Macie가 지정된 백분율까지 분석할 적격의 객체를 임의로 선택하고 해당 객체의 모든 데이터를 분석합니다. 예를 들어 10,000개의 객체를 분석하도록 작업을 구성하고 샘플링 깊이를 20% 로 지정하는 경우 Macie는 작업이 실행될 때 무작위로 선택된 약 2,000개의 적합한 객체를 분석합니다.

작업의 샘플링 깊이를 줄이면 비용을 절감하고 작업 기간을 단축할 수 있습니다. 객체의 데이터가 매우 일관되고 민감한 데이터를 각 객체가 아닌 S3 버킷에 저장하는지 여부를 결정하려는 경우에 유용합니다.

참고로 이 옵션은 분석되는 객체의 비율을 제어하는 것이지 분석되는 바이트의 비율을 제어하는 것이 아닙니다. 샘플링 깊이를 100% 미만으로 입력하면 Macie는 선택한 각 객체에 있는 데이터의 해당 비율이 아니라 선택한 각 객체에 있는 모든 데이터를 분석합니다.

S3 객체 기준

민감한 데이터 검색 작업의 범위를 세밀하게 조정하기 위해 Macie가 작업 분석에 포함하거나 제외할 S3 객체를 결정하는 사용자 지정 기준을 정의할 수도 있습니다. 이 기준은 S3 객체의 속성에서 파생된 하나 이상의 조건으로 구성됩니다. 조건은 분석할 작업을 구성하는 모든 S3 버킷의 객체에 적용됩니다. 버킷에 여러 버전의 객체를 저장하는 경우 조건은 객체의 최신 버전에 적용됩니다.

여러 조건을 객체 기준으로 정의하는 경우 Macie는 AND 논리를 사용하여 조건을 결합합니다. 또한 제외 조건은 포함 조건보다 우선합니다. 예를 들어, 파일 이름 확장자가 .pdf인 개체를 포함하고 5MB보다 큰 객체는 제외하는 경우, 작업은 객체가 5MB보다 크지 않은 한 파일 이름 확장자가 .pdf인 모든 객체를 분석합니다.

S3 객체에 대해 다음 속성 기반 필드 중 하나에서 파생되는 조건을 정의할 수 있습니다.

파일 이름 확장자

이는 S3 객체의 파일 이름 확장자와 관련이 있습니다. 이 유형의 조건을 사용하여 파일 유형에 따라 객체를 포함하거나 제외할 수 있습니다. 여러 유형의 파일에 대해 이 작업을 수행하려면 각 유형의 파일 이름 확장자를 입력하고 각 항목을 쉼표로 구분합니다(예: **`docx,pdf,xlsx`**). 조건 값으로 여러 파일 이름 확장자를 입력하면 Macie는 OR 논리를 사용하여 값을 결합합니다.

와 는 대소문자를 구분합니다. 또한, Macie는 이런 유형의 조건에 와일드카드 문자나 부분값 사용을 지원하지 않습니다.

Macie에서 분석할 수 있는 파일 유형에 대한 자세한 내용은 지원되는 파일 및 스토리지 형식을 참조하십시오.

마지막 수정

이는 Amazon S3의 마지막 수정 필드와 관련이 있습니다. Amazon S3에서 이 필드에는 S3 객체가 생성되거나 마지막으로 변경된 날짜 및 시간 중 가장 최근 날짜와 시간이 저장됩니다.

민감한 데이터 검색 작업의 경우 이 조건은 특정 날짜, 특정 날짜 및 시간 또는 전용 시간 범위가 될 수 있습니다.

- 특정 날짜 또는 날짜 및 시간 이후에 마지막으로 수정된 객체를 분석하려면 시작 필드에 값을 입력합니다.
- 특정 날짜 또는 날짜 및 시간 이후에 마지막으로 수정된 객체를 분석하려면 To 필드에 값을 입력합니다.
- 특정 시간 범위 동안 마지막으로 수정된 객체를 분석하려면 시작 필드를 사용하여 시간 범위에 첫 번째 날짜 또는 날짜 및 시간에 대한 값을 입력합니다. 종료 필드를 사용하여 시간 범위의 마지막 날짜 또는 날짜 및 시간 값을 입력합니다.
- 특정 날짜 중 언제든지 마지막으로 수정된 객체를 분석하려면 시작 날짜 필드에 날짜를 입력합니다. 종료 날짜 필드에 다음 날 날짜를 입력합니다. 그런 다음 두 시간 필드가 모두 비어 있는지 확인합니다. (Macie는 빈 시간 필드를 `00:00:00`로 취급합니다.) 예를 들어, 2023년 8월 9일에 변경된 객체를 분석하려면 시작 날짜 필드에 입력하고 종료 날짜 **`2023/08/10`** 필드에 입력합니다. 단, 어느 시간 필드에도 값을 입력하지 마십시오. **`2023/08/09`**

시간 값을 협정 세계시(UTC)로 입력하고 24시간 표기법을 사용합니다.

접두사

이는 Amazon S3의 키 필드와 관련이 있습니다. Amazon S3에서 이 필드에는 객체의 접두사를 포함하여 S3 객체의 이름이 저장됩니다. 접두사는 버킷 내 디렉터리 경로와 비슷합니다. 파일 시스템의 폴더에 비슷한 파일을 함께 저장하는 것처럼 비슷한 객체를 버킷에 함께 그룹화할 수 있습니다. Amazon S3의 객체 접두사 및 폴더에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에 있는 폴더를 사용하여 Amazon S3 콘솔에서 객체 구성하기를 참조하십시오.

이 유형의 조건을 사용하여 키(이름)가 특정 값으로 시작하는 객체를 포함하거나 제외할 수 있습니다. 예를 들어, 키가 로 AWSLogs시작하는 모든 객체를 제외하려면 접두사 조건의 **AWSLogs** 값으로 를 입력한 다음 제외를 선택합니다.

조건 값으로 여러 접두사를 입력하면 Macie는 OR 논리를 사용하여 값을 결합합니다. 예를 들어 조건의 **AWSLogs2** 값으로 **AWSLogs1** 및 를 입력하면 키가 AWSLogs1 또는 AWSLogs2로 시작하는 모든 객체가 조건의 기준과 일치합니다.

접두사 조건에 값을 입력할 때는 다음 사항에 유의해야 합니다.

- 값은 대소문자를 구분합니다.
- Macie는 이러한 값에 와일드카드 문자 사용을 지원하지 않습니다.
- Amazon S3에서는 객체 키에 객체를 저장하는 버킷 이름이 포함되지 않습니다. 따라서 이러한 값에 버킷 이름을 지정하지 마십시오.
- 접두사에 구분 기호가 포함된 경우 값에 구분 기호를 입력합니다. 예를 들어, 키가 AWSLogs/eventlogs로 시작하는 모든 객체의 조건을 **AWSLogs/eventlogs** 정의하려면 를 입력합니다. Macie는 기본 Amazon S3 구분 기호(슬래시(/)) 및 사용자 지정 구분 기호를 지원합니다.

또한 객체의 키가 객체 키의 첫 문자부터 시작하여 입력한 값과 정확히 일치하는 경우에만 객체가 조건의 기준과 일치하게 됩니다. 또한 Macie는 객체의 파일 이름을 포함하여 객체의 전체 키 값에 조건을 적용합니다.

예를 들어, 객체 키가 AWSLogs/eventlogs/testlog.csv 이고 조건에 다음 값 중 하나를 입력하면 객체는 조건의 기준과 일치합니다.

- **AWSLogs**
- **AWSLogs/event**
- **AWSLogs/eventlogs/**
- **AWSLogs/eventlogs/testlog**

- **`AWSLogs/eventlogs/testlog.csv`**

  하지만 를 입력하면 객체가 기준과 일치하지 않습니다. 즉***`eventlogs`***, 조건의 값에는 키의 첫 부분인 /가 포함되지 않습니다. AWSLogs 마찬가지로, **`awslogs`**를 입력하면 대소문자 차이로 인해 객체가 기준과 일치하지 않습니다.

스토리지 크기

이는 Amazon S3의 크기 필드와 관련이 있습니다. Amazon S3에서 이 필드는 S3 객체의 총 스토리지 크기를 나타냅니다. 객체가 압축 파일인 경우 이 값은 압축을 푼 후 실제 파일 크기를 반영하지 않습니다.

이 유형의 조건을 사용하여 특정 크기보다 작거나, 특정 크기보다 크거나, 특정 크기 범위에 속하는 객체를 포함하거나 제외할 수 있습니다. Macie는 압축 또는 보관 파일과 그 안에 포함된 파일을 포함한 모든 유형의 객체에 이러한 유형의 조건을 적용합니다. 지원되는 각 형식의 크기 기반 제한에 대한 자세한 내용은 Amazon Macie 할당량을 참조하십시오.

태그

S3 객체와 연결된 태그 태그는 S3 객체를 비롯한 특정 유형의 AWS 리소스에 정의하여 할당할 수 있는 레이블입니다. 각 태그는 필수 태그 키 및 선택적 태그 값으로 구성됩니다. S3 객체의 태그에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 태그를 사용해 공간 구분하기를 참조하십시오.

민감한 데이터 검색 작업의 경우 이 유형의 조건을 사용하여 특정 태그가 있는 객체를 포함하거나 제외할 수 있습니다. 이는 특정 태그 키 또는 특정 태그 키와 태그 값(쌍으로)일 수 있습니다. 조건 값으로 여러 태그를 지정하면 Macie는 OR 논리를 사용하여 값을 결합합니다. 예를 들어 조건의 태그 키로 **`Project1`**와 **`Project2`**를 지정하면 Project1 또는 Project2 태그 키가 있는 모든 개체가 조건의 기준과 일치합니다.

태그 키와 값은 대/소문자를 구분합니다. Macie는 이러한 유형의 조건에 와일드카드 문자나 부분값 사용을 지원하지 않습니다.

민감한 데이터 검색 작업 생성

Amazon Macie를 사용하면 민감한 데이터 검색 작업을 생성하고 실행하여 Amazon Simple Storage Service (Amazon S3) 범용 버킷에서 민감한 데이터의 검색, 로깅 및 보고를 자동화할 수 있습니다. 민감한 데이터 검색 작업은 Amazon S3 객체에서 민감한 데이터를 감지하고 보고하기 위해 Macie가 수행하는 일련의 자동화된 처리 및 분석 작업입니다. 분석이 진행됨에 따라, Macie는 민감한 데이터를 발견하고 분석한 자세한 보고서를 다음과 같이 제공합니다 - 민감한 데이터 조사 결과: Macie가 개별 S3

객체에서 발견한 민감한 데이터의 조사 결과를 보고합니다. 민감한 데이터 검색 결과: 개별 S3 객체의 분석에 대한 세부 정보를 기록합니다. 자세한 정보는 작업 통계 및 결과 검토을 참조하세요.

작업을 생성할 때는 먼저 작업 실행 시 Macie가 분석할 객체를 저장할 S3 버킷 (선택한 특정 버킷 또는 특정 기준에 맞는 버킷) 을 지정합니다. 그런 다음, 작업 실행 빈도를 한 번 또는 일별, 주별 또는 월별로 주기적으로 지정합니다. 옵션을 선택하여 작업 분석 범위를 구체화합니다. 옵션에는 태그, 접두사, 객체 최종 수정 날짜 등 S3 객체의 속성에서 파생되는 사용자 지정 기준이 포함됩니다.

작업의 일정과 범위를 정의한 후 사용할 관리형 데이터 식별자와 사용자 지정 데이터 식별자를 지정합니다.

- 관리형 데이터 식별자는 특정 유형의 민감한 데이터 (예: 특정 국가 또는 지역의 신용 카드 번호, AWS 보안 액세스 키 또는 여권 번호) 를 탐지하도록 설계된 일련의 기본 제공 기준 및 기법입니다. 이 식별자를 통해 여러 유형의 자격 증명 데이터, 금융 정보 및 프라이빗 식별 정보(PII)를 포함하여 많은 국가 또는 지역에 대해 증가하는 대규모 민감한 데이터 유형의 목록을 감지할 수 있습니다. 자세한 내용은 관리형 데이터 식별자 사용 섹션을 참조하세요.
- 사용자 지정 데이터 식별자는 민감한 데이터를 감지하기 위해 정의하는 기준 집합입니다. 사용자 지정 데이터 식별자를 사용하면, 조직의 특정 시나리오, 지적 재산 또는 독점 데이터(예: 직원 ID, 고객 계정 번호 또는 내부 데이터 분류)를 반영하는 민감한 데이터를 감지할 수 있습니다. Macie에서 제공하는 관리형 데이터 식별자를 보완할 수 있습니다. 자세한 정보는 사용자 지정 데이터 식별자 빌드을 참조하세요.

그런 다음 선택적으로 사용할 허용 목록을 선택합니다. 허용 목록은 Macie가 무시할 텍스트나 텍스트 패턴을 지정합니다. 이는 일반적으로 특정 시나리오나 환경의 민감한 데이터 예외사항(예: 조직의 공개 이름이나 전화번호, 조직에서 테스트에 사용하는 샘플 데이터)입니다. 자세한 내용은 허용 목록을 사용하여 민감한 데이터 예외사항 정의 섹션을 참조하세요.

이러한 옵션 선택을 마치면 작업 이름 및 설명과 같은 작업에 대한 일반 설정을 입력할 준비가 된 것입니다. 그런 다음, 작업을 검토하고 저장할 수 있습니다.

Tasks

- 시작하기 전 준비 사항
- 1단계: S3 버킷 선택
- 2단계: S3 버킷 선택 항목 또는 기준 검토
- 3단계: 일정 정의 및 범위 구체화
- 4단계: 관리형 데이터 식별자 선택
- 5단계: 사용자 지정 데이터 식별자 선택

- 6단계: 허용 목록 선택
- 7단계: 일반 설정 입력
- 8단계: 검토 및 생성

시작하기 전 준비 사항

작업을 생성하기 전에 다음 단계를 거치는 것이 좋습니다.

- 민감한 데이터 검색 결과의 리포지토리를 구성했는지 확인합니다. 이렇게 하려면, Amazon Macie 콘솔의 탐색 창에서 검색 결과를 선택합니다. 이러한 설정에 대해 알아보려면 민감한 데이터 검색 결과 저장 및 유지을(를) 참조하세요.
- 작업에 사용할 사용자 지정 데이터 식별자를 생성합니다. 자세한 방법은 사용자 지정 데이터 식별자 빌드(을)를 참조하세요.
- 작업에 사용할 허용 목록을 생성합니다. 자세한 방법은 허용 목록 생성 및 관리(을)를 참조하세요.
- 암호화된 S3 객체를 분석하려면 Macie가 적절한 암호화 키에 액세스하여 이를 사용할 수 있는지 확인합니다. 자세한 내용은 암호화된 S3 객체 분석 섹션을 참조하세요.
- 제한적인 버킷 정책이 적용되는 S3 버킷의 객체를 분석하려면 Macie가 객체에 액세스할 수 있는지 확인합니다. 자세한 내용은 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용 섹션을 참조하세요.

작업을 생성하기 전에 이러한 내용들을 진행하는 경우, 작업을 생성하는 과정을 간소화시키고 작업이 원하는 데이터를 분석할 수 있는지 확인할 수 있습니다.

1단계: S3 버킷 선택

작업을 생성할 때 첫 번째 단계는 작업이 실행될 때 Macie가 분석할 객체를 저장할 S3 버킷을 지정하는 것입니다. 이 단계의 경우, 두 가지 옵션이 있습니다.

- 특정 버킷 선택 - 이 옵션을 사용하면 분석할 각 S3 버킷을 명시적으로 선택합니다. 그런 다음, 작업이 실행되면 선택한 버킷의 객체만 분석합니다.
- 버킷 기준 지정 - 이 옵션을 사용하면 분석할 S3 버킷을 결정하는 런타임 기준을 정의합니다. 기준은 버킷 속성에서 파생된 하나 이상의 조건으로 구성됩니다. 그런 다음, 작업이 실행되면 기준과 일치하는 버킷을 식별하고 해당 버킷의 객체를 분석합니다.

이러한 옵션에 대한 자세한 내용은 작업에 대한 범위 옵션(을)를 참조하세요.

다음 섹션들은 각 옵션을 선택하고 구성하는 방법을 제공합니다. 원하는 옵션에 대한 선택사항을 선택합니다.

특정 버킷 선택

분석할 각 S3 버킷을 명시적으로 선택하는 경우 Macie는 현재 범용 버킷의 전체 인벤토리를 제공합니다. AWS 리전그런 다음 이 인벤토리를 사용하여 작업에 사용할 버킷을 하나 이상 선택할 수 있습니다. 이 인벤토리에 대해 알아보려면 특정 S3 버킷 선택을(를) 참조하세요.

조직의 Macie 관리자인 경우 인벤토리에는 구성원 계정이 소유한 버킷이 포함됩니다. 최대 1,000개의 계정에서 이러한 버킷을 1,000개까지 선택할 수 있습니다.

작업에 사용할 특정 S3 버킷을 선택하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다.
3. 작업 생성을 선택합니다.
4. S3 버킷 선택 페이지에서 특정 버킷 선택을 선택합니다. Macie는 현재 지역의 계정에 대한 모든 범용 버킷의 표를 표시합니다.
5. S3 버킷 선택 섹션에서 선택적으로 새로 고침
   ( )
   을 선택하여 Amazon S3에서 최신 버킷 메타데이터를 검색합니다.

   버킷 이름 옆에 정보 아이콘
   ( )
   이 표시되면 이렇게 하는 것이 좋습니다. 정보 아이콘은 지난 24시간 동안 버킷이 생성되었음을 의미합니다. 아마도 Macie가 일일 새로 고침 주기의 일부로 Amazon S3에서 버킷과 객체 메타데이터를 마지막으로 검색한 이후일 것입니다.
6. 테이블에서 작업이 분석할 각 버킷의 확인란을 선택합니다.

> **Tip**
>
> - 특정 버킷을 더 쉽게 찾으려면 테이블 위의 필터 상자에 필터 기준을 입력합니다. 열 머리글을 선택하여 테이블을 정렬할 수 있습니다.
> - 버킷의 객체를 정기적으로 분석하도록 작업을 이미 구성했는지 확인하려면 작업별 모니터링 필드를 참조합니다. 필드에 예가 표시되면 해당 버킷이 정기 작업에 명시적으로 포함되어 있거나 버킷이 지난 24시간 이내에 정기 작업 기준과 일치한 것입니다. 또한 이

러한 작업 중 하나 이상의 상태는 취소되지 않습니다. Macie는 이 데이터를 매일 업데이트합니다.

- 기존 정기 또는 일회성 작업에서 버킷의 객체를 가장 최근에 분석한 시점을 확인하려면 최근 작업 실행 필드를 참조합니다. 해당 작업에 대한 추가 정보는 버킷의 세부 정보를 참조하세요.
- 버킷의 세부 정보를 표시하려면 버킷의 이름을 선택합니다. 세부 정보 패널은 작업 관련 정보 외에도 버킷의 공개 액세스 설정과 같은 버킷에 대한 통계 및 기타 정보를 제공합니다. 이 데이터에 대해 알아보려면 S3 버킷 인벤토리 검토을(를) 참조하세요.

7. 버킷 선택을 마치면 다음을 선택합니다.

다음 단계에서는 선택 항목을 검토하고 검증하겠습니다.

버킷 기준 지정

분석할 S3 버킷을 결정하는 런타임 기준을 지정하기로 선택한 경우 Macie는 기준의 개별 조건에 대한 필드, 연산자 및 값을 선택하는 데 도움이 되는 옵션을 제공합니다. 이러한 옵션에 대해 자세히 알아보려면 S3 버킷 기준 지정 단원을 참조하세요.

작업에 대한 S3 버킷 기준을 지정하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다.
3. 작업 생성을 선택합니다.
4. S3 버킷 선택 페이지에서 버킷 기준 지정을 선택합니다.
5. 버킷 기준 지정 하에서, 다음을 수행하여 기준에 조건을 추가합니다.

   a. 필터 상자에 커서를 놓고 조건에 사용할 버킷 속성을 선택합니다.
   b. 첫 번째 상자에서 조건의 연산자(같음 또는 같지 않음)를 선택합니다.
   c. 다음 상자에서, 속성 값을 하나 이상 입력합니다.

      버킷 속성의 유형과 특성에 따라, Macie는 값을 입력하기 위한 다양한 옵션을 표시합니다. 예를 들어, 유효 권한 속성을 선택하면 Macie는 선택할 수 있는 값 목록을 표시합니다. 계정 ID 속성을 선택하면 Macie는 하나 이상의 AWS 계정 ID를 입력할 수 있는 텍스트 상자를 표시합니다. 텍스트 상자에 여러 값을 입력하려면 각각의 값을 입력하고 각각의 항목을 쉼표로 구분합니다.
   d. 적용을 선택합니다. Macie는 조건을 추가하여 필터 상자 아래에 표시합니다.

기본적으로, Macie는 include 문을 사용하여 조건을 추가합니다. 즉, 조건과 일치하는 버킷의 객체를 분석(포함)하도록 작업이 구성되어 있습니다. 조건과 일치하는 버킷을 건너뛰려면(제외시키려면) 조건에 대해 포함을 선택한 다음, 제외를 선택합니다.

e. 기준에 추가할 각 조건에 대해 이전 단계를 반복합니다.

6. 기준을 테스트하려면 기준 결과 미리 보기 섹션을 펼치십시오. 이 섹션에는 현재 기준과 일치하는 범용 버킷 표가 표시됩니다.
7. 기준을 구체화하려면, 다음 작업 중 하나를 수행합니다.

   - 조건을 제거하려면 조건에 대해 X를 선택합니다.
   - 조건을 변경하려면 조건에 대해 X를 선택하여 조건을 제거합니다. 그런 다음, 올바른 설정이 있는 조건을 추가합니다.
   - 모든 조건을 제거하려면 필터 지우기를 선택합니다.

   Macie는 변경 내용을 반영하도록 기준 결과 테이블을 업데이트합니다.
8. 버킷 기준 지정을 마치면 다음을 선택합니다.

다음 단계에서는 기준을 검토하고 검증하겠습니다.

2단계: S3 버킷 선택 항목 또는 기준 검토

이 단계의 경우, 이전 단계에서 올바른 설정을 선택했는지 확인합니다.

- 버킷 선택 검토 - 작업에 대해 특정 S3 버킷을 선택한 경우 버킷 테이블를 검토하고 필요에 따라 버킷 선택을 변경합니다. 이 테이블은 작업 분석의 예상 범위와 비용에 대한 통찰력을 제공합니다. 데이터는 현재 버킷에 저장되어 있는 객체의 크기 및 유형을 기반으로 합니다.

  테이블에서 추정 비용 필드는 S3 버킷에 있는 객체를 분석하는 데 대한 총 예상 비용(미국 달러 기준)을 나타냅니다. 각 추정치는 작업이 버킷에서 분석할 압축되지 않은 데이터의 예상 양을 반영합니다. 객체를 압축하거나 파일을 보관하는 경우, 추정치에서는 파일이 3:1 의 압축률을 사용하며 작업에서 추출된 모든 파일을 분석할 수 있다고 가정합니다. 자세한 내용은 작업 비용 예측 및 모니터링 섹션을 참조하세요.
- 버킷 기준 검토 - 작업에 대한 버킷 기준을 지정한 경우, 기준의 각 조건을 검토합니다. 기준을 변경하려면, 이전을 선택한 다음, 이전 단계의 필터 옵션을 사용하여 올바른 기준을 입력합니다. 마쳤으면 다음을 선택합니다.

설정 검토 및 확인을 마치면 다음을 선택합니다.

3단계: 일정 정의 및 범위 구체화

이 단계에서는 작업을 실행할 빈도(한 번 또는 매일, 매주 또는 매월 정기적으로)를 지정합니다. 다양한 옵션을 선택하여 작업 분석 범위를 구체화합니다. 이러한 옵션에 대해 자세히 알아보려면 작업에 대한 범위 옵션을(를) 참조하세요.

일정을 정의하고 작업 범위를 구체화하려면

1. 범위 구체화 페이지에서 작업을 실행할 빈도를 지정합니다.

   - 작업을 한 번만 실행하려면 작업 생성을 완료한 직후 일회성 작업을 선택합니다.
   - 작업을 정기적으로 반복적으로 실행하려면 예약된 작업을 선택합니다. 업데이트 빈도에서 작업을 매일, 매주 또는 매월 실행할지 선택합니다. 그런 다음, 기존 객체 포함 옵션을 사용하여 작업의 첫 번째 실행 범위를 정의합니다.
     - 이 확인란을 선택하여 작업을 생성한 후에 즉시 기존의 적격 객체를 모두 분석합니다. 이후에 실행할 때는 이전 실행 후에 생성되거나 변경된 객체만 분석됩니다.
     - 모든 기존 객체의 분석을 건너뛰려면 이 확인란의 선택을 취소합니다. 작업의 첫 번째 실행에서는 작업을 생성한 후 첫 번째 실행이 시작되기 전에 생성되거나 변경된 객체만 분석됩니다. 이후에 실행할 때는 이전 실행 후에 생성되거나 변경된 객체만 분석됩니다.

       이미 데이터를 분석한 후 주기적으로 해당 내용을 계속 분석하려는 경우에 이 확인란의 선택을 취소하면 유용합니다. 예를 들어, 이전에 다른 서비스나 응용 프로그램을 사용하여 데이터를 분류했고 최근에 Macie를 사용하기 시작한 경우, 이 옵션을 사용하면 불필요한 비용이 발생하거나 분류 데이터를 복제하지 않고도 데이터를 계속 검색하고 분류할 수 있습니다.
2. (선택 사항) 작업을 통해 분석할 객체의 비율을 지정하려면 샘플링 깊이 상자에 백분율을 입력합니다.

   이 값이 100%보다 작으면 Macie가 지정된 백분율까지 분석할 객체를 임의로 선택하고 해당 객체의 모든 데이터를 분석합니다. 기본값은 100%입니다.
3. (선택 사항) 작업 분석에 포함시키거나 제외시킬 S3 객체를 결정하는 특정 기준을 추가하려면 추가 설정 섹션을 확장한 다음 기준을 입력합니다. 이러한 기준은 객체의 속성에서 파생된 개별 조건으로 구성됩니다.

   - 특정 조건에 맞는 객체를 분석하려면(포함시키려면) 조건 유형과 값을 입력한 다음 포함을 선택합니다.

- 특정 조건에 맞는 객체를 건너뛰려면(제외시키려면) 조건 유형과 값을 입력한 다음 제외를 선택합니다.

  원하는 각 포함 또는 제외 조건에 대해 이 단계를 반복합니다.

  조건을 여러 개 입력하면 모든 제외 조건이 포함 조건보다 우선합니다. 예를 들어, 파일 이름 확장자가 .pdf인 개체를 포함하고 5MB보다 큰 객체는 제외하는 경우, 작업은 객체가 5MB보다 크지 않은 한 파일 이름 확장자가 .pdf인 모든 객체를 분석합니다.

4. 마쳤으면 다음을 선택합니다.

4단계: 관리형 데이터 식별자 선택

이 단계에서는 S3 객체를 분석할 때 작업에서 사용할 관리형 데이터 식별자를 지정합니다. 여기에는 두 가지 옵션이 있습니다.

- 권장 설정 사용 - 이 옵션을 사용하면 작업에서 작업에 권장하는 관리형 데이터 식별자 세트를 사용하여 S3 객체를 분석합니다. 이 세트는 민감한 데이터의 일반적인 범주와 유형을 탐지하도록 설계되었습니다. 현재 세트에 있는 관리형 데이터 식별자 목록을 검토하려면 작업에 권장되는 관리형 데이터 식별자을(를) 참조합니다. 세트에서 관리형 데이터 식별자를 추가하거나 제거할 때마다 해당 목록이 업데이트됩니다.
- 사용자 지정 설정 사용 - 이 옵션을 사용하면 작업에서 선택한 관리형 데이터 식별자를 사용하여 S3 객체를 분석합니다. 이는 현재 사용 가능한 관리형 데이터 식별자 전부 또는 일부만 될 수 있습니다. 관리형 데이터 식별자를 사용하지 않도록 작업을 구성할 수도 있습니다. 대신 다음 단계에서 선택한 사용자 지정 데이터 식별자만 작업에서 사용할 수 있습니다. 현재 사용 가능한 관리형 데이터 식별자 목록을 검토하려면 빠른 참조: Amazon Macie 관리형 데이터 식별자을(를) 참조하세요. 새 관리형 데이터 식별자를 릴리스할 때마다 해당 목록이 업데이트됩니다.

두 옵션 중 하나를 선택하면 Macie는 관리형 데이터 식별자 테이블를 표시합니다. 테이블에서, 민감한 데이터 유형 필드는 관리형 데이터 식별자의 고유 식별자(ID)를 지정합니다. 이 ID는 관리형 데이터 식별자가 탐지하도록 설계된 민감한 데이터의 유형을 설명합니다. 예를 들어, 미국 여권 번호의 경우 USA_PASSPORT_NUMBER, 신용 카드 번호의 경우 CREDIT_CARD_NUMBER, PGP 프라이빗 키의 경우 PGP_PRIVATE_KEY 등이 있습니다. 특정 식별자를 더 빨리 찾으려면, 민감한 데이터 범주 또는 유형별로 테이블을 정렬하고 필터링할 수 있습니다.

작업에 대한 관리형 데이터 식별자를 선택하려면

1. 관리형 데이터 식별자 선택 페이지의 관리형 데이터 식별자 옵션에서 다음 중 하나를 수행하세요.

- 작업에 대해 권장하는 관리형 데이터 식별자 세트를 사용하려면 권장을 선택합니다.

  이 옵션을 선택하고 작업을 두 번 이상 실행하도록 구성한 경우, 각 실행은 실행 시작 시 권장 세트에 있는 모든 관리형 데이터 식별자를 자동으로 사용합니다. 여기에는 릴리즈하여 세트에 추가한 새로운 관리형 데이터 식별자가 포함됩니다. 세트에서 제거하고 더 이상 작업에 권장되지 않는 관리형 데이터 식별자는 제외됩니다.

- 선택한 특정 관리형 데이터 식별자만 사용하려면, 사용자 지정을 선택한 다음, 특정 관리형 데이터 식별자 사용을 선택합니다. 그런 다음, 테이블에서 작업에서 사용하고자 하는 각 관리형 데이터 식별자의 확인란을 선택합니다.

  이 옵션을 선택하고 작업을 두 번 이상 실행하도록 구성한 경우, 각 실행은 선택한 관리형 데이터 식별자만 사용합니다. 즉, 작업은 실행될 때마다 이와 동일한 관리형 데이터 식별자를 사용합니다.

- Macie에서 현재 제공하는 모든 관리형 데이터 식별자를 사용하려면, 사용자 지정을 선택한 다음, 특정 관리형 데이터 식별자 사용을 선택합니다. 그런 다음, 테이블에서 선택 열 머리글의 확인란을 선택하여 모든 행을 선택합니다.

  이 옵션을 선택하고 작업을 두 번 이상 실행하도록 구성한 경우, 각 실행은 선택한 관리형 데이터 식별자만 사용합니다. 즉, 작업은 실행될 때마다 이와 동일한 관리형 데이터 식별자를 사용합니다.

- 관리형 데이터 식별자를 사용하지 않고 사용자 지정 데이터 식별자만 사용하려면, 사용자 지정을 선택한 다음, 관리형 데이터 식별자 사용 안 함을 선택합니다. 그런 다음, 다음 단계에서 사용할 사용자 지정 데이터 식별자를 선택합니다.

2. 마쳤으면 다음을 선택합니다.

5단계: 사용자 지정 데이터 식별자 선택

이 단계에서는 S3 객체를 분석할 때 작업에 사용할 사용자 지정 데이터 식별자를 선택합니다. 작업에서는 사용하도록 구성한 관리 데이터 식별자 외에도 선택된 식별자도 사용합니다. 사용자 지정 데이터 식별자에 대한 자세한 내용은 사용자 지정 데이터 식별자 빌드을(를) 참조하세요.

작업에 대해 사용할 사용자 지정 데이터 식별자를 선택하려면

1. 사용자 지정 데이터 식별자 선택 페이지에서 작업에서 사용할 각 사용자 지정 데이터 식별자의 확인란을 선택합니다. 사용자 지정 데이터 식별자를 30개까지 선택할 수 있습니다.

> **Tip**
>
> 사용자 지정 데이터 식별자를 선택하기 전에 식별자의 설정을 검토하거나 테스트하려면, 식별자 이름 옆의 링크 아이콘 ( ) 을 선택합니다. Macie는 식별자 설정을 표시하는 페이지를 엽니다. 이 페이지를 사용하여 샘플 데이터로 식별자를 테스트할 수도 있습니다. 이렇게 하려면 샘플 데이터 상자에 텍스트를 1,000자까지 입력한 다음 테스트를 선택합니다. Macie는 식별자를 사용하여 샘플 데이터를 평가한 다음 일치 개수를 보고합니다.

2. 사용자 지정 데이터 식별자를 모두 선택했으면 다음을 선택합니다.

6단계: 허용 목록 선택

이 단계에서는 S3 객체를 분석할 때 작업에서 사용할 허용 목록을 선택합니다. 허용 목록에 대해 자세히 알아보려면 허용 목록을 사용하여 민감한 데이터 예외사항 정의을(를) 참조하세요.

작업에 대한 허용 목록을 선택하려면

1. 허용 목록 선택 페이지에서 작업에서 사용할 각 허용 목록의 확인란을 선택합니다. 리스트를 10개까지 선택할 수 있습니다.

> **Tip**
>
> 허용 목록을 선택하기 전에 목록을 검토하려면 목록 이름 옆의 링크 아이콘 ( ) 을 선택합니다. Macie는 목록 설정을 표시하는 페이지를 엽니다. 목록에 정규 표현식(regex)이 지정된 경우, 이 페이지를 사용하여 샘플 데이터로 정규 표현식을 테스트할 수도 있습니다. 이렇게 하려면 샘플 데이터 상자에 텍스트를 1,000자까지 입력한 다음 테스트를 선택합니다. Macie는 regex를 사용하여 샘플 데이터를 평가한 다음 일치 개수를 보고합니다.

2. 허용 목록 선택을 마치면 다음을 선택합니다.

7단계: 일반 설정 입력

이 단계에서는 작업의 이름을 지정하고 선택적으로 설명을 지정합니다. 작업에 태그를 할당할 수도 있습니다. 태그는 사용자가 정의하여 특정 유형의 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별, 분류, 관리하는 데 도움이 됩니다. 자세한 내용은 Amazon Macie에 리소스 태그 지정(을)를 참조하세요.

작업에 대한 일반 설정을 입력하려면

1. 일반 설정 입력 페이지의 작업 이름 상자에 작업 이름을 입력합니다. 이름은 최대 500자까지 포함할 수 있습니다.
2. (선택 사항) 작업 설명의 경우, 작업에 대한 간략한 설명을 입력합니다. 설명은 200자까지 포함할 수 있습니다.
3. (선택 사항) 태그의 경우, 태그 추가를 선택한 다음, 작업에 할당할 태그를 50개까지 입력합니다.
4. 마쳤으면 다음을 선택합니다.

8단계: 검토 및 생성

마지막 단계에서 작업의 구성 설정을 검토하고 설정이 올바른지 확인합니다. 이것은 중요한 단계입니다. 작업을 생성한 후에는 이러한 설정을 변경할 수 없습니다. 이를 통해 수행하는 데이터 프라이버시 및 보호 감사 또는 조사에 대한 민감한 데이터 조사 결과 및 검색 결과에 대한 변경 불가능한 기록이 있는지 확인할 수 있습니다.

작업 설정에 따라 또한 작업을 한 번 실행하는 예상 비용(미국 달러)을 검토할 수 있습니다. 작업을 위해 특정 S3 버킷을 선택한 경우, 예상 값은 선택한 버킷의 객체 크기 및 유형, 그리고 해당 데이터에서 분석할 수 있는 데이터의 양을 기반으로 합니다. 작업에 대해 버킷 기준을 지정한 경우, 현재 기준과 일치하는 최대 500개 버킷의 객체 크기 및 유형, 그리고 해당 데이터에서 작업에서 분석할 수 있는 데이터의 양을 기준으로 추정치가 산출됩니다. 이 예상치에 대한 자세한 내용은 작업 비용 예측 및 모니터링을(를) 참조하세요.

작업을 검토하고 생성하려면

1. 검토 및 생성 페이지에서, 각 설정을 검토하고 올바른지 확인하세요. 설정을 변경하려면, 설정이 포함된 섹션에서 편집을 선택한 다음, 올바른 설정을 입력합니다. 탐색 탭을 사용하여 설정이 포함된 페이지로 이동할 수도 있습니다.
2. 설정 확인을 마치면 제출을 선택하여 작업을 생성하고 저장합니다. Macie가 설정을 확인하고 해결해야 할 문제를 알려줍니다.

> **Note**
>
> 민감한 데이터 검색 결과를 위한 리포지토리를 구성하지 않은 경우, Macie는 경고를 표시하고 작업을 저장하지 않습니다. 이 문제를 해결하려면 민감한 데이터 검색 결과를 위한 리포지토리 섹션에서 구성을 선택합니다. 그런 다음, 리포지토리의 구성 설정을 입력합니다. 자세한 방법은 민감한 데이터 검색 결과 저장 및 유지(을)를 참조하세요. 설정을 입력한 후, 검토 및 생성 페이지로 돌아가서 해당 페이지의 민감한 데이터 검색 결과를 위한 리포지토리 섹션에서 새로 고침 () 을 선택합니다.
>
> 권장하지는 않지만 리포지토리 요구 사항을 일시적으로 재정의하고 작업을 저장할 수 있습니다. 이렇게 할 경우, 작업의 검색 결과를 잃을 위험이 있습니다. Macie는 결과를 90일 동안만 보존하기 때문입니다. 요구 사항을 일시적으로 무시하려면 우선 적용 옵션의 확인란을 선택합니다.

3. Macie에서 해결해야 할 문제를 알리면, 문제를 해결하고 제출을 다시 선택하여 작업을 만들고 저장합니다.

한 번, 매일 또는 현재 요일 또는 월에 실행하도록 작업을 구성한 경우, Macie는 작업을 저장한 후 즉시 작업을 실행하기 시작합니다. 그렇지 않은 경우, Macie는 지정된 요일 또는 월에 작업을 실행하도록 준비합니다. 작업을 모니터링하기 위해 작업 상태를 확인할 수 있습니다.

민감한 데이터 검색 작업에 대한 통계 및 결과 검토

민감한 데이터 검색 작업을 실행하면 Amazon Macie는 해당 작업에 대한 특정 통계 데이터를 자동으로 계산하여 보고합니다. 예를 들어 Macie는 작업이 실행된 횟수와 현재 작업이 실행 중인 가운데 아직 처리하지 않은 Amazon Simple Storage Service(S3) 객체의 대략적인 수를 보고합니다. 또한 Macie는 로그 이벤트, 민감한 데이터 조사 결과, 민감한 데이터 조사 결과 등 여러 유형의 작업 조사 결과를 생성합니다.

주제

- 민감한 데이터 검색 작업에 대한 결과 유형
- 민감한 데이터 검색 작업에 대한 통계 및 결과 검토

민감한 데이터 검색 작업에 대한 결과 유형

민감한 데이터 검색 작업이 진행됨에 따라 Amazon Macie는 해당 작업에 대해 다음과 같은 유형의 결과를 생성합니다.

로그 이벤트

이는 작업이 실행되는 동안 발생한 이벤트의 레코드입니다. Macie는 특정 이벤트에 대한 데이터를 자동으로 기록하고 Amazon CloudWatch Logs에 게시합니다. 이러한 로그의 데이터는 작업이 시작되거나 중지된 정확한 날짜 및 시간과 같은 작업 진행 상황 또는 상태의 변경 기록을 제공합니다. 이 데이터는 작업이 실행되는 동안 발생한 계정 또는 버킷 수준의 오류에 대한 세부 정보도 제공합니다.

로그 이벤트를 통해 작업을 모니터링하고 작업에서 원하는 데이터를 분석하지 못하게 했던 문제를 해결할 수 있습니다. 작업에서 런타임 기준을 사용하여 분석할 S3 버킷을 결정하는 경우, 로그 이벤트를 통해 작업 실행 시 기준과 일치하는지 여부와 해당 S3 버킷을 확인할 수도 있습니다.

Amazon CloudWatch 콘솔 또는 Amazon CloudWatch Logs API를 사용하여 로그 이벤트에 액세스할 수 있습니다. Amazon Macie 콘솔은 작업에 대한 로그 이벤트를 쉽게 탐색할 수 있도록 해당 로그 이벤트로 연결되는 링크를 제공합니다. 자세한 정보는 작업 모니터링을 참조하세요.

민감한 데이터 조사 결과

Macie가 S3 객체에서 찾은 민감한 데이터에 대한 보고서입니다. 각 조사 결과는 심각도 등급과 다음과 같은 세부 정보를 제공합니다.

- Macie가 민감한 데이터를 발견한 날짜 및 시간.
- Macie가 발견한 민감한 데이터의 범주 및 유형.
- Macie가 발견한 각 유형의 민감한 데이터 발생 횟수.
- 조사 결과를 생성한 작업에 대한 고유 식별자.
- 영향을 받는 S3 버킷 및 객체에 대한 이름, 퍼블릭 액세스 설정, 암호화 유형 및 기타 정보.

영향을 받는 S3 객체의 파일 유형이나 스토리지 형식에 따라 세부 정보에는 Macie가 발견한 최대 15개의 민감한 데이터 위치가 포함될 수 있습니다. 위치 데이터를 보고하기 위해 민감한 데이터 조사 결과는 표준화된 JSON 스키마를 사용합니다.

민감한 데이터 조사 결과에는 Macie가 발견한 민감한 데이터는 포함되지 않습니다. 대신 필요에 따라 추가 조사 및 수정에 사용할 수 있는 정보를 제공합니다.

Macie는 민감한 데이터 조사 결과를 90일 동안 저장합니다. Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 이러한 결과에 액세스할 수 있습니다. 또한 다른 애플리케이션, 서비스 및 시스템을 사용하여 모니터링하고 처리할 수 있습니다. 자세한 정보는 조사 결과 분석을 참조하세요.

민감한 데이터 검색 결과

S3 객체의 분석에 대한 세부 정보를 기록하는 레코드입니다. Macie는 사용자가 분석하도록 작업을 구성하는 각 개체에 대해 민감한 데이터 검색 결과를 자동으로 생성합니다. 여기에는 Macie가 민감한 데이터를 발견하지 못하여 민감한 데이터 결과를 생성하지 않는 객체와 권한 설정 또는 지원되지 않는 파일 또는 저장 형식 사용과 같은 오류나 문제로 인해 Macie가 분석할 수 없는 객체가 포함됩니다.

Macie가 S3 객체에서 민감한 데이터를 발견한 경우 민감한 데이터 조사 결과에는 민감한 데이터 조사 결과의 데이터가 포함됩니다. Macie가 객체에서 발견한 각 유형의 민감한 데이터가 1,000건 이상 발생한 위치와 같은 추가 정보도 제공합니다. 예:

- Microsoft Excel 통합 문서, CSV 파일 또는 TSV 파일에 있는 셀 또는 필드의 열 및 행 번호
- JSON 또는 JSON 라인 파일에 있는 필드 또는 배열의 경로
- CSV, JSON, JSON 라인 또는 TSV 파일이 아닌 비이진 텍스트 파일(예: HTML, TXT 또는 XML 파일)의 줄 번호
- Adobe PDF(휴대용 문서 형식) 파일에 있는 페이지의 페이지 번호
- Apache Avro 객체 컨테이너 또는 Apache Parquet 파일에 있는 레코드 인덱스 및 레코드 내 필드 경로

영향을 받는 S3 객체가 아카이브 파일 (예: .tar 또는.zip 파일) 인 경우, 민감한 데이터 검색 결과는 Macie가 아카이브에서 추출한 개별 파일의 민감한 데이터 발생에 대한 자세한 위치 데이터도 제공합니다. Macie는 아카이브 파일에 대한 민감한 데이터 조사 결과에 이 정보를 포함시키지 않습니다. 위치 데이터를 보고하기 위해 민감한 데이터 검색 결과는 표준화된 JSON 스키마를 사용합니다.

민감한 데이터 검색 결과에는 Macie가 발견한 민감한 데이터는 포함되지 않습니다. 대신 데이터 프라이버시 및 보호 감사 또는 조사에 도움이 될 수 있는 분석 기록을 제공합니다.

Macie는 민감한 데이터 검색 결과를 90일 동안 저장합니다. Amazon Macie 콘솔이나 Amazon Macie API에서는 바로 액세스할 수 없습니다. 대신 Macie를 구성하여 S3 버킷에 저장할 수 있습니다. 버킷은 모든 민감한 데이터 검색 결과를 위한 확정적이고 장기적인 리포지토리 역할을 할 수 있습니다. 그런 다음, 필요에 따라 해당 리포지토리에 있는 결과에 액세스하고 쿼리할 수 있습니다. 이러한 설정을 구성하는 방법에 대해 알아보려면 민감한 데이터 검색 결과 저장 및 유지 단원을 참조하세요.

설정을 구성하면 Macie는 민감한 데이터 검색 결과를 JSON 라인(.jsonl) 파일에 기록하고, 해당 파일을 암호화하여 GNU Zip(.gz) 파일로 S3 버킷에 추가합니다. 결과를 쉽게 찾을 수 있도록 Amazon Macie 콘솔은 결과에 대한 링크를 제공합니다.

민감한 데이터 탐지 조사 결과와 민감한 데이터 조사 결과 모두 표준화된 스키마를 따릅니다. 이렇게 하면 다른 애플리케이션, 서비스 및 시스템을 사용하여 선택적으로 쿼리, 모니터링 및 처리하는 데 도움이 될 수 있습니다.

> **Tip**
>
> 민감한 데이터 검색 결과를 쿼리하고 사용하여 잠재적 데이터 보안 위험을 분석하고 보고하는 방법에 대한 자세한 지침 예제는 보안 QuickSight 블로그의 Amazon Athena와 Amazon을 사용하여 Macie의 민감한 데이터 검색 결과를 쿼리하고 시각화하는 방법 블로그 게시물을 참조하십시오.AWS
>
> 민감한 데이터 검색 결과를 분석하는 데 사용할 수 있는 Amazon Athena 쿼리 샘플을 보려면의 Amazon Macie 결과 분석 리포지토리를 방문하십시오. GitHub 또한 이 리포지토리는 결과를 검색하고 해독할 수 있게 Athena를 구성하는 지침과 결과에 대한 테이블을 생성하는 스크립트도 제공합니다.

민감한 데이터 검색 작업에 대한 통계 및 결과 검토

개별 민감한 데이터 검색 작업에 대한 처리 통계 및 결과를 검토하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 다음 단계에 따라 콘솔을 사용하여 작업 통계 및 결과를 검토할 수 있습니다.

프로그래밍 방식으로 작업의 처리 통계에 액세스하려면 Amazon DescribeClassificationJobMacie API의 작업을 사용하십시오. 작업에서 얻은 결과에 프로그래밍 방식으로 액세스하려면 Amazon Macie API ListFindings작업을 사용하고 필드의 필터 조건에 작업의 고유 식별자를 지정하십시오. `classificationDetails.jobId` 자세한 방법은 조사 결과에 필터 생성 및 적용(을)를 참조하세요. 그런 다음 GetFindings작업을 사용하여 검색 결과의 세부 정보를 검색할 수 있습니다.

작업에 대한 통계 및 결과를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다.
3. 작업 페이지에서 통계 및 결과를 검토하려는 작업의 이름을 선택합니다. 세부 정보 패널에는 작업에 대한 통계, 설정 및 기타 정보가 표시됩니다.

4. 세부 정보 패널에서 다음 작업 중 하나를 수행합니다.

- 작업에 대한 처리 통계를 검토하려면 패널의 통계 섹션을 참조하세요. 이 섹션에는 작업이 실행된 횟수, 현재 실행 중에 작업이 아직 처리하지 않은 대략적인 개체 수와 같은 통계가 표시됩니다.
- 작업에 대한 로그 이벤트를 검토하려면 패널 상단에 있는 결과 표시를 선택한 다음 CloudWatch 로그 표시를 선택합니다. Macie는 Amazon CloudWatch 콘솔을 열고 Macie가 작업에 대해 게시한 로그 이벤트 테이블을 표시합니다.
- 작업에서 생성된 민감한 데이터 조사 결과를 모두 검토하려면 패널 상단에 결과 표시를 선택한 다음 조사 결과 표시를 선택합니다. Macie는 조사 결과 페이지를 열고 작업의 모든 조사 결과를 표시합니다. 특정 조사 결과의 세부 정보를 검토하려면 조사 결과를 선택한 다음 세부 정보 패널을 참조합니다.

> **Tip**
>
> 조사 결과 세부 정보 패널에서 세부 결과 위치 필드의 링크를 사용하여 Amazon S3의 해당 민감한 데이터 조사 결과로 이동할 수 있습니다.
>
> - 조사 결과가 대용량 아카이브 또는 압축 파일에 적용되는 경우 링크에는 해당 파일에 대한 조사 결과가 들어 있는 폴더가 표시됩니다. 조사 결과가 100개 이상인 아카이브 또는 압축 파일은 큽니다.
> - 조사 결과가 작은 아카이브 또는 압축 파일에 적용되는 경우 링크에는 해당 파일의 조사 결과가 포함된 파일이 표시됩니다. 조사 결과가 100개 이하인 아카이브 또는 압축 파일은 작습니다.
> - 조사 결과가 다른 유형의 파일에 적용되는 경우 링크에는 해당 파일에 대한 조사 결과가 포함된 파일이 표시됩니다.

- 작업에서 생성된 민감한 데이터 조사 결과를 모두 검토하려면 패널 상단에 결과 표시를 선택한 다음 분류 표시를 선택합니다. Macie는 Amazon S3 콘솔을 열고 작업에 대한 모든 조사 결과가 들어 있는 폴더를 표시합니다. S3 버킷에 민감한 데이터 조사 결과를 저장하도록 Macie를 구성한 후에만 이 옵션을 사용할 수 있습니다.

Amazon CloudWatch Logs를 사용하여 민감한 데이터 검색 작업 모니터링

민감한 데이터 검색 작업의 전체 상태를 모니터링하는 것 외에도 작업이 진행되면서 발생하는 특정 이벤트를 모니터링하고 분석할 수 있습니다. Amazon Macie가 Amazon CloudWatch Logs에 자동으로 게시하는 실시간에 가까운 로깅 데이터를 사용하여 이 작업을 수행할 수 있습니다. 이러한 로그의 데이터

는 작업 실행이 시작되거나 일시 중지되거나 실행이 완료된 정확한 날짜 및 시간과 같은 작업 진행 상황 또는 상태의 변경 기록을 제공합니다.

로그 데이터는 작업이 실행되는 동안 발생하는 계정 또는 버킷 수준의 오류에 대한 세부 정보도 제공합니다. 예를 들어, S3 버킷의 권한 설정으로 인해 작업이 버킷의 객체를 분석할 수 없는 경우 Macie는 이벤트를 기록합니다. 이벤트는 오류가 발생한 시기를 나타내며, 영향을 받는 버킷과 해당 버킷을 소유한 계정을 모두 식별합니다. 이러한 유형의 이벤트에 대한 데이터는 Macie가 원하는 데이터를 분석하지 못하게 하는 오류를 식별, 조사 및 해결하는 데 도움이 될 수 있습니다.

Amazon CloudWatch Logs를 사용하면 Macie를 비롯한 여러 시스템, 애플리케이션 및 AWS 서비스의 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. 또한 로그 데이터를 쿼리 및 분석하고, 특정 이벤트가 발생하거나 임계값이 충족되면 알려주도록 CloudWatch Logs를 구성할 수 있습니다. CloudWatch Logs는 로그 데이터를 보관하고 Amazon S3에 데이터를 내보내는 기능도 제공합니다. CloudWatch Logs에 대한 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하세요.

주제

민감한 데이터 검색 작업의 로깅 작동 방식

민감한 데이터 검색 작업을 실행하기 시작하면 Macie는 Amazon CloudWatch Logs에 적절한 리소스를 자동으로 생성하고 구성하여 현재 AWS 리전에서 모든 작업에 대한 이벤트를 기록합니다. 그러면 Macie는 작업이 실행될 때 해당 리소스에 이벤트 데이터를 자동으로 게시합니다. 계정의 Macie 서비스 연결 역할에 대한 권한 정책을 통해 Macie가 사용자를 대신하여 이러한 작업을 수행할 수 있습니다. CloudWatch Logs에서 리소스를 생성 또는 구성하거나 작업에 대한 이벤트 데이터를 기록하기 위한 별도의 조치를 취할 필요가 없습니다.

CloudWatch Logs에서 로그는 로그 그룹으로 정리됩니다. 각 로그 그룹에는 로그 스트림이 포함되어 있습니다. 각 로그 스트림에는 로그 이벤트가 포함됩니다. 각 리소스의 일반적인 용도는 다음과 같습니다.

- 로그 그룹은 동일한 보존, 모니터링 및 액세스 제어 설정을 공유하는 로그 스트림 모음입니다. 예를 들어 모든 민감한 데이터 검색 작업에 대한 로그 모음입니다.
- 로그 스트림은 동일한 소스(예: 개별적인 민감한 데이터 검색 작업)를 공유하는 일련의 로그 이벤트입니다.

- 로그 이벤트는 애플리케이션이나 리소스에서 기록한 활동(예: Macie가 특정 민감한 데이터 검색 작업에 대해 기록하고 게시한 개별 이벤트)에 대한 기록입니다.

Macie는 모든 민감한 데이터 검색 작업에 대한 이벤트를 하나의 로그 그룹에 게시하고 각 작업에는 해당 로그 그룹에 고유의 로그 스트림이 있습니다. 로그 그룹에는 다음과 같은 접두사와 이름이 있습니다.

```
/aws/macie/classificationjobs
```

이 로그 그룹이 이미 있는 경우 Macie는 이 로그 그룹을 사용하여 작업에 대한 로그 이벤트를 저장합니다. 이 기능은 조직에서 작업 이벤트에 대해 미리 정의된 로그 보존 기간, 암호화 설정, 태그, 메트릭 필터 등이 있는 로그 그룹을 생성하는 등 AWS CloudFormation와 같은 자동 구성을 사용하는 경우 유용할 수 있습니다.

이 로그 그룹이 없는 경우 Macie는 CloudWatch Logs가 새 로그 그룹에 사용하는 기본 설정을 사용하여 그룹을 생성합니다. 설정에는 만료 안 함 로그 보존 기간이 포함됩니다. 즉, CloudWatch Logs는 로그를 무기한 저장합니다. 로그 그룹의 보존 기간을 변경하려면 Amazon CloudWatch 콘솔 또는 Amazon CloudWatch Logs API를 사용하면 됩니다. 자세한 내용을 알아보려면 Amazon CloudWatch Logs 사용 설명서의 로그 그룹 및 로그 스트림 작업을 참조하세요.

이 로그 그룹 내에서 Macie는 작업을 처음 실행할 때 사용자가 실행하는 각 작업에 대해 고유한 로그 스트림을 생성합니다. 로그 스트림의 이름은 `85a55dc0fa6ed0be5939d0408example`와 같은 작업의 고유 식별자이며 다음 형식을 따릅니다.

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

각 로그 스트림에는 Macie가 해당 작업에 대해 기록하고 게시한 모든 로그 이벤트가 들어 있습니다. 정기 작업의 경우 여기에는 모든 작업 실행에 대한 이벤트가 포함됩니다. 정기 작업의 로그 스트림을 삭제하면 Macie는 다음에 작업이 실행될 때 스트림을 다시 만듭니다. 일회성 작업의 로그 스트림을 삭제하면 복원할 수 없습니다.

모든 작업에 기본적으로 로깅이 활성화되어 있다는 점에 유의하세요. 이를 비활성화하거나 Macie가 CloudWatch Logs에 작업 이벤트를 게시하지 못하게 할 수 없습니다. 로그를 저장하지 않으려는 경우 로그 그룹의 보존 기간을 하루로 줄일 수 있습니다. 보존 기간이 끝나면 CloudWatch Logs는 로그 그룹에서 만료된 이벤트 데이터를 자동으로 삭제합니다.

민감한 데이터 검색 작업 로그 검토

Amazon CloudWatch 콘솔 또는 Amazon CloudWatch Logs API를 사용하여 민감한 데이터 검색 작업 로그를 검토할 수 있습니다. 콘솔과 API는 모두 로그 데이터를 검토하고 분석하는 데 도움이 되도록 설계된 기능을 제공합니다. CloudWatch Logs에서 다른 유형의 로그 데이터를 처리하는 것처럼 이러한 기능을 사용하여 작업에 대한 로그 스트림 및 이벤트를 처리할 수 있습니다.

예를 들어 집계 데이터를 검색하고 필터링하여 특정 시간 범위 동안 모든 작업에서 발생한 특정 유형의 이벤트를 식별할 수 있습니다. 또는 특정 작업에서 발생한 모든 이벤트를 대상으로 검토할 수 있습니다. 또한 CloudWatch Logs는 로그 데이터를 모니터링하고, 지표 필터를 정의하고, 사용자 지정 경보를 생성하는 옵션을 제공합니다.

> **Tip**
>
> Amazon Macie 콘솔을 사용하여 특정 작업에 대한 로그 이벤트로 이동하려면 다음을 수행하세요. 작업 페이지에서 작업 이름을 선택합니다. 세부 정보 패널 상단에서 결과 표시를 선택한 다음 CloudWatch 로그 보기를 선택합니다. Macie는 Amazon CloudWatch 콘솔을 열고 작업에 대한 로그 이벤트 테이블을 표시합니다.

작업 로그를 검토하려면(Amazon CloudWatch 콘솔)

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 로그를 검토할 작업을 실행한 리전을 선택합니다.
3. 왼쪽 탐색 창에서 로그(Logs)를 선택한 다음, 로그 그룹(Log groups)을 선택합니다.
4. 로그 그룹 페이지에서 /aws/macie/classificationjobs 로그 그룹을 선택합니다. CloudWatch Logs는 실행한 작업에 대한 로그 스트림 테이블을 표시합니다. 각 작업에는 고유한 스트림이 하나씩 있습니다. 각 스트림의 이름은 작업의 고유 식별자와 관련이 있습니다.
5. 로그 스트림에서 다음 중 하나를 수행합니다.

   - 특정 작업에 대한 로그 이벤트를 검토하려면 해당 작업의 로그 스트림을 선택합니다. 스트림을 더 쉽게 찾으려면 표 위의 필터 상자에 작업의 고유 식별자를 입력하세요. 로그 스트림을 선택하면 CloudWatch Logs에 작업에 대한 로그 이벤트 테이블이 표시됩니다.
   - 모든 작업에 대한 로그 이벤트를 검토하려면 모든 로그 스트림 검색을 선택합니다. CloudWatch Logs에는 모든 작업에 대한 로그 이벤트 테이블이 표시됩니다.

6. (선택 사항) 표 위의 필터 상자에 검토할 특정 이벤트의 특성을 지정하는 용어, 문구 또는 값을 입력합니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서에서 필터 패턴을 사용하여 로그 데이터 검색을 참조하세요.
7. 특정 로그 이벤트의 세부 정보를 검토하려면 해당 이벤트 행에서 오른쪽 화살표 ( ) 를 선택합니다. CloudWatch Logs에는 이벤트의 세부 정보가 JSON 형식으로 표시됩니다.

로그 이벤트의 데이터에 익숙해지면 로그 데이터를 수치형 CloudWatch 지표로 변환하는 지표 필터를 생성하고, 특정 로그 이벤트를 쉽게 식별하고 이에 대응할 수 있는 사용자 지정 경보를 생성하는 등의 작업을 수행할 수도 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하세요.

민감한 데이터 검색 작업에 대한 로그 이벤트 스키마

민감한 데이터 검색 작업의 각 로그 이벤트는 Amazon CloudWatch Logs 이벤트 스키마를 준수하는 JSON 객체이며 표준 필드 세트를 포함합니다. 일부 유형의 이벤트에는 해당 유형의 이벤트에 특히 유용한 정보를 제공하는 추가 필드가 있습니다. 예를 들어 계정 수준 오류에 대한 이벤트에는 영향을 받는 AWS 계정의 계정 ID가 포함됩니다. 버킷수준 오류 이벤트에는 영향을 받는 S3 버킷의 이름이 포함됩니다. Macie가 CloudWatch Logs에 게시하는 작업 이벤트의 자세한 목록은 작업의 로그 이벤트 유형 단원을 참조하세요.

다음 예에서는 민감한 데이터 검색 작업에 대한 로그 이벤트 스키마를 보여줍니다. 이 예제에서 이벤트는 Amazon S3가 버킷에 대한 액세스를 거부했기 때문에 Macie가 S3 버킷의 어떤 객체도 분석할 수 없었다고 보고합니다.

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:08:30.345809Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

이전 예제에서 Macie는 Amazon S3 API의 ListObjectsv2 작업을 사용하여 버킷의 객체를 나열하려고 했습니다. Macie가 Amazon S3에 요청을 보냈을 때 Amazon S3는 버킷에 대한 액세스를 거부했습니다.

다음 필드는 민감한 데이터 검색 작업의 모든 로그 이벤트에 공통적으로 사용됩니다.

- `adminAccountId` - 작업을 생성한 AWS 계정의 고유 식별자입니다.
- `jobId` – 작업의 고유 식별자입니다.
- `eventType` – 발생한 이벤트의 유형입니다. 가능한 값의 전체 목록과 각 값에 대한 설명은 작업의 로그 이벤트 유형 단원을 참조하세요.
- `occurredAt` - 이벤트 발생 날짜 및 시간(협정 세계시(UTC) 및 확장 ISO 8601 형식)입니다.
- `description` – 이벤트에 대한 간단한 설명입니다.
- `jobName` - 작업의 사용자 지정 이름입니다.

이벤트의 유형과 특성에 따라 로그 이벤트에는 다음 필드도 포함될 수 있습니다.

- `affectedAccount` - 영향을 받는 리소스를 소유한 사람의 AWS 계정에 대한 고유 식별자입니다.
- `affectedResource` - 영향을 받는 리소스에 대한 세부 정보를 제공하는 객체입니다. 객체에서 필드는 리소스에 대한 메타데이터를 저장하는 `type` 필드를 지정합니다. `value` 필드는 필드(`type`)의 값을 지정합니다.
- `operation` - Macie가 수행하려고 시도하여 오류를 일으킨 작업입니다.
- `runDate` - 적용 가능한 작업 또는 작업 실행이 시작된 날짜 및 시간(협정 세계시(UTC) 및 확장 ISO 8601 형식)입니다.

민감한 데이터 검색 작업에 대한 로그 이벤트 유형

Macie는 세 가지 범주의 이벤트에 대한 로그 이벤트를 게시합니다.

- 작업 상태 이벤트: 작업 또는 작업 실행의 상태 또는 진행 상황에 대한 변경 사항을 기록합니다.
- 계정 수준 오류 이벤트: Macie가 특정 AWS 계정에 대한 Amazon S3 데이터를 분석하지 못하게 하는 오류를 기록합니다.
- 버킷 수준 오류 이벤트: Macie가 특정 S3 버킷의 데이터를 분석하지 못하게 하는 오류를 기록합니다.

이 섹션의 항목에서는 Macie가 각 범주에 게시하는 이벤트 유형을 나열하고 설명합니다.

주제

작업 상태 이벤트

작업 상태 이벤트는 작업 또는 작업 실행의 상태 또는 진행 상황에 대한 변경 사항을 기록합니다. 정기 작업의 경우 Macie는 전체 작업과 개별 작업 실행 모두에 대해 이러한 이벤트를 기록하고 게시합니다. 작업의 전체 상태를 확인하는 방법에 대한 자세한 내용은 민감한 데이터 검색 작업의 상태 확인을(를) 참조하세요.

다음 예제에서는 샘플 데이터를 사용하여 작업 상태 이벤트의 필드 구조와 특성을 보여줍니다. 이 예제에서 SCHEDULED_RUN_COMPLETED 이벤트는 정기 작업의 예약된 실행이 완료되었음을 나타냅니다. runDate 필드에 표시된 대로 실행은 2021년 4월 14일 17:09:30 UTC에 시작되었습니다. occurredAt 필드에 표시된 대로 달리기는 2021년 4월 14일 17:16:30 UTC에 종료되었습니다.

```
{
    "adminAccountId": "123456789012",
    "jobId": "ffad0e71455f38a4c7c220f3cexample",
    "eventType": "SCHEDULED_RUN_COMPLETED",
    "occurredAt": "2021-04-14T17:16:30.574809Z",
    "description": "The scheduled job run finished running.",
    "jobName": "My_Daily_Macie_Job",
    "runDate": "2021-04-14T17:09:30.574809Z"
}
```

다음 표는 Macie가 기록하고 CloudWatch Logs에 게시하는 작업 상태 이벤트의 유형을 나열하고 설명합니다. 이벤트 유형 열에는 이벤트의 eventType 필드에 나타나는 각 이벤트의 이름이 표시됩니다. 설명 열은 이벤트 description 필드에 나타나는 이벤트에 대한 간략한 설명을 제공합니다. 추가 정보는 이벤트가 적용되는 작업 유형에 대한 정보를 제공합니다. 테이블은 먼저 이벤트가 발생할 수 있는 일반적인 연대순으로 정렬된 다음 이벤트 유형별 알파벳 오름차순으로 정렬됩니다.

이벤트 유형	설명	추가 정보
JOB_CREATED	작업이 생성되었습니다.	일회성 및 정기 작업에 적용됩니다.

이벤트 유형	설명	추가 정보
ONE_TIME_JOB_STARTED	작업이 실행되기 시작했습니다.	일회성 작업에만 적용됩니다.
SCHEDULED_RUN_STARTED	스케줄링된 작업 실행이 시작되었습니다.	정기 작업에만 적용됩니다. Macie는 일회성 작업의 시작을 기록하기 위해 이러한 유형의 이벤트가 아닌 ONE_TIME_JOB_STARTED 이벤트를 게시합니다.
BUCKET_MATCHED_THE_CRITERIA	영향을 받은 버킷이 작업에 지정된 버킷 기준과 일치했습니다.	런타임 버킷 기준을 사용하여 분석할 S3 버킷을 결정하는 일회성 및 주기적 작업에 적용됩니다. `affectedResource` 객체는 기준과 일치하고 작업 분석에 포함된 버킷의 이름을 지정합니다.
기준과 일치하는 버킷 수는 없습니다.	작업이 실행되기 시작했지만 현재 작업에 지정된 버킷 기준과 일치하는 버킷이 없습니다. 작업에서 데이터를 분석하지 않았습니다.	런타임 버킷 기준을 사용하여 분석할 S3 버킷을 결정하는 일회성 및 주기적 작업에 적용됩니다.
SCHEDULED_RUN_COMPLETED	예약된 작업 실행이 완료되었습니다.	정기 작업에만 적용됩니다. Macie는 일회성 작업의 완료를 기록하기 위해 이러한 유형의 이벤트가 아닌 JOB_COMPLETED 이벤트를 게시합니다.

이벤트 유형	설명	추가 정보
JOB_PAUSED_BY_USER	사용자가 작업을 일시 중지했습니다.	일시적으로 중지(일시 중지)한 일회성 및 정기 작업에 적용됩니다.
JOB_RESUMED_BY_USER	사용자가 작업을 재개했습니다.	일시적으로 중지(일시 중지)했다가 나중에 재개한 일회성 및 정기 작업에 적용됩니다.
JOB_PAUSED_BY_MACIE_SERVICE_QUOTA_MET	Macie가 작업을 일시 중지했습니다. 작업을 완료하면 해당 계정의 월 할당량을 초과할 수 있습니다.	Macie가 일시적으로 중지(일시 중지)한 일회성 및 정기 작업에 적용됩니다. Macie는 작업 또는 작업 실행으로 인한 추가 처리가 해당 작업에서 데이터를 분석하는 하나 이상의 계정에 대한 월간 민감한 데이터 검색 할당량을 초과할 경우 자동으로 작업을 일시 중지합니다. 이 문제를 방지하려면 영향을 받는 계정의 할당량을 늘리는 것이 좋습니다.

이벤트 유형	설명	추가 정보
JOB_RESUMED_BY_MACIE_SERVICE_QUOTA_LIFTED	Macie가 작업을 재개했습니다. 영향을 받은 계정의 월간 서비스 할당량이 해제되었습니다.	Macie가 일시적으로 중지(일시 중지)했다가 나중에 재개한 일회성 및 정기 작업에 적용됩니다. Macie가 일회성 작업을 자동으로 일시 중지한 경우, Macie는 다음 달이 시작되거나 영향을 받는 모든 계정에 대해 월별 민감한 데이터 검색 할당량이 늘어나는 시점(둘 중 먼저 발생하는 날짜)에 자동으로 작업을 재개합니다. Macie가 정기 작업을 자동으로 일시 중지한 경우 Macie는 다음 실행이 시작되거나 다음 달이 시작될 때(둘 중 먼저 발생하는 날짜) 작업을 자동으로 재개합니다.
JOB_CANCELLED	작업이 취소되었습니다.	영구적으로 중지(취소), 한 번 또는 일시 중지되었다가 30일 이내에 재개되지 않은 1회성 및 정기 작업에 적용됩니다. Macie를 일시 중지하거나 비활성화한 경우 이러한 유형의 이벤트는 Macie를 일시 중지하거나 비활성화했을 때 활성 상태였거나 일시 중지된 작업에도 적용됩니다. 해당 리전에서 Macie를 일시 중지하거나 비활성화하면 AWS 리전에서 Macie는 자동으로 작업을 취소합니다.

이벤트 유형	설명	추가 정보
JOB_COMPLETED	작업 실행이 완료되었습니다.	일회성 작업에만 적용됩니다. Macie는 정기 작업에 대한 작업 실행 완료를 기록하기 위해 이러한 유형의 이벤트가 아닌 SCHEDULED_RUN_COMPLETED 이벤트를 게시합니다.

계정 수준 오류 이벤트

계정 수준 오류 이벤트는 Macie가 특정 AWS 계정가 소유한 S3 버킷의 객체를 분석하지 못하게 하는 오류를 기록합니다. 각 이벤트의 `affectedAccount` 필드는 해당 계정의 계정 ID를 지정합니다.

다음 예시에서는 샘플 데이터를 사용하여 계정 수준 오류 이벤트의 필드 구조와 특성을 보여줍니다. 이 예제에서 `ACCOUNT_ACCESS_DENIED` 이벤트는 Macie가 계정 444455556666에서 소유한 S3 버킷의 객체를 분석할 수 없었음을 나타냅니다.

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "ACCOUNT_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:08:30.585709Z",
    "description": "Macie doesn’t have permission to access S3 bucket data for the
 affected account.",
    "jobName": "My_Macie_Job",
    "operation": "ListBuckets",
    "runDate": "2021-04-14T17:05:27.574809Z",
    "affectedAccount": "444455556666"
}
```

다음 표는 Macie가 기록하고 CloudWatch Logs에 게시하는 계정 수준 오류 이벤트의 유형을 나열하고 설명합니다. 이벤트 유형 열에는 이벤트의 `eventType` 필드에 나타나는 각 이벤트의 이름이 표시됩니다. 설명 열은 이벤트 `description` 필드에 나타나는 이벤트에 대한 간략한 설명을 제공합니다. 추가 정보 열에는 발생한 오류를 조사하거나 해결하는 데 필요한 모든 관련 팁이 제공됩니다. 테이블은 이벤트 유형별로 알파벳 오름차순으로 정렬됩니다.

이벤트 유형	설명	추가 정보
ACCOUNT_ACCESS_DENIED	Macie는 영향을 받는 계정의 S3 버킷 데이터에 액세스할 권한이 없습니다.	이는 일반적으로 해당 계정이 소유한 버킷에 제한적인 버킷 정책이 있기 때문에 발생합니다. 이 문제를 해결하는 방법에 대한 자세한 내용은 Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을(를) 참조하세요. 이벤트의 `operation` 필드 값은 어떤 권한 설정으로 인해 Macie가 계정의 S3 데이터에 액세스하지 못했는지 확인할 수 있습니다. 이 필드는 오류가 발생했을 때 Macie가 수행하려고 시도한 Amazon S3 작업을 나타냅니다.
ACCOUNT_DISABLED	작업이 영향을 받은 계정에서 소유한 리소스를 건너뛰었습니다. Macie는 계정에 사용할 수 없게 되었습니다.	이 문제를 해결하려면 같은 AWS 리전에서 해당 계정의 Macie를 다시 활성화하세요.
ACCOUNT_DISASSOCIATED	작업이 영향을 받은 계정에서 소유한 리소스를 건너뛰었습니다. 이 계정은 더 이상 Macie 관리자 계정과 멤버 계정으로 연결되지 않습니다.	이 문제는 조직의 Macie 관리자로서 관련 멤버 계정의 데이터를 분석하도록 작업을 구성한 후 해당 멤버 계정이 조직에서 제거되는 경우에 발생합니다. 이 문제를 해결하려면 영향을 받은 계정을 멤버 계정인 Macie 관리자 계정과 다시 연

이벤트 유형	설명	추가 정보
		결하세요. 자세한 내용은 여러 계정 관리 섹션을 참조하세요.
ACCOUNT_ISOLATED	작업이 영향을 받은 계정에서 소유한 리소스를 건너뛰었습니다. AWS 계정가 격리되었습니다.	–
ACCOUNT_REGION_DISABLED	작업이 영향을 받은 계정에서 소유한 리소스를 건너뛰었습니다. 현재 AWS 리전에서 AWS 계정가 활성화되어 있지 않습니다.	–
ACCOUNT_SUSPENDED	작업이 취소되었거나 영향을 받은 계정이 소유한 리소스를 건너뛰었습니다. Macie는 계정에 대해 일시 중지되었습니다.	지정한 계정이 본인 계정인 경우, 같은 리전에서 Macie를 일시 중지하면 Macie가 자동으로 작업을 취소한 것입니다. 문제를 해결하려면 해당 리전에서 Macie를 다시 활성화하세요. 지정된 계정이 멤버 계정인 경우 동일한 리전의 해당 계정에 대해 Macie를 다시 활성화하세요.
ACCOUNT_TERMINATED	작업이 영향을 받은 계정에서 소유한 리소스를 건너뛰었습니다. AWS 계정가 종료되었습니다.	–

버킷 수준 오류 이벤트

버킷 수준 오류 이벤트는 Macie가 특정 S3 버킷의 객체를 분석하지 못하게 하는 오류를 기록합니다. 각 이벤트의 `affectedAccount` 필드는 버킷을 소유한 AWS 계정의 계정 ID를 지정합니다. 각 이벤트의 `affectedResource` 객체는 버킷 이름을 지정합니다.

다음 예제에서는 샘플 데이터를 사용하여 버킷 수준 오류 이벤트의 필드 구조와 특성을 보여줍니다. 이 예제에서 `BUCKET_ACCESS_DENIED` 이벤트는 Macie가 `DOC-EXAMPLE-BUCKET`라는 S3 버킷의 어떤 객체도 분석할 수 없었음을 나타냅니다. Macie가 Amazon S3 API의 ListObjectsv2 작업을 사용하여 버킷의 객체를 나열하려고 시도했을 때 Amazon S3는 버킷에 대한 액세스를 거부했습니다.

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:09:30.685209Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

다음 표는 Macie가 기록하고 CloudWatch Logs에 게시하는 버킷 수준 오류 이벤트의 유형을 나열하고 설명합니다. 이벤트 유형 열에는 이벤트의 `eventType` 필드에 나타나는 각 이벤트의 이름이 표시됩니다. 설명 열은 이벤트 `description` 필드에 나타나는 이벤트에 대한 간략한 설명을 제공합니다. 추가 정보 열에는 발생한 오류를 조사하거나 해결하는 데 필요한 모든 관련 팁이 제공됩니다. 테이블은 이벤트 유형별로 알파벳 오름차순으로 정렬됩니다.

이벤트 유형	설명	추가 정보
BUCKET_ACCESS_DENIED	Macie는 영향을 받는 S3 버킷에 액세스할 수 있는 권한이 없습니다.	이는 일반적으로 버킷에 제한적인 버킷 정책이 있기 때문에 발생합니다. 이 문제를 해결하는 방법에 대한 자세한 내용은

이벤트 유형	설명	추가 정보
		Macie가 S3 버킷 및 객체에 액세스할 수 있도록 허용을(를) 참조하세요. 이벤트의 `operation` 필드 값은 어떤 권한 설정으로 인해 Macie가 버킷에 액세스하지 못했는지 확인할 수 있습니다. 이 필드는 오류가 발생했을 때 Macie가 수행하려고 시도한 Amazon S3 작업을 나타냅니다.
BUCKET_DETAILS_UNAVAILABLE	일시적인 문제로 인해 Macie가 버킷 및 버킷 객체에 대한 세부 정보를 검색하지 못했습니다.	이는 일시적인 문제로 인해 Macie가 버킷 객체를 분석하는 데 필요한 버킷 및 객체 메타데이터를 검색하지 못한 경우에 발생합니다. 예를 들어 Macie가 버킷에 액세스할 수 있는지 확인하려고 할 때 Amazon S3 예외가 발생했습니다. 일회성 작업의 문제를 해결하려면 버킷의 객체를 분석하기 위한 새로운 일회성 작업을 만들고 실행하는 것을 고려해 보세요. 예약된 작업의 경우 Macie는 다음 작업 실행 중에 메타데이터 검색을 다시 시도합니다.
BUCKET_DOES_NOT_EXIST	영향을 받은 S3 버킷은 더 이상 존재하지 않습니다.	이는 일반적으로 버킷이 삭제되었기 때문에 발생합니다.

이벤트 유형	설명	추가 정보
BUCKET_IN_DIFFERENT_REGION	영향을 받은 S3 버킷이 다른 AWS 리전으로 이동되었습니다.	–
BUCKET_OWNER_CHANGED	영향을 받은 S3 버킷의 소유자가 변경되었습니다. Macie는 더 이상 버킷에 액세스할 수 있는 권한이 없습니다.	이는 일반적으로 버킷 소유권이 조직의 일부가 아닌 AWS 계정로 이전된 경우에 발생합니다. 이벤트의 `affectedAccount` 필드는 이전에 버킷을 소유한 계정의 계정 ID를 나타냅니다.

민감한 데이터 검색 작업 관리

민감한 데이터 검색 작업을 관리할 수 있도록 Amazon Macie는 각 작업의 전체 인벤토리를 제공합니다. AWS 리전이 인벤토리를 사용하면, 작업을 단일 컬렉션으로 관리하고 개별 작업에 대한 구성 설정, 상태 및 처리 통계에 액세스할 수 있습니다. 또한 각 작업에서 생성된 민감한 데이터 조사 결과 및 기타 결과에 액세스할 수도 있습니다.

이러한 작업 외에도, 기존 작업을 복사하고, 복사본의 설정을 조정한 다음, 복사본을 새 작업으로 저장하는 등 개별 작업의 사용자 정의 변형본을 만들 수 있습니다. 이는 서로 다른 데이터 세트를 같은 방식으로 분석하거나, 같은 데이터 세트를 서로 다른 방식으로 분석하려는 경우에 유용할 수 있습니다. 또는 기존 작업을 취소하고, 해당 내용을 복사한 다음, 사본을 조정하여 새 작업으로 저장하는 등 기존 작업의 구성 설정을 조정하고 싶을 수도 있습니다.

주제

- 민감한 데이터 검색 작업의 인벤토리 검토
- 민감한 데이터 검색 작업에 대한 구성 설정 검토
- 민감한 데이터 검색 작업의 상태 확인
- 민감한 데이터 검색 작업 일시 중지, 재개 또는 취소
- 민감한 데이터 검색 작업 복사

민감한 데이터 검색 작업의 인벤토리 검토

Amazon Macie 콘솔의 작업 페이지는 현재 AWS 리전에서 계정의 모든 민감한 데이터 검색 작업에 대한 정보를 제공합니다. 각 작업의 경우, 테이블에는 작업의 현재 상태, 작업이 일정에 따라 주기적으로 실행되는지 여부, 작업이 특정 수의 S3 버킷을 분석하는지 또는 런타임 기준과 일치하는 S3 버킷을 분석하는지 여부를 포함하는 요약 정보가 표시됩니다. 테이블에서 작업을 선택하면, 세부 정보 패널에 구성 설정 및 작업에 대한 기타 정보가 표시됩니다.

작업 인벤토리를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다. 작업 페이지가 열리고, 여기에 인벤토리의 작업 수와 해당 작업의 테이블이 표시됩니다.
3. 특정 작업을 더 빨리 찾으려면 다음 작업 중 하나를 수행합니다.

   - 특정 필드를 기준으로 테이블을 정렬하려면 해당 필드의 열 제목을 선택합니다. 정렬 순서를 변경하려면 열 제목을 다시 선택합니다.
   - 필드에 대한 특정 값이 있는 해당 작업만 표시하려면, 필터 상자에 커서를 놓습니다. 나타나는 메뉴에서, 필터에 대해 사용할 필드를 선택하고, 필터에 대한 값을 입력합니다. 그런 다음, 적용을 선택합니다.
   - 필드에 대한 특정 값이 있는 작업을 숨기려면, 필터 상자에 커서를 놓습니다. 나타나는 메뉴에서, 필터에 대해 사용할 필드를 선택하고, 필터에 대한 값을 입력합니다. 그런 다음, 적용을 선택합니다. 필터 상자에서, 필터에 대한 등호 아이콘 (●) 을 선택합니다. 이렇게 하면 필터 연산자가 같음에서 같지 않음(⦸) 으로 변경됩니다.
   - 필터를 제거하려면, 제거할 필터에 대한 필터 제거 아이콘 (⊗) 을 선택합니다.
4. 특정 작업에 대한 구성 설정과 기타 세부 정보를 검토하려면, 테이블에서 작업의 이름을 선택한 다음, 세부 정보 패널을 참조합니다.

민감한 데이터 검색 작업에 대한 구성 설정 검토

Amazon Macie 콘솔에서는 작업 페이지의 세부 정보 패널을 사용하여 개별적인 민감한 데이터 검색 작업에 대한 구성 설정 및 기타 정보를 검토할 수 있습니다. 예를 들어, 작업이 분석하도록 구성된 S3 버킷 목록과 해당 버킷의 객체를 분석하기 위해 작업이 어떤 관리형 데이터 식별자를 사용하는지를 검토할 수 있습니다.

> **Note**
>
> 기존 작업에 대한 구성 설정은 변경할 수 없습니다. 이를 통해 수행하는 데이터 프라이버시 및 보호 감사 또는 조사에 대한 민감한 데이터 조사 결과 및 검색 결과에 대한 변경 불가능한 기록이 있는지 확인할 수 있습니다. 기존 작업을 변경하려면, 작업을 취소합니다. 그런 다음, 작업을 복사하고, 원하는 설정을 사용하도록 복사본을 구성한 다음, 복사본을 새 작업으로 저장합니다.
>
> 이렇게 할 경우, 새 작업이 기존 데이터를 같은 방식으로 다시 분석하지 않도록 하는 단계를 또한 거쳐야 합니다. 이렇게 하려면, 기존 작업을 취소하는 날짜 및 시간을 기록해 두십시오. 그런 다음, 원래 작업을 취소한 후에 생성되거나 변경되는 해당 객체만 포함하도록 새 작업의 범위를 구성합니다. 예를 들어, 객체 기준을 사용하여 원래 작업을 취소한 날짜 및 시간을 지정하는 마지막 수정 제외 조건을 추가합니다.

작업의 구성 설정을 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다.
3. 작업 페이지에서, 검토하려는 설정이 있는 작업의 이름을 선택합니다. 세부 정보 패널에 구성 설정 및 작업에 대한 기타 정보가 표시됩니다. 작업의 설정에 따라, 패널에는 다음 섹션이 포함됩니다.

   일반 정보

   이 섹션에서는 작업에 대한 일반 정보(예: 작업의 Amazon 리소스 이름(ARN)), 작업이 가장 최근에 실행되기 시작한 시점, 작업의 현재 상태를 제공합니다. 작업을 일시 중지한 경우, 이 섹션에는 작업을 일시 중지한 시점과 작업 또는 최근 작업 실행이 만료되었거나 이를 재개하지 않을 경우 해당 내용이 만료되는 시점도 표시됩니다.

통계

이 섹션에는 작업에 대한 처리 통계(예: 작업이 실행된 횟수 및 해당하는 현재 실행 중에 작업이 여전히 처리해야 하는 대략적인 객체 수)가 표시됩니다.

범위

이 섹션에는 작업이 얼마나 자주 실행되는지가 표시됩니다. 또한 이에는 작업 범위를 구체화하는 설정(예: 샘플링 깊이 및 작업 분석에 S3 객체를 포함시키거나 제외시키는 모든 객체 기준)이 표시됩니다.

S3 버킷

이 섹션은 작업을 생성할 때 명시적으로 선택한 버킷을 분석하도록 작업이 구성되어 있는 경우에 패널에 나타납니다. 이는 데이터를 분석하도록 구성된 작업의 AWS 계정 수를 나타냅니다. 또한 작업이 분석하도록 구성되어 있는 버킷 수와 해당 버킷의 이름(계정별로 그룹화되어 있음)을 나타냅니다.

계정 및 버킷의 전체 목록을 JSON 형식으로 표시하려면, 총 버킷 수 필드에서 숫자를 선택합니다.

S3 버킷 기준

이 섹션은 작업이 런타임 기준을 사용하여 어떤 버킷을 분석하지를 확인하는 경우에 패널에 나타납니다. 여기에는 작업이 사용하도록 구성되어 이있는 기준이 나열됩니다.

기준을 JSON 형식으로 표시하려면, 세부 정보를 선택한 다음, 나타나는 창에서 기준 탭을 선택합니다.

현재 기준과 일치하는 버킷 테이블을 검토하려면, 세부 정보를 선택한 다음, 나타나는 창에서 일치하는 버킷 탭을 선택합니다. 선택적으로, 새로 고침 ()을 선택하여 최신 데이터를 검색할 수 있습니다.

> **Tip**
>
> 작업이 이미 실행된 경우, 작업이 실행되었을 때 버킷이 기준과 일치했는지 여부와 일치하는 경우 해당 버킷의 이름을 확인할 수도 있습니다. 이렇게 하려면 작업의 로그 이벤트를 검토하십시오. 패널 상단에 결과 표시를 선택한 다음 CloudWatch 로그 표시를 선택합니다. Macie는 Amazon CloudWatch 콘솔을 열고 작업에 대한 로그 이벤트 테이블을 표시합니다. 이벤트에는 기준과 일치하고 작업 분석에 포함되었던 각 버킷의

BUCKET_MATCHED_THE_CRITERIA 이벤트가 포함됩니다. 자세한 내용은 작업 모니터링 섹션을 참조하세요.

사용자 지정 데이터 식별자

이 섹션은 작업이 하나 이상의 사용자 지정 데이터 식별자를 사용하도록 구성되어 있는 경우 패널에 나타납니다. 이것은 해당 사용자 지정 데이터 식별자의 이름을 지정합니다.

허용 목록

이 섹션은 작업이 하나 이상의 허용 목록을 사용하도록 구성되어 있는 경우 패널에 나타납니다. 이것은 해당 목록의 이름을 지정합니다. 목록의 설정과 상태를 검토하려면, 목록 이름 옆에 있는 링크 아이콘 ( ) 을 선택합니다.

관리형 데이터 식별자

이 섹션에는 어떤 관리형 데이터 식별자를 작업이 사용하도록 구성되어 있는지 표시됩니다. 이는 작업의 관리형 데이터 식별자 선택 유형에 따라 결정됩니다.

- 권장 - 작업 실행 시 권장 세트에 있는 관리형 데이터 식별자를 사용합니다.
- 선택 항목 포함 - 선택 사항 섹션에 나열된 관리형 데이터 식별자만 사용합니다.
- 모두 포함 - 작업 실행 시 사용할 수 있는 모든 관리형 데이터 식별자를 사용합니다.
- 선택 항목 제외 - 선택 사항 섹션에 나열된 내용을 제외하고 작업 실행 시 사용할 수 있는 모든 관리형 데이터 식별자를 사용합니다.
- 모두 제외 - 어떠한 관리형 데이터 식별자도 사용하지 않습니다. 지정된 사용자 지정 데이터 식별자만 사용합니다.

이러한 설정을 JSON 형식으로 검토하려면, 세부 정보를 선택합니다.

태그

이 섹션은 태그가 작업과 연결된 경우 패널에 나타납니다. 이것은 해당 태그를 나열합니다.

태그는 사용자가 정의하여 특정 유형의 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별, 분류, 관리하는 데 도움이 됩니다. 자세한 내용은 Amazon Macie에 리소스 태그 지정(을)를 참조하세요.

4. 작업 설정을 JSON 형식으로 검토하고 저장하려면, 패널 상단에서 작업의 고유 식별자(작업 ID)를 선택한 다음, 다운로드를 선택합니다.

민감한 데이터 검색 작업의 상태 확인

민감한 데이터 검색 작업을 만드는 경우, 작업의 유형과 일정에 따라 초기 상태는 활성(실행 중) 또는 활성(유휴)입니다. 그런 다음, 작업은 추가 상태를 거치며, 이를 통해 사용자는 작업이 진행됨에 따라 이 상태를 모니터링할 수 있습니다.

> **Tip**
>
> 작업의 전체 상태를 모니터링하는 것 외에도 작업이 진행되면서 발생하는 특정 이벤트를 모니터링할 수 있습니다. Macie가 Amazon CloudWatch Logs에 자동으로 게시하는 로깅 데이터를 사용하여 이 작업을 수행할 수 있습니다. 이러한 로그의 데이터는 작업 상태의 변경 기록과 작업 실행 중에 발생하는 계정 또는 버킷 수준 오류에 대한 세부 정보를 제공합니다. 자세한 내용은 작업 모니터링 섹션을 참조하세요.

작업의 상태를 확인하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다.
3. 작업 페이지에서 확인하려는 상태가 있는 작업을 찾습니다. 상태 필드는 작업의 현재 상태를 나타냅니다.

   활성(유휴)

   정기 작업의 경우, 이전 실행이 완료되고 다음 예약된 실행은 보류 중입니다. 이 값은 일회성 작업에는 적용되지 않습니다.

   활성(실행 중)

   일회성 작업의 경우, 작업이 현재 진행 중입니다. 정기 작업의 경우, 예약된 실행이 진행 중입니다.

   취소됨

   모든 유형의 작업의 경우, 작업이 영구적으로 중지(취소)되었습니다.

명시적으로 해당 작업을 취소한 경우 또는 해당 작업이 일회성 작업일 때 작업을 일시 중지하고 30일 이내에 이를 재개하지 않은 경우, 작업은 이 상태가 됩니다. 현재 AWS 리전에서 Macie를 일시 중단한 경우에도 작업이 이 상태가 될 수 있습니다.

완료

일회성 작업의 경우, 작업이 성공적으로 실행되어 이제 완료되었습니다. 이 값은 정기 작업에는 적용되지 않습니다. 대신 각 실행이 성공적으로 완료되면 정기 작업의 상태가 활성(유휴)으로 변경됩니다.

Macie에 의해 일시 중지됨

Macie는 모든 유형의 작업에 대해 작업을 일시적으로 중지(일시 중지)했습니다.

작업 완료 또는 작업 실행이 사용자 계정의 월간 민감한 데이터 검색 할당량을 초과할 경우 작업은 이 상태가 됩니다. 이러한 상황이 발생할 때, Macie는 자동으로 작업을 일시 중지합니다. Macie는 다음 달이 시작되거나 계정에 대한 월별 할당량이 재설정되거나 사용자가 계정 할당량을 늘리면 자동으로 작업을 재개합니다.

조직의 Macie 관리자로서 멤버 계정의 데이터를 분석하도록 작업을 구성한 경우, 작업 완료 또는 작업 실행이 멤버 계정의 월간 민감한 데이터 검색 할당량을 초과할 경우에도 작업이 이 상태가 될 수 있습니다.

작업이 실행 중이고 적합한 객체에 대한 분석 결과가 멤버 계정에 대한 이 할당량에 도달하면 작업은 해당 계정이 소유한 객체에 대한 분석을 중단합니다. 할당량을 충족하지 못한 다른 모든 계정의 객체 분석 작업이 완료되면 Macie는 자동으로 작업을 일시 중지합니다. 일회성 작업인 경우 Macie는 다음 달이 시작되거나 영향을 받는 모든 계정의 할당량이 늘어나는 시점(둘 중 먼저 발생하는 날짜)에 자동으로 작업을 재개합니다. 정기 작업인 경우 Macie는 다음 실행이 시작되거나 다음 달이 시작될 때(둘 중 먼저 발생하는 날짜) 작업을 자동으로 재개합니다. 다음 달이 시작되기 전에 예약된 실행이 시작되거나 영향을 받는 계정의 할당량이 증가하면 작업은 해당 계정이 소유한 객체를 분석하지 않습니다.

사용자에 의해 일시 중지됨

모든 유형의 작업에 대해 사용자가 작업을 일시적으로 중지(일시 중지)했습니다.

일회성 작업을 일시 중지하고 30일 이내에 이를 재개하지 않으면 작업이 만료되고 Macie는 작업을 취소합니다. 정기 작업이 현재 실행 중일 때 이를 일시 중지하고 30일 이내에 재개하지 않으면 작업 실행이 만료되고 Macie는 실행을 취소합니다. 일시 중지된 작업 또는 작업 실행의 만료 날짜를 확인하려면 테이블에서 작업 이름을 선택한 다음, 세부 정보 패널의 상태 세부 정보 섹션에서 만료 필드를 참조합니다.

작업이 취소되거나 일시 중지된 경우 작업 세부 정보를 참조하여 작업이 실행되기 시작했는지 아니면 정기 작업의 경우 취소되거나 일시 중지되기 전에 한 번 이상 실행되었는지 확인할 수 있습니다. 이 작업을 수행하려면 테이블에서 작업의 이름을 선택한 다음, 세부 정보 패널을 참조합니다. 패널의 실행 횟수 필드는 작업이 실행된 횟수를 나타냅니다. 마지막 실행 시간 필드는 작업이 실행되기 시작한 가장 최근 날짜 및 시간을 나타냅니다.

작업의 현재 상태에 따라 선택적으로 작업을 일시 중지, 재개 또는 취소할 수 있습니다.

민감한 데이터 검색 작업 일시 중지, 재개 또는 취소

민감한 데이터 검색 작업을 만든 후에는 작업을 일시적으로 일시 중지하거나 영구적으로 취소할 수 있습니다. 현재 실행 중인 작업을 일시 중지하면 Macie는 즉시 해당 작업에 대한 모든 처리 작업을 일시 중지하기 시작합니다. 현재 실행 중인 작업을 취소하면 Macie는 즉시 해당 작업에 대한 모든 처리 작업을 중지하기 시작합니다. 작업이 취소된 후에는 작업을 재개하거나 다시 시작할 수 없습니다.

일회성 작업을 일시 중지한 경우, 30일 이내에 이를 재개할 수 있습니다. 작업을 재개하면 Macie는 작업을 일시 중지한 시점부터 즉시 처리를 재개합니다. Macie는 작업을 처음부터 다시 시작하지 않습니다. 일회성 작업을 일시 중지한 후 30일 이내에 이를 재개하지 않으면 작업이 만료되고 Macie는 작업을 취소합니다.

정기 작업을 일시 중지하면 언제든지 이를 재개할 수 있습니다. 정기 작업을 재개하고 일시 중지했을 때 작업이 유휴 상태였던 경우, Macie는 작업을 만들 때 선택한 일정 및 기타 구성 설정에 따라 작업을 재개합니다. 정기 작업을 재개하고 일시 중지했을 때 작업이 활발하게 실행 중이었던 경우, Macie가 작업을 재개하는 방법은 작업을 재개한 시점에 따라 달라집니다.

- 작업을 일시 중지한 후 30일 이내에 재개하면, Macie는 작업을 일시 중지한 시점부터 가장 최근에 예약된 실행을 즉시 재개합니다. Macie는 실행을 처음부터 다시 시작하지 않습니다.
- 일시 중지한 후 30일 이내에 작업을 재개하지 않으면, 예약된 최신 실행이 만료되고 Macie는 해당 실행의 나머지 처리 작업을 모두 취소합니다. 이후에 작업을 재개하면, Macie는 작업을 만들 때 선택한 일정 및 기타 구성 설정에 따라 작업을 재개합니다.

일시 중지된 작업 또는 작업 실행이 만료되는 시점을 결정하는 데 도움이 되도록, Macie는 작업이 일시 중지된 동안 작업 세부 정보에 만료 날짜를 추가합니다. 이 날짜를 확인하려면, 작업 페이지의 테이블에서 작업 이름을 선택한 다음, 세부 정보 패널의 상태 세부 정보 섹션에서 만료 필드를 참조하세요. 또한, 작업 또는 작업 실행이 만료되기 약 7일 전에 알림을 보내드립니다. 작업 또는 작업 실행이 만료되어 취소되면 다시 알려드립니다. 이를 알리기 위해 당사는 AWS 계정에 연결된 주소로 이메일을 보내드립니다. 또한 계정에 대한 AWS Health 이벤트와 Amazon CloudWatch 이벤트를 생성합니다.

작업을 일시 중지, 재개 또는 취소하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다.
3. 작업 페이지에서 일시 중지, 재개 또는 취소할 작업의 확인란을 선택한 후 작업 메뉴에서 다음 중 하나를 수행합니다.

   - 작업을 일시적으로 중지하려면 일시 중지를 선택합니다. 이 옵션은 작업의 현재 상태가 활성(유휴), 활성(실행 중) 또는 Macie에 의해 일시 중지됨인 경우에만 사용할 수 있습니다.
   - 작업을 재개하려면 재개를 선택합니다. 이 옵션은 작업의 현재 상태가 사용자에 의해 일시 중지됨인 경우에만 사용할 수 있습니다.
   - 작업을 영구적으로 취소하려면 취소를 선택합니다. 이 옵션을 선택하면 이후에 작업을 재개하거나 다시 시작할 수 없습니다.

민감한 데이터 검색 작업 복사

기존 작업과 유사한 새로운 민감한 데이터 검색 작업을 빠르게 만들려면 작업의 복사본을 만들고, 복사본 설정을 편집한 다음, 복사본을 새 작업으로 저장하면 됩니다. 이는 기존 작업의 사용자 정의 변형본을 만들려는 경우에 유용할 수 있습니다. 또는 작업을 취소한 다음, 설정을 새 작업으로 복사, 변경 및 저장하여 기존 작업의 구성 설정을 조정하려는 경우도 있습니다.

작업을 복사하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서, 작업을 선택합니다.
3. 복사할 작업에 대한 확인란을 선택합니다.
4. 작업 메뉴에서 새로 복사를 선택합니다.
5. 콘솔에서 단계를 완료하여 작업 복사본에 대한 설정을 검토하고 조정합니다. 범위 구체화 단계의 경우, 작업에서 기존 데이터를 같은 방식으로 다시 분석하지 못하도록 하는 옵션을 선택하는 것을 고려합니다.

   - 일회성 작업의 경우, 특정 시간 이후에 생성되거나 변경된 객체만 포함하도록 객체 기준을 사용합니다. 예를 들어, 취소한 작업의 복사본을 만드는 경우 기존 작업을 취소한 날짜와 시간을 지정하는 마지막 수정 조건을 추가합니다.
   - 정기 작업의 경우, 기존 객체 포함 확인란의 선택을 취소합니다. 이렇게 할 경우, 작업의 첫 번째 실행은 작업을 생성한 후에 그리고 작업의 첫 번째 실행 전에 생성되거나 변경되는 해당 객체만

분석합니다. 또한 객체 기준을 사용하여 특정 날짜 및 시간 이전에 마지막으로 수정된 객체를 제외할 수도 있습니다.

이 단계 및 기타 단계에 대한 추가 세부 정보는 민감한 데이터 검색 작업 생성을(를) 참조하세요.

6. 작업을 마치면 제출을 선택하여 사본을 새 작업으로 저장합니다.

민감한 데이터 검색 작업의 비용 예측 및 모니터링

Amazon Macie 요금은 민감한 데이터 검색 작업을 실행하여 분석하는 데이터의 양을 부분적으로 기준으로 합니다. 민감한 데이터 검색 작업을 실행하는 데 드는 예상 비용을 예측하고 모니터링하려면 작업을 생성할 때와 작업 실행을 시작한 후에 Macie가 제공하는 예상 비용을 검토할 수 있습니다.

AWS Billing and Cost Management을(를) 사용하여 실제 비용을 검토하고 모니터링할 수 있습니다. AWS Billing and Cost Management은(는) 사용자의 AWS 서비스에 대한 비용을 추적 및 분석하고 계정 또는 조직의 예산을 관리하는 데 도움이 되도록 설계된 기능을 제공합니다. 또한 과거 데이터를 기반으로 사용자가 사용 비용을 예측하는 데 도움이 되는 기능을 제공합니다. 자세한 내용은 AWS Billing 사용 설명서를 참조하세요.

Macie 요금에 대한 자세한 내용은 Amazon Macie 요금을 참조하세요.

주제

- 민감한 데이터 검색 작업의 비용 예측
- 민감한 데이터 검색 작업의 예상 비용 모니터링

민감한 데이터 검색 작업의 비용 예측

민감한 데이터 검색 작업을 생성하면 Amazon Macie는 작업 생성 프로세스의 두 가지 주요 단계, 즉 작업에 대해 선택한 S3 버킷 테이블을 검토하는 단계(2단계)와 작업에 대한 모든 설정을 검토하는 단계(8단계)에서 예상 비용을 계산하여 표시할 수 있습니다. 이러한 추정치는 작업을 저장하기 전에 작업 설정을 조정할지 여부를 결정하는 데 도움이 될 수 있습니다. 예상치의 사용 가능 여부 및 특성은 작업에 대해 선택한 설정에 따라 달라집니다.

개별 버킷의 예상 비용 검토(2단계)

분석할 작업의 개별 버킷을 명시적으로 선택하면 각 버킷의 객체 분석 예상 비용을 검토할 수 있습니다. Macie는 작업 생성 프로세스의 2단계에서 버킷 선택을 검토할 때 이러한 추정치를 표시합니

다. 이 단계의 표에서 추정 비용 필드는 S3 버킷에 있는 객체를 분석하기 위해 작업을 한 번 실행한 총 예상 비용(미국 달러)을 나타냅니다.

각 추정치는 현재 버킷에 저장된 객체의 크기 및 유형을 기반으로 작업이 버킷에서 분석할 압축되지 않은 데이터의 예상 양을 반영합니다. 이 추정치에는 현재 AWS 리전에 대한 Macie의 요금도 반영됩니다.

분류 가능한 객체만 버킷 예상 비용에 포함됩니다. 분류 가능한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식의 파일 이름 확장자를 갖는 S3 객체입니다. 분류 가능한 객체를 압축하거나 파일을 보관하는 경우, 추정치에서는 파일이 3:1 의 압축률을 사용하며 작업에서 추출된 모든 파일을 분석할 수 있다고 가정합니다.

작업의 총 예상 비용 검토(8단계)

일회성 작업을 생성하거나 기존 S3 객체를 포함하도록 주기적 작업을 생성하고 구성하는 경우, Macie는 작업 생성 프로세스의 마지막 단계에서 작업의 총 예상 비용을 계산하여 표시합니다. 작업에 대해 선택한 모든 설정을 검토 및 확인하면서 이 예상치를 검토할 수 있습니다.

이 예상치는 현재 리전에서 작업을 한 번 실행하는 데 대한 총 예상 비용(미국 달러)을 나타냅니다. 추정치는 작업이 분석할 압축되지 않은 데이터의 예상 양을 반영합니다. 작업 설정에 따라 작업을 위해 명시적으로 선택한 버킷에 현재 저장되어 있는 객체의 크기 및 유형 또는 작업에 지정된 버킷 기준과 현재 일치하는 최대 500개의 버킷을 기준으로 합니다.

참고로 이 추정치에는 작업 범위를 좁히고 축소하기 위해 선택한 옵션(예: 더 낮은 샘플링 깊이 또는 특정 S3 객체를 작업에서 제외하는 기준)이 반영되지 않습니다. 또한 월별 민감한 데이터 검색 할당량(작업 분석의 범위와 비용이 제한될 수 있음)이나 계정에 적용될 수 있는 할인도 반영되지 않습니다.

예상 총 작업 비용 외에도 예상 작업 범위와 비용을 파악할 수 있는 집계 데이터가 제공됩니다.

- 크기 값은 작업에서 분석할 수 있는 개체와 분석할 수 없는 개체의 총 스토리지 크기를 나타냅니다.
- 객체 수 값은 작업에서 분석할 수 있는 개체와 분석할 수 없는 객체의 총 개수를 나타냅니다.

이러한 값에서 분류 가능한 객체는 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 파일 또는 스토리지 형식의 파일 이름 확장자를 갖는 S3 객체입니다. 분류 가능한 객체만 예상 비용에 포함됩니다. 분류할 수 없는 객체란 지원되는 스토리지 클래스를 사용하지 않거나 지원되는 파일 또는 스토리지 형식에 대한 파일 이름 확장자가 없는 객체를 말합니다. 이러한 객체는 예상 비용에 포함되지 않습니다.

이 추정치는 압축 또는 아카이브 파일인 S3 객체에 대한 추가 집계 데이터를 제공합니다. 압축 값은 지원되는 Amazon S3 스토리지 클래스를 사용하고 지원되는 유형의 압축 또는 아카이브 파일에 대

한 파일 이름 확장자를 갖는 객체의 총 스토리지 크기를 나타냅니다. 압축되지 않은 값은 지정된 압축률에 따라 이러한 객체를 압축 해제할 경우의 대략적인 크기를 나타냅니다. 이 데이터는 Macie가 압축 파일 및 아카이브 파일을 분석하는 방식 때문에 관련이 있습니다.

Macie가 압축 또는 아카이브 파일을 분석할 때 전체 파일과 파일의 내용을 모두 검사합니다. 파일 내용을 검사하기 위해 Macie는 파일의 압축을 푼 다음 지원되는 형식을 사용하는 추출된 각 파일을 검사합니다. 따라서 작업에서 분석하는 실제 데이터 양은 다음에 따라 달라집니다.

- 파일이 압축을 사용하는지 여부 및 사용하는 경우, 사용하는 압축 비율입니다.
- 추출된 파일의 수, 크기 및 형식

기본적으로 Macie는 작업에 대한 예상 비용을 계산할 때 다음을 가정합니다.

- 모든 압축 및 아카이브 파일은 3:1 압축률을 사용합니다.
- 추출된 모든 파일은 지원되는 파일 또는 스토리지 형식을 사용합니다.

이러한 가정을 통해 작업에서 분석할 데이터 범위의 예상 크기가 더 커질 수 있으며, 결과적으로 작업에 대한 예상 비용도 더 높아질 수 있습니다.

다른 압축률을 기준으로 작업의 총 예상 비용을 다시 계산할 수 있습니다. 이렇게 하려면 예상 비용 섹션의 예상 압축률 선택 목록에서 비율을 선택합니다. 그러면 Macie는 선택과 일치하도록 예상치를 업데이트합니다.

Macie의 추정 비용 계산 방식에 대한 자세한 정보는 예상 사용 비용 계산 방법의 이해의 내용을 참조하세요.

민감한 데이터 검색 작업의 예상 비용 모니터링

민감한 데이터 검색 작업을 이미 실행 중인 경우, Amazon Macie 콘솔의 사용량 페이지를 통해 해당 작업의 예상 비용을 모니터링할 수 있습니다. 이 페이지에서는 이번 달 현재 AWS 리전에서 Macie 이벤트 비용에 대한 예상 비용 (미국 달러) 을 표시합니다. Macie의 이러한 추정치 계산 방식에 대한 정보는 예상 사용 비용 계산 방법의 이해의 내용을 참조하세요.

작업 실행에 드는 예상 비용을 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 추정 비용을 검토하려는 리전을 선택합니다.
3. 탐색 창에서 사용량을 선택합니다.
4. 사용량 페이지에서 계정의 예상 비용 내역을 참조하세요. 민감한 데이터 검색 작업 항목은 이번 달 현재 리전에서 지금까지 실행한 작업의 총 예상 비용을 보고합니다.

사용자가 조직의 Macie 관리자인 경우, 예상 비용 섹션에는 현재 리전의 이번 달에 대한 조직 전체의 예상 비용이 표시됩니다. 특정 계정에서 실행된 작업의 총 예상 비용을 표시하려면 표에서 해당 계정을 선택합니다. 그러면 예상 비용 섹션에는 실행된 작업의 예상 비용을 포함하여 계정의 예상 비용 내역이 표시됩니다. 다른 계정의 이 데이터를 표시하려면 표에서 계정을 선택하세요. 선택을 지우려면, 계정 ID 옆에 있는 X를 선택합니다.

실제 비용을 검토하고 모니터링하려면 AWS Billing and Cost Management를 사용합니다.

민감한 데이터 검색 작업에 권장되는 관리형 데이터 식별자

민감한 데이터 검색 작업의 결과를 최적화하기 위해 작업에 권장되는 관리형 데이터 식별자 세트를 자동으로 사용하도록 개별 작업을 구성할 수 있습니다. 각 관리형 데이터 식별자는 신용카드 번호, AWS 보안 액세스 키 또는 특정 국가 또는 지역의 여권 번호와 같은 특정 유형의 민감한 데이터를 를 탐지하도록 설계된 일련의 기본 기준 및 기술입니다.

권장되는 관리형 데이터 식별자 세트는 민감한 데이터의 일반적인 범주 및 유형을 탐지하도록 설계되었습니다. 연구 결과에 따르면 민감한 데이터의 일반적인 범주와 유형을 감지하는 동시에 노이즈를 줄여 작업 결과를 최적화할 수 있습니다. 새로운 관리형 데이터 식별자를 출시하면서 작업 결과를 더욱 최적화할 가능성이 있는 경우 이 세트에 추가합니다. 시간이 지나면서 세트에 기존 관리형 데이터 식별자를 추가하거나 제거할 수도 있습니다. 권장 세트에서 관리형 데이터 식별자를 추가하거나 제거하면 이 페이지를 업데이트하여 변경 사항의 특성과 시점을 표시합니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Macie 문서 기록 페이지에서 RSS 피드를 구독하세요.

민감한 데이터 검색 작업을 생성할 때는 Amazon Simple Storage Service(S3) 버킷의 객체를 분석하는데 작업에서 사용할 관리형 데이터 식별자를 지정합니다. 권장되는 관리형 데이터 식별자 세트를 사용하도록 작업을 구성하려면 작업을 생성할 때 권장 옵션을 선택하세요. 그러면 작업이 실행되기 시작할 때 권장 세트에 있는 모든 관리형 데이터 식별자가 자동으로 사용됩니다. 작업을 두 번 이상 실행하도록 구성한 경우 각 실행은 실행 시작 시 권장 세트에 있는 모든 관리형 데이터 식별자를 자동으로 사용합니다.

다음 항목에서는 현재 권장 세트에 있는 관리형 데이터 식별자를 민감한 데이터 범주 및 유형별로 정리하여 나열합니다. 세트의 각 관리형 데이터 식별자에 대해 고유 식별자(ID)를 지정합니다. 이 ID는 관리형 데이터 식별자가 감지하도록 설계된 민감한 데이터의 유형을 설명합니다(예: PGP 개인 키는 `PGP_PRIVATE_KEY`. 미국 여권 번호는 `USA_PASSPORT_NUMBER`).

주제

- 보안 인증

- 금융 정보
- 개인 식별 정보(PII)
- 권장 세트에 대한 업데이트

특정 관리형 데이터 식별자 또는 Macie가 현재 제공하는 모든 관리형 데이터 식별자의 전체 목록에 대한 자세한 내용은 관리형 데이터 식별자 사용 섹션을 참조하세요.

보안 인증

S3 객체에서 자격 증명 데이터의 발생을 탐지하기 위해 권장 세트는 다음과 같은 관리형 데이터 식별자를 사용합니다.

민감한 데이터 유형	관리형 데이터 식별자 ID
AWS 비밀 액세스 키	`AWS_CREDENTIALS`
HTTP Basic Authorization 헤더	`HTTP_BASIC_AUTH_HEADER`
OpenSSH 프라이빗 키	`OPENSSH_PRIVATE_KEY`
PGP 프라이빗 키	`PGP_PRIVATE_KEY`
퍼블릭 키 암호화 표준(PKCS) 프라이빗 키	`PKCS`
PuTTY 프라이빗 키	`PUTTY_PRIVATE_KEY`

금융 정보

S3 객체에서 발생하는 금융 정보를 탐지하기 위해 권장 세트는 다음과 같은 관리형 데이터 식별자를 사용합니다.

민감한 데이터 유형	관리형 데이터 식별자 ID
신용 카드 마그네틱 스트립 데이터	`CREDIT_CARD_MAGNETIC_STRIPE`
신용 카드 번호	`CREDIT_CARD_NUMBER` (키워드 근처에 있는 신용 카드 번호의 경우)

개인 식별 정보(PII)

S3 객체에서 프라이빗 식별 정보(PII) 발생을 탐지하기 위해 권장 세트는 다음과 같은 관리형 데이터 식별자를 사용합니다.

민감한 데이터 유형	관리형 데이터 식별자 ID
운전면허증 식별 번호	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (미국의 경우), UK_DRIVERS_LICENSE
선거인단 번호	UK_ELECTORAL_ROLL_NUMBER
국적 식별 번호	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
National Insurance Number(NINO)	UK_NATIONAL_INSURANCE_NUMBER
여권 번호	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Social Insurance Number(SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
사회 보장 번호	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
납세자 식별 번호 또는 참조 번호	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX

민감한 데이터 유형	관리형 데이터 식별자 ID
	`_IDENTIFICATION_NUMBER`, `USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`

권장 세트에 대한 업데이트

다음 테이블에는 민감한 데이터 검색 작업에 권장되는 관리형 데이터 식별자 세트의 변경 사항이 설명되어 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
정식 출시	권장 세트의 최초 릴리스.	2023년 6월 27일

Amazon Macie를 사용한 암호화된 Amazon S3 객체 분석

Amazon Macie를 활성화하면 Macie는 사용자를 대신하여 AWS 계정 Amazon Simple Storage Service (Amazon S3) 및 기타 서비스를 호출하는 데 필요한 권한을 Macie에게 부여하는 서비스 연결 역할을 생성합니다. AWS 서비스 서비스 연결 역할을 사용하면 사용자 대신 작업을 완료하기 위해 서비스에 권한을 수동으로 추가할 필요가 AWS 서비스 없으므로 설정 프로세스가 간소화됩니다. 이러한 유형의 역할에 대해 자세히 알아보려면 AWS Identity and Access Management 사용 설명서의 서비스 연결 역할 사용을 참조하세요.

Macie 서비스 연결 역할(`AWSServiceRoleForAmazonMacie`)에 대한 권한 정책을 통해 Macie는 S3 버킷 및 객체에 대한 정보 검색, S3 버킷의 객체 검색 및 분석 등의 작업을 수행할 수 있습니다. 사용자 계정이 조직의 Macie Administrator 계정인 경우, 그 정책을 사용하면 Macie가 사용자를 대신하여 조직의 구성원 계정에 대해 이러한 작업을 수행할 수도 있습니다.

S3 객체가 암호화된 경우, Macie 서비스 연결 역할의 권한 정책은 일반적으로 Macie에게 객체 암호 해독에 필요한 권한을 부여하는 것입니다. 하지만, 이는 사용된 암호화 유형에 따라 달라질 수 있습니다. 또한 Macie가 적절한 암호화 키를 사용할 수 있는지 여부에 따라서도 달라질 수 있습니다.

주제

- Amazon S3 객체의 암호화 옵션

- Amazon Macie가 고객 관리형 앱을 사용할 수 있도록 허용 AWS KMS key

Amazon S3 객체의 암호화 옵션

Amazon S3는 S3 객체에 대한 여러 암호화 옵션을 지원합니다. 이러한 옵션 대부분에서 Amazon Macie는 계정의 Macie 서비스 연결 역할을 사용하여 객체를 복호화할 수 있습니다. 하지만, 이는 객체를 암호화하는 데 사용된 암호화 유형에 따라 달라질 수 있습니다.

Amazon S3 관리형 키를 사용한 서버 측 암호화(SSE-S3)

Amazon S3 관리 키 (SSE-S3) 를 사용한 서버 측 암호화를 사용하여 객체를 암호화하는 경우 Macie는 객체를 해독할 수 있습니다.

이 암호화 유형에 대해 자세히 알아보려면 Amazon Simple Storage Service 사용 설명서의 Amazon S3 관리형 키를 사용하여 서버 측 암호화 사용을 참조하세요.

(DSSE-KMS 및 SSE-KMS) 를 사용한 서버 측 암호화 AWS KMS keys

이중 레이어 서버측 암호화 또는 관리형 (DSSE-KMS 또는 SSE-KMS) 을 사용한 서버측 암호화를 사용하여 객체를 암호화하는 경우 Macie는 객체를 해독할 수 있습니다. AWS AWS KMS key

고객이 관리하는 서버 측 암호화 또는 서버 측 암호화 AWS KMS key (DSSE-KMS 또는 SSE-KMS) 를 사용하여 객체를 암호화하는 경우 Macie가 키를 사용하도록 허용한 경우에만 Macie가 객체의 암호를 해독할 수 있습니다. 이는 전적으로 KMS 키 내에서 관리되는 KMS 키와 외부 키 저장소의 KMS 키로 암호화된 객체의 경우입니다. AWS KMS Macie가 해당 KMS 키를 사용할 수 없는 경우 Macie는 객체에 대한 메타데이터만 저장하고 보고할 수 있습니다.

이러한 유형의 암호화에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서의 이중 레이어 서버 측 암호화 사용 AWS KMS keys및 서버 측 암호화 사용을 참조하십시오. AWS KMS keys

> **Tip**
>
> Macie가 사용자 계정의 S3 버킷에 있는 객체를 분석하기 위해 액세스해야 AWS KMS keys 하는 모든 고객 관리 항목의 목록을 자동으로 생성할 수 있습니다. 이렇게 하려면 Amazon Macie Scripts 리포지토리에서 사용할 수 있는 AWS KMS 권한 분석기 스크립트를 실행하십시오. GitHub 스크립트는 AWS Command Line Interface (AWS CLI) 명령의 추가 스크립트를 생성할 수도 있습니다. 선택적으로 이러한 명령을 실행하여 지정한 KMS 키의 필수 구성 설정 및 정책을 업데이트할 수 있습니다.

고객 제공 키를 사용한 서버 측 암호화(SSE-C)

고객 제공 키 (SSE-C) 를 사용한 서버 측 암호화를 사용하여 개체를 암호화하는 경우 Macie는 개체를 해독할 수 없습니다. Macie는 객체에 대한 메타데이터만 저장하고 보고할 수 있습니다.

이러한 유형의 암호화에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서의 고객 제공 키를 사용한 서버 측 암호화 사용을 참조하세요.

클라이언트측 암호화

클라이언트측 암호화를 사용하여 객체가 암호화된 경우, Macie는 객체를 복호화할 수 없습니다. Macie는 객체에 대한 메타데이터만 저장하고 보고할 수 있습니다. 예를 들어, Macie는 객체의 크기 및 객체와 관련된 태그를 보고할 수 있습니다.

Amazon S3와 관련된 이러한 유형의 암호화에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서의 클라이언트 측 암호화를 사용하여 데이터 보호를 참조하세요.

Macie에서 버킷 인벤토리를 필터링하여 특정 유형의 암호화를 사용하는 객체를 저장하는 S3 버킷을 확인할 수 있습니다. 또한 새 객체를 저장할 때 어떤 버킷이 특정 유형의 서버 측 암호화를 기본적으로 사용하는지 결정할 수 있습니다. 다음 표에는 이 정보를 찾기 위해 버킷 인벤토리에 적용할 수 있는 필터의 예가 나와 있습니다.

버킷을 표시하려면...	이 필터 적용...
SSE-C 암호화를 사용하는 객체 저장	암호화에 따른 객체 수는 고객이 제공한 값이며 From = 1
DSSE-KMS 또는 SSE-KMS 암호화를 사용하는 객체를 저장합니다.	암호화를 기준으로 관리되는 객체 수는 From = 1입니다.AWS KMS
SSE-S3 암호화를 사용하는 객체 저장	암호화에 따른 객체 수는 Amazon S3에서 관리되며 From = 1입니다.
클라이언트측 암호화를 사용하는(또는 암호화되지 않은) 객체 저장	암호화에 따른 객체 수는 암호화 안함이고 From = 1
DSSE-KMS 암호화를 사용하여 기본적으로 새 객체를 암호화합니다.	기본 암호화 = aws:kms:dsse

버킷을 표시하려면...	이 필터 적용...
기본적으로 SSE-KMS 암호화를 사용하여 새 객체를 암호화합니다	기본 암호화 = aws:kms
기본적으로 SSE-S3 암호화를 사용하여 새 객체를 암호화합니다	기본 암호화 = AES256

기본적으로 DSSE-KMS 또는 SSE-KMS 암호화를 사용하여 새 객체를 암호화하도록 버킷을 구성한 경우 어느 것을 사용할지 결정할 수도 있습니다. AWS KMS key 이렇게 하려면 S3 버킷 페이지에서 버킷을 선택합니다. 버킷 세부 정보 패널의 서버 측 암호화에서 필드를 참조하십시오. AWS KMS key 이 필드에는 키의 Amazon 리소스 이름(ARN) 또는 고유 식별자(키 ID)가 표시됩니다.

Amazon Macie가 고객 관리형 앱을 사용할 수 있도록 허용 AWS KMS key

고객이 관리하는 서버 측 암호화 또는 서버 측 암호화 AWS KMS key (DSSE-KMS 또는 SSE-KMS) 를 사용하여 Amazon S3 객체를 암호화하는 경우, Amazon Macie는 키 사용이 허용된 경우에만 객체의 암호를 해독할 수 있습니다. 이 액세스를 제공하는 방법은 키를 소유한 계정이 객체를 저장하는 S3 버킷도 소유하고 있는지 여부에 따라 달라집니다.

- 동일한 계정이 AWS KMS key 및 버킷을 소유한 경우 해당 계정의 사용자가 키 정책을 업데이트해야 합니다.
- 한 계정이 버킷을 소유하고 다른 계정이 버킷을 소유하는 경우, 키를 소유한 계정의 사용자는 키에 대한 교차 계정 액세스를 허용해야 합니다. AWS KMS key

이 주제에서는 이러한 작업을 수행하는 방법을 설명하고 두 시나리오를 위한 예를 제공합니다. 고객 관리형 서비스에 대한 AWS KMS액세스를 허용하는 방법에 대해 자세히 AWS KMS keys알아보려면 개발자 안내서의 인증 및 액세스 제어를 참조하십시오.AWS Key Management Service

고객 관리형 키에 대한 동일 계정 액세스 허용

동일한 계정이 AWS KMS key 버킷과 S3 버킷을 모두 소유하는 경우 계정 사용자는 키에 대한 설명을 정책에 추가해야 합니다. 추가 문은 계정에 대한 Macie 서비스 연결 역할이 키를 사용하여 데이터를 해독할 수 있도록 허용해야 합니다. 키 정책을 수정하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 변경을 참조하세요.

성명문에서:

- `Principal`요소는 및 S3 버킷을 소유한 계정의 Macie 서비스 연결 역할의 Amazon 리소스 이름(ARN) 을 지정해야 합니다. AWS KMS key

  계정이 옵트인 AWS 리전상태인 경우 ARN에는 해당 지역의 적절한 지역 코드도 포함되어야 합니다. 예를 들어 계정이 리전 코드 me-south-1인 중동(바레인) 리전에 있는 경우, `Principal` 요소에서 `arn:aws:iam::123456789012:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`을(를) 지정해야 하는데, *123456789012*는 해당 계정의 계정 ID입니다. 현재 Macie를 사용할 수 있는 리전의 리전 코드 목록은 AWS 일반 참조의 Amazon Macie 엔드포인트 및 할당량을 참조하세요.
- `Action` 배열은 `kms:Decrypt` 작업을 지정해야 합니다. 키로 암호화된 S3 객체의 암호를 해독하기 위해 Macie가 수행할 수 있어야 하는 유일한 AWS KMS 작업입니다.

다음은 AWS KMS key에 대한 정책에 추가할 문의 예입니다.

```
{
    "Sid": "Allow the Macie service-linked role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

이전 예제에서:

- `Principal` 요소의 `AWS` 필드는 계정의 Macie 서비스 연결 역할(`AWSServiceRoleForAmazonMacie`)의 ARN을 지정합니다. 이 정책을 사용하면 Macie Service 연결 역할이 정책 성명문에 의해 지정된 작업을 수행할 수 있습니다. *123456789012*는 예시 계정 ID입니다. 이 값을 KMS 키와 S3 버킷을 소유한 계정의 계정 ID로 바꿉니다.
- `Action` 배열은 Macie 서비스 연결 역할이 KMS 키를 사용하여 수행할 수 있는 작업, 즉 키로 암호화된 사이퍼텍스트를 해독하는 작업을 지정합니다.

이 성명문을 키 정책에 추가하는 위치는 정책에 현재 포함되어 있는 구조 및 요소에 따라 달라집니다. 정책에 성명문을 추가할 때 구문이 올바른지 확인합니다. 키 정책은 JSON 형식입니다. 즉, 정책에 성명문을 추가하는 위치에 따라 명령문 앞이나 뒤에 쉼표를 추가해야 합니다.

고객 관리형 키에 대한 크로스 계정 액세스 허용

한 계정이 AWS KMS key (키 소유자) 을 소유하고 다른 계정이 S3 버킷을 소유하는 경우 (버킷 소유자), 키 소유자는 버킷 소유자에게 KMS 키에 대한 계정 간 액세스 권한을 제공해야 합니다. 이를 위해 키 소유자는 먼저 키 정책이 버킷 소유자가 키를 사용하고 키에 대한 권한 부여를 생성하는 것을 허용하는 지 확인해야 합니다. 그러면 버킷 소유자가 키에 대한 권한 부여를 생성합니다. 권한 부여는 AWS 보안 주체가 암호화 작업에서 KMS 키를 사용할 수 있도록 하는 정책 도구입니다. 이 경우 권한 부여는 버킷 소유자의 계정에 대한 Macie 서비스 연결 역할에 관련 권한을 위임합니다.

키 정책을 수정하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 변경을 참조하세요. 권한 부여에 대해 자세히 알아보려면 AWS Key Management Service 개발자 안내서의 AWS KMS권한 부여를 참조하세요.

1단계: 키 정책 업데이트

키 정책에서 키 소유자는 정책에 두 가지 문이 포함되도록 해야 합니다.

- 첫 번째 성명문은 버킷 소유자가 키를 사용하여 데이터를 해독할 수 있도록 허용합니다.
- 두 번째 문은 버킷 소유자가 자신(버킷 소유자)의 계정에 대한 Macie 서비스 연결 역할 권한을 생성할 수 있도록 합니다.

첫 번째 성명문에서 `Principal` 요소는 버킷 소유자 계정의 ARN을 지정해야 합니다. `Action` 배열은 `kms:Decrypt` 작업을 지정해야 합니다. 키로 암호화된 객체를 해독하기 위해 Macie가 수행할 수 있는 유일한 AWS KMS 작업입니다. 다음은 AWS KMS key에 대한 정책에서 이 문의 예입니다.

```
{
    "Sid": "Allow account 111122223333 to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

이전 예제에서:

- `Principal` 요소의 `AWS` 필드는 버킷 소유자 계정(*111122223333*)의 ARN을 지정합니다. 이 정책을 사용하여 버킷 소유자는 정책 성명문이 지정한 작업을 수행할 수 있습니다. *111122223333*은 예시 계정 ID입니다. 이 값을 버킷 소유자 계정의 계정 ID로 바꿉니다.
- `Action` 배열은 버킷 소유자가 키로 암호화된 KMS 키-암호 해독 사이퍼텍스트를 사용하여 수행할 수 있는 작업을 지정합니다.

키 정책의 두 번째 성명문은 버킷 소유자가 버킷 소유자 계정의 Macie 서비스 연결 역할에 대한 권한 부여를 생성할 수 있도록 허용합니다. 이 성명문에서 `Principal` 요소는 버킷 소유자 계정의 ARN을 지정해야 합니다. `Action` 배열은 `kms:CreateGrant` 작업을 지정해야 합니다. `Condition`요소는 성명문에서 지정된 `kms:CreateGrant` 작업에 대한 액세스를 필터링할 수 있습니다. 다음은 AWS KMS key에 대한 정책에서 이 문의 예입니다.

```
{
    "Sid": "Allow account 111122223333 to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
        }
    }
}
```

이전 예제에서:

- `Principal` 요소의 `AWS` 필드는 버킷 소유자 계정(*111122223333*)의 ARN을 지정합니다. 이 정책을 사용하여 버킷 소유자는 정책 성명문이 지정한 작업을 수행할 수 있습니다. *111122223333*은 예시 계정 ID입니다. 이 값을 버킷 소유자 계정의 계정 ID로 바꿉니다.
- `Action` 배열은 버킷 소유자가 KMS 키에 대해 수행할 수 있는 작업(키에 대한 권한 부여 생성)을 지정합니다.

- Condition 요소는 StringEquals 조건 연산자kms:GranteePrincipal와 조건 키를 사용하여 정책 성명문에 지정된 작업에 대한 액세스를 필터링합니다. 이 경우 버킷 소유자는 계정에 대한 Macie 서비스 연결 역할의 ARN인 지정된 GranteePrincipal에 대해서만 권한 부여를 생성할 수 있습니다. 해당 ARN에서 *111122223333#* 예시계정 ID입니다. 이 값을 버킷 소유자 계정의 계정 ID로 바꿉니다.

  버킷 소유자 계정이 옵트인 AWS 리전상태인 경우 Macie 서비스 연결 역할의 ARN에 적절한 지역 코드도 포함하십시오. 예를 들어 계정이 리전 코드 me-south-1인 중동(바레인) 리전에 있는 경우 ARN에서 macie.amazonaws.com을 macie.me-south-1.amazonaws.com으로 바꾸세요. 현재 Macie를 사용할 수 있는 리전의 리전 코드 목록은 AWS 일반 참조의 Amazon Macie 엔드포인트 및 할당량을 참조하세요.

이 성명문 소유자는 이 성명문은 키 정책에 추가하는 위치는 정책에 현재 포함되어 있는 구조 및 요소에 따라 달라집니다. 키 소유자가 문을 추가할 때는 구문이 유효한지 확인해야 합니다. 키 정책에는 JSON 형식이 사용됩니다. 이는 키 소유자가 정책에서 문을 추가하는 위치에 따라 각 문 앞이나 뒤에 쉼표도 추가해야 함을 의미합니다.

2단계: 권한 부여 생성

키 소유자가 필요에 따라 키 정책을 업데이트한 후, 버킷 소유자는 그 키에 대한 권한 부여를 생성해야 합니다. 권한 부여는 관련 권한을 버킷 소유자 계정의 Macie 서비스 연결 역할에 위임합니다. 버킷 소유자는 권한 부여를 생성하기 전에 자신의 계정에 대한 kms:CreateGrant작업을 수행하도록 허용되었는지 확인해야 합니다. 이 작업을 통해 기존 고객 관리형 AWS KMS key에 권한 부여를 추가할 수 있습니다.

허가를 생성하기 위해 버킷 소유자는 API 작업을 사용할 수 있습니다. CreateGrant AWS Key Management Service 버킷 소유자는 권한 부여를 생성할 때 필수 파라미터에 다음 값을 지정해야 합니다.

- KeyId - KMS 키의 ARN. KMS 키에 대한 크로스 계정 액세스의 경우 이 값은 ARN이어야 합니다. 키 ID일 수 없습니다.
- GranteePrincipal - 계정에 대한 Macie 서비스 연결 역할(AWSServiceRoleForAmazonMacie)의 ARN 이 값은 arn:aws:iam::*111122223333*:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie이어야 하며, 여기서 *111122223333*은 버킷 소유자 계정의 계정 ID입니다.

  계정이 옵트인 리전에 있는 경우 ARN에 해당 리전 코드가 포함되어야 합니다. 예를 들어 계정이 중동(바레인) 리전에 있고 리전 코드가 me-south-1인 경우 ARN

은 arn:aws:iam::*111122223333*:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie가 되어야 하며, 여기서 *111122223333*은 버킷 소유자 계정의 계정 ID입니다.

- Operations— AWS KMS 암호 해독 작업 ()Decrypt. KMS 키로 암호화된 객체를 해독하기 위해 Macie가 수행할 수 있어야 하는 유일한 AWS KMS 작업입니다.

AWS Command Line Interface (AWS CLI) 를 사용하여 고객 관리형 KMS 키에 대한 권한 부여를 생성하려면 create-grant 명령을 실행합니다. 다음 예에서는 이 작업을 수행하는 방법을 보여줍니다. 이 예제는 Microsoft Windows용으로 포맷되었으며 가독성을 높이기 위해 캐럿 (^) 줄 연속 문자를 사용합니다.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie ^
--operations "Decrypt"
```

위치:

- key-id권한 부여를 적용할 KMS 키의 ARN을 지정합니다.
- grantee-principal은 권한 부여로 지정된 작업을 수행할 수 있는 계정에 대한 Macie 서비스 연결 역할의 ARN을 지정합니다. 이 값은 키 정책의 두 번째 문의 kms:GranteePrincipal 조건에 지정된 ARN과 일치해야 합니다.
- operations는 지정된 주체가 권한을 통해 수행할 수 있는 작업(KMS 키로 암호화된 사이퍼텍스트 해독)을 지정합니다.

이 명령이 성공적으로 실행되면 다음과 비슷한 출력이 표시됩니다.

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

여기서 GrantToken은 생성된 권한 부여를 나타내는 고유하고 암호화되지 않은 가변 길이 base64 인코딩 문자열이며 GrantId은 권한 부여의 고유 식별자입니다.

Amazon Macie의 민감한 데이터 검색 결과 저장 및 유지

민감한 데이터 검색 작업을 실행하거나 Amazon Macie가 민감한 데이터 자동 검색을 수행할 때 Macie는 분석 범위에 포함된 각 Amazon Simple Storage Service(S3) 객체에 대한 분석 레코드를 생성합니다. 민감한 데이터 검색 결과라고 하는 이러한 레코드는 Macie가 개별 S3 객체에 대해 수행하는 분석에 대한 상세 정보를 기록합니다. 여기에는 민감한 데이터를 찾지 못해서 민감한 데이터 결과가 생성되지 않는 객체와 오류 또는 문제로 인해 Macie가 분석할 수 없는 객체도 포함됩니다. Macie가 물체에서 민감한 데이터를 감지하면 기록에는 해당 발견의 데이터와 추가 정보가 포함됩니다. 민감한 데이터 검색 결과에는 데이터 프라이버시 및 보호 감사 또는 조사에 도움이 될 수 있는 분석 기록이 표시됩니다.

Macie는 민감한 데이터 검색 결과를 90일 동안만 저장합니다. 결과에 액세스하고 결과를 장기간 저장 및 보관하려면, 결과를 AWS Key Management Service (AWS KMS)키로 암호화하고 S3 버킷에 저장하도록 Macie를 구성하십시오. 버킷은 모든 민감한 데이터 검색 결과를 위한 확정적이고 장기적인 리포지토리 역할을 할 수 있습니다. 그런 다음, 필요에 따라 해당 리포지토리에 있는 결과에 액세스하고 쿼리할 수 있습니다.

이 항목에서는 를 사용하여 민감한 데이터 검색 결과를 위한 리포지토리를 구성하는 프로세스를 안내합니다. AWS Management Console 구성은 결과를 AWS KMS key 암호화하는 S3 범용 버킷, 결과를 저장하는 S3 범용 버킷, 사용할 키와 버킷을 지정하는 Macie 설정의 조합입니다. 프로그래밍 방식으로 Macie 설정을 구성하려는 경우 Amazon Macie API의 PutClassificationExportConfiguration작업을 사용할 수 있습니다.

Macie에서 설정을 구성할 때 선택한 항목은 현재 AWS 리전에만 적용됩니다. 조직의 Macie 관리자인 경우 선택 사항은 해당 계정에만 적용됩니다. 연결된 멤버 계정에는 적용되지 않습니다.

Macie를 여러 AWS 리전곳에서 사용하는 경우 Macie를 사용하는 각 지역의 리포지토리 설정을 구성하십시오. 필요에 따라 여러 리전에 대한 민감한 데이터 검색 결과를 동일한 S3 버킷에 저장할 수 있습니다. 그러나 다음과 같은 요구 사항을 확인해야 합니다.

- 미국 동부 (버지니아 북부) 지역과 같이 기본적으로 AWS 활성화되는 지역의 결과를 저장하려면 기본적으로 활성화된 지역의 버킷을 선택해야 합니다. AWS 계정옵트인 리전(기본적으로 비활성화되어 있는 리전)에서는 결과를 버킷에 저장할 수 없습니다.
- 중동(바레인) 리전과 같은 옵트인 리전에 대한 결과를 저장하려면 동일한 리전 또는 기본적으로 활성화된 리전의 버킷을 선택해야 합니다. 결과는 다른 옵트인 리전의 버킷에 저장할 수 없습니다.

리전이 기본적으로 활성화되어 있는지 확인하려면 AWS Identity and Access Management 사용 설명서에서 지역 및 엔드포인트를 참조하세요. 위의 요구 사항 외에도 Macie가 개별 조사 결과에서 보고하는 민감한 데이터의 샘플을 검색할지 여부도 고려하십시오. 영향을 받는 S3 객체에서 민감한 데이터

샘플을 검색하려면 영향 받는 객체, 해당 검색 결과, 해당하는 민감한 데이터 검색 결과 등 모든 리소스와 데이터를 동일한 지역에 저장해야 합니다.

Tasks

개요

Amazon Macie는 민감한 데이터 검색 작업을 실행하거나 민감한 데이터 자동 검색을 수행할 때 분석 또는 분석을 시도하는 각 Amazon S3 객체에 대해 민감한 데이터 검색 결과를 자동으로 생성합니다. 여기에는 다음이 포함됩니다.

- Macie가 민감한 데이터를 감지하여 민감한 데이터 결과를 생성하는 객체.
- Macie가 민감한 데이터를 감지하지 못해 민감한 데이터 결과를 생성하지 않는 객체.
- 권한 설정 또는 지원되지 않는 파일 또는 저장 형식 사용과 같은 오류나 문제로 인해 Macie가 분석할 수 없는 객체.

Macie가 S3 개체에서 민감한 데이터를 감지하는 경우, 민감한 데이터 검색 결과에는 해당 민감한 데이터에 대한 조사 결과도 포함됩니다. Macie가 객체에서 발견한 각 유형의 민감한 데이터가 1,000건 이상 발생한 위치와 같은 추가 정보도 제공합니다. 예:

- Microsoft Excel 통합 문서, CSV 파일 또는 TSV 파일에 있는 셀 또는 필드의 열 및 행 번호
- JSON 또는 JSON 라인 파일에 있는 필드 또는 배열의 경로
- CSV, JSON, JSON 라인 또는 TSV 파일이 아닌 비이진 텍스트 파일(예: HTML, TXT 또는 XML 파일)의 줄 번호
- Adobe PDF(휴대용 문서 형식) 파일에 있는 페이지의 페이지 번호
- Apache Avro 객체 컨테이너 또는 Apache Parquet 파일에 있는 레코드 인덱스 및 레코드 내 필드 경로

영향을 받는 S3 객체가 아카이브 파일 (예: .tar 또는.zip 파일) 인 경우, 민감한 데이터 검색 결과는 Macie가 아카이브에서 추출한 개별 파일의 민감한 데이터 발생에 대한 자세한 위치 데이터도 제공합

니다. Macie는 아카이브 파일에 대한 민감한 데이터 조사 결과에 이 정보를 포함시키지 않습니다. 위치 데이터를 보고하기 위해 민감한 데이터 검색 결과는 표준화된 JSON 스키마를 사용합니다.

민감한 데이터 검색 결과에는 Macie가 발견한 민감한 데이터는 포함되지 않습니다. 대신 감사 또는 조사에 도움이 될 수 있는 분석 기록을 제공합니다.

Macie는 민감한 데이터 검색 결과를 90일 동안 저장합니다. Amazon Macie 콘솔이나 Amazon Macie API에서는 바로 액세스할 수 없습니다. 대신 이 항목의 단계에 따라 사용자가 지정한 S3 범용 버킷으로 결과를 암호화하고 사용자가 지정한 S3 범용 버킷에 결과를 저장하도록 Macie를 구성하십시오. AWS KMS key 그런 다음 Macie는 결과를 JSON 라인(.jsonl) 파일에 쓰고, 버킷에 GNU Zip(.gz) 파일로 파일을 추가하고, SSE-KMS 암호화를 사용하여 데이터를 암호화합니다. 또한 2023년 11월 8일부터 Macie는 해시 기반 메시지 인증 코드 (HMAC) 로 결과 S3 객체에 서명합니다. AWS KMS key

민감한 데이터 검색 결과를 S3 버킷에 저장하도록 Macie를 구성한 후에는 이 버킷이 결과의 최종적이고 장기적인 리포지토리 역할을 수행할 수 있습니다. 그런 다음, 필요에 따라 해당 리포지토리에 있는 결과에 액세스하고 쿼리할 수 있습니다.

> **Tip**
>
> 민감한 데이터 검색 결과를 쿼리하고 사용하여 잠재적 데이터 보안 위험을 분석하고 보고하는 방법에 대한 자세한 지침 예제는 보안 QuickSight 블로그의 Amazon Athena와 Amazon을 사용하여 Macie의 민감한 데이터 검색 결과를 쿼리하고 시각화하는 방법 블로그 게시물을 참조하십시오.AWS
>
> 민감한 데이터 검색 결과를 분석하는 데 사용할 수 있는 Amazon Athena 쿼리 샘플을 보려면의 Amazon Macie 결과 분석 리포지토리를 방문하십시오. GitHub 또한 이 리포지토리는 결과를 검색하고 해독할 수 있게 Athena를 구성하는 지침과 결과에 대한 테이블을 생성하는 스크립트도 제공합니다.

1단계: 권한 확인

민감한 데이터 검색 결과에 대한 리포지토리를 구성하기 전에 결과를 암호화하고 저장하는 데 필요한 권한이 있는지 확인합니다. 권한을 확인하려면 AWS Identity and Access Management (IAM) 을 사용하여 IAM ID에 연결된 IAM 정책을 검토하십시오. 그런 다음 해당 정책의 정보를 리포지토리를 구성하기 위해 수행할 수 있는 다음 작업 목록과 비교합니다.

Amazon Macie

Macie의 경우 다음 작업을 수행할 수 있는지 확인합니다.

`macie2:PutClassificationExportConfiguration`

이 작업을 통해 Macie에서 리포지토리 설정을 추가하거나 변경할 수 있습니다.

Amazon S3

Amazon S3의 경우 다음 작업을 수행할 수 있는지 확인합니다.

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

이러한 작업을 통해 리포지토리 역할을 할 수 있는 S3 범용 버킷에 액세스하고 구성할 수 있습니다.

AWS KMS

Amazon Macie 콘솔을 사용하여 리포지토리 설정을 추가하거나 변경하려면 다음 AWS KMS 작업을 수행할 수 있는 권한이 있는지 확인합니다.

- `kms:DescribeKey`
- `kms:ListAliases`

이러한 작업을 통해 계정의 AWS KMS keys 에 대한 정보를 검색하고 표시할 수 있습니다. 그런 다음 이러한 키 중 하나를 선택하여 민감한 데이터 검색 결과를 암호화할 수 있습니다.

새 데이터를 생성하여 데이터를 AWS KMS key 암호화하려는 경우 `kms:CreateKey`, `kms:GetKeyPolicy`, 및 `kms:PutKeyPolicy` 다음 작업도 수행할 수 있어야 합니다.

필요한 작업을 수행할 수 없는 경우 다음 단계로 진행하기 전에 AWS 관리자에게 도움을 요청하십시오.

2단계: AWS KMS key구성

권한을 확인한 후 Macie가 AWS KMS key 민감한 데이터 검색 결과를 암호화하는 데 사용할 권한을 결정하십시오. 키는 결과를 저장하려는 S3 버킷과 AWS 리전 동일하게 활성화된 고객 관리형 대칭 암호화 KMS 키여야 합니다.

키는 사용자 AWS KMS key 계정의 기존 키이거나 다른 계정이 AWS KMS key 소유한 기존 키일 수 있습니다. 새 KMS 키를 사용하려면 진행하기 전에 키를 생성합니다. 다른 계정이 소유하고 있는 기존 키를 사용하려면 해당 키의 Amazon 리소스 이름(ARN)이 필요합니다. Macie에서 리포지토리 설정을 구성할 때 이 ARN을 입력해야 합니다. KMS 키의 설정을 만들고 검토하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 키 관리를 참조하십시오.

> **Note**
>
> 키는 외부 키 스토어에 있을 수 있습니다. AWS KMS key 하지만 이 키는 AWS KMS내에서 완전히 관리되는 키보다 속도가 느리고 안정성이 떨어질 수 있습니다. 민감한 데이터 검색 결과를 S3 버킷 키로 사용하도록 구성된 S3 버킷에 저장하면 이러한 위험을 줄일 수 있습니다. 이렇게 하면 민감한 데이터 검색 결과를 암호화하기 위해 수행해야 하는 AWS KMS 요청 횟수를 줄일 수 있습니다.
>
> 외부 키 저장소에 있는 KMS 키 사용에 대한 정보는 AWS Key Management Service 개발자 가이드의 외부 키 저장소를 참조하십시오. S3 버킷 키 사용에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 버킷 키로 SSE-KMS 비용 절감을 참조하세요.

Macie가 사용할 KMS 키를 결정한 후에는 Macie에 키 사용 권한을 부여합니다. 그렇지 않으면 Macie는 결과를 암호화하거나 리포지토리에 저장할 수 없습니다. Macie에게 키 사용 권한을 부여하려면 키에 대한 키 정책을 업데이트하십시오. 키 정책 및 KMS 키 액세스 관리에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드에서 AWS KMS의 키 정책을 참조하십시오.

키 정책을 업데이트하려면

1. https://console.aws.amazon.com/kms 에서 AWS KMS 콘솔을 엽니다.
2. 를 변경하려면 페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS 리전
3. Macie에서 민감한 데이터 검색 결과를 암호화하는 데 사용할 키를 선택합니다.
4. 키 정책 탭에서 편집을 선택합니다.
5. 다음 설명을 클립보드에 복사한 다음 정책에 추가합니다.

```
{
    "Sid": "Allow Macie to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "macie.amazonaws.com"
    },
```

```
    "Action": [
        "kms:GenerateDataKey",
        "kms:Encrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
         },
         "ArnLike": {
             "aws:SourceArn": [
                 "arn:aws:macie2:Region:111122223333:export-configuration:*",
                 "arn:aws:macie2:Region:111122223333:classification-job/*"
             ]
         }
    }
}
```

> **Note**
>
> 정책에 문을 추가할 때 구문이 올바른지 확인합니다. 정책은 JSON 형식입니다. 즉, 정책에 성명문을 추가하는 위치에 따라 명령문 앞이나 뒤에 쉼표를 추가해야 합니다. 문을 정책의 마지막 문으로 추가하는 경우 이전 섹션의 닫는 괄호 뒤에 쉼표를 추가합니다. 문을 첫 번째 문으로 추가하거나 기존 두 문 사이에 추가하는 경우 닫는 괄호 뒤에 쉼표를 추가합니다.

6. 환경에 맞는 올바른 값으로 명령문을 업데이트합니다.

- `Condition` 필드에서 자리 표시자 값을 다음과 같이 바꿉니다.
  - *111122223333*은 AWS 계정의 계정 ID입니다.
  - *###* Macie를 사용하고 있으며 Macie가 키를 사용하도록 허용하려는 지역입니다. AWS 리전

    여러 리전에서 Macie를 사용하고 있으며 Macie가 다른 리전에서도 키를 사용할 수 있도록 허용하려면 각 리전에 `aws:SourceArn` 조건을 추가합니다. 예:

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
    "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
```

```
]
```

또는 Macie가 모든 리전에서 키를 사용하도록 허용할 수도 있습니다. 이렇게 하려면 자리표시자 값을 와일드카드 문자(*)로 바꿉니다. 예:

```
"aws:SourceArn": [
    "arn:aws:macie2:*:111122223333:export-configuration:*",
    "arn:aws:macie2:*:111122223333:classification-job/*"
]
```

- 옵트인 리전에서 Macie를 사용하는 경우 `Service` 필드 값에 적절한 리전 코드를 추가합니다. 예를 들어 계정이 지역 코드 me-south-1인 중동(바레인) 지역서 Macie를 사용하는 경우 ARN에서 `macie.amazonaws.com`를 `macie.me-south-1.amazonaws.com`으로 바꾸십시오. 현재 Macie를 사용할 수 있는 리전 목록 및 각 리전의 지역 코드는 AWS 일반 참조의 Amazon Macie 엔드포인트 및 할당량을 참조하세요.

참고로 `Condition` 필드에는 두 개의 IAM 글로벌 조건 키가 사용됩니다.

- aws: SourceAccount — 이 조건을 사용하면 Macie가 사용자 계정에 대해서만 지정된 작업을 수행할 수 있습니다. 좀 더 구체적으로 설명하면 `aws:SourceArn` 조건으로 지정된 리소스 및 작업에 대해 지정된 작업을 수행할 수 있는 계정을 결정합니다.

  Macie가 다른 계정에서도 지정된 작업을 수행할 수 있도록 하려면 각 계정의 계정 ID를 이 조건에 추가합니다. 예:

  ```
  "aws:SourceAccount": [111122223333,444455556666]
  ```

- aws: SourceArn — 이 조건은 다른 AWS 서비스 사람이 지정된 작업을 수행하는 것을 방지합니다. 또한 계정에서 다른 작업을 수행하는 동안 Macie가 키를 사용하지 못하도록 합니다. 즉, Macie는 객체가 민감한 데이터 검색 결과이고 결과가 지정된 지역의 지정된 계정으로 생성된 자동 민감한 데이터 검색 또는 민감한 데이터 검색 작업에 대한 결과인 경우에만 키를 사용하여 S3 객체를 암호화할 수 있습니다.

  Macie가 다른 계정에서도 지정된 작업을 수행할 수 있도록 하려면 각 계정의 ARN을 이 조건에 추가합니다. 예:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
      "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
  ```

```
    "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
    "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
]
```

`aws:SourceAccount` 및 `aws:SourceArn` 조건에 지정된 계정이 일치해야 합니다.

이러한 조건은 Macie와 거래하는 동안 혼란스러운 대리인으로 사용되는 것을 방지하는 데 도움이 됩니다. AWS KMS권장하지는 않지만 명령문에서 이러한 조건을 직접 삭제할 수 있습니다.

7. 명령문 추가 및 업데이트를 마치면 변경 사항 저장을 선택합니다.

3단계: S3 버킷 선택

권한을 확인하고 구성했으면 민감한 데이터 검색 결과를 위한 리포지토리로 사용할 S3 버킷을 지정할 준비가 된 것입니다. AWS KMS key여기에는 두 가지 옵션이 있습니다.

- Macie가 생성한 새 S3 버킷 사용 — 이 옵션을 선택하면 Macie는 검색 결과를 AWS 리전 위해 최신 S3 범용 버킷을 자동으로 생성합니다. Macie는 또한 해당 버킷에 버킷 정책을 적용합니다. 이 정책을 통해 Macie는 버킷에 객체를 추가할 수 있습니다. 또한 SSE-KMS 암호화를 사용하여 지정한 AWS KMS key 로 개체를 암호화해야 합니다. 정책을 검토하려면 버킷의 이름과 사용할 KMS 키를 지정한 후 Amazon Macie 콘솔에서 정책 보기를 선택합니다.
- 생성한 기존 S3 버킷 사용 - 생성한 특정 S3 버킷에 검색 결과를 저장하려면 진행하기 전에 버킷을 생성해야 합니다. 버킷은 범용 버킷이어야 합니다. 또한 버킷의 설정 및 정책에서 Macie가 버킷에 객체를 추가할 수 있도록 허용해야 합니다. 이 주제에서는 확인해야 할 설정과 정책을 업데이트하는 방법을 설명합니다. 또한 정책에 추가할 명령문의 예도 제공합니다.

다음 단원에서는 그 방법에 대해서 설명합니다. 원하는 옵션에 대한 선택사항을 선택합니다.

Macie가 생성한 새 S3 버킷 사용

Macie가 생성한 새 S3 버킷을 사용하려는 경우 프로세스의 마지막 단계에서 Macie에 리포지토리 설정을 구성해야 합니다.

Macie에서 리포지토리 설정을 구성하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 결과 찾기를 선택합니다.
3. 민감한 데이터 검색 결과에 대한 리포지토리에서 버킷 생성을 선택합니다.

4. 버킷 만들기 대화 상자에서 버킷 이름을 입력합니다.

   이 이름은 모든 S3 버킷에 대해 고유해야 합니다. 버킷 이름은 소문자, 숫자, 점(.) 및 하이픈(-)으로만 구성될 수 있습니다. 이름 지정 규칙의 추가 요건은 Amazon Simple Storage Service 사용 설명서의 버킷 이름 지정 규칙을 참조하세요.

5. [Advanced] 단원을 확장합니다.

6. (선택 사항) 버킷의 위치 경로에 사용할 접두사를 지정하려면 데이터 검색 결과 접두사 상자에 접두사를 입력합니다.

   값을 입력하면 Macie는 상자 아래의 예를 업데이트하여 검색 결과를 저장할 버킷의 위치 경로를 표시합니다.

7. 모든 퍼블릭 액세스 차단에서 예를 선택하여 버킷에 대한 모든 퍼블릭 액세스 차단 설정을 활성화합니다.

   이 설정에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 Storage에 대한 퍼블릭 액세스 차단을 참조하세요.

8. 암호화 설정에서 Macie가 결과를 암호화하는 데 사용하려는 AWS KMS key 를 지정합니다.

   - 자신의 계정에 있는 키를 사용하려면 내 계정에서 키 선택을 선택합니다. 그런 다음 AWS KMS key목록에서 사용할 키를 선택합니다. 목록에는 계정의 고객 관리형 대칭 암호화 KMS 키가 표시됩니다.
   - 다른 계정이 소유한 키를 사용하려면 다른 계정에 있는 키의 ARN 입력을 선택합니다. 그런 다음 AWS KMS key ARN 상자에 사용할 키의 Amazon 리소스 이름(ARN)을 입력합니다(예: **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**).

9. 규칙에 대한 설정 입력을 마치면 저장를 선택합니다.

   Macie는 설정이 올바른지 테스트합니다. 설정이 올바르지 않으면 Macie는 문제 해결에 도움이 되는 오류 메시지를 표시합니다.

리포지토리 설정을 저장하면 Macie는 이전 90일 동안의 기존 검색 결과를 리포지토리에 추가합니다. 또한 Macie는 새 검색 결과를 리포지토리에 추가하기 시작합니다.

생성한 기존 S3 버킷 사용

민감한 데이터 검색 결과를 생성한 특정 S3 버킷에 저장하려면 Macie에서 설정을 구성하기 전에 버킷을 만들고 구성하십시오. 버킷을 생성할 때 다음 요구 사항에 유의합니다.

- 버킷은 범용 버킷이어야 합니다. 디렉터리 버킷이 될 수 없습니다.
- 버킷에 대해 객체 잠금을 활성화하면 해당 기능에 대한 기본 보존 설정을 비활성화해야 합니다. 그렇지 않으면 Macie는 검색 결과를 버킷에 추가할 수 없습니다. 이 설정에 대한 정보는 Amazon Simple Storage Service 사용 설명서의 Amazon S3 객체 잠금 사용을 참조하세요.
- 미국 동부 (버지니아 북부) 지역과 같이 기본적으로 활성화된 지역의 검색 결과를 저장하려면 버킷이 기본적으로 활성화된 지역에 있어야 합니다. AWS 계정옵트인 리전(기본적으로 비활성화되어 있는 리전)에서는 결과를 버킷에 저장할 수 없습니다.
- 중동(바레인) 리전과 같은 옵트인 리전에 대한 검색 결과를 저장하려면 버킷이 동일한 리전 또는 기본적으로 활성화된 리전에 있어야 합니다. 결과는 다른 옵트인 리전의 버킷에 저장할 수 없습니다.

리전이 기본적으로 활성화되어 있는지 확인하려면 AWS Identity and Access Management 사용 설명서에서 지역 및 엔드포인트를 참조하세요.

버킷을 생성한 후에는 Macie가 버킷에 대한 정보를 검색하고 버킷에 객체를 추가할 수 있도록 버킷 정책을 업데이트합니다. 그런 다음 Macie에서 설정을 구성할 수 있습니다.

버킷의 버킷 정책을 업데이트하는 방법

1. https://console.aws.amazon.com/s3/에서 S3 콘솔을 엽니다.
2. 검색 결과를 저장할 버킷을 선택합니다.
3. 권한 탭을 선택합니다.
4. 버킷 정책 섹션에서 편집을 선택합니다.
5. 다음 예제 정책을 클립보드에 복사합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Macie to use the GetBucketLocation operation",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
```

```
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
            "Sid": "Allow Macie to add objects to the bucket",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
```

```
        },
        {
            "Sid": "Deny incorrect encryption headers. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:Region:111122223333:key/KMSKeyId"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::myBucketName/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

6. Amazon S3 콘솔의 버킷 정책 편집기에서 예제 정책을 붙여넣습니다.
7. 환경에 맞는 올바른 값으로 정책을 업데이트합니다.

   - 잘못된 암호화 헤더를 거부하는 선택적 명령문에서:
     - 버킷 *myBucketName*이름으로 바꾸십시오.
     - 이 StringNotEquals 경우 *KeyIdARN:AWS:KMS:region:111122223333:key/KMS #* 검색 결과의 암호화에 사용할 Amazon 리소스 이름 (ARN) 으로 대체하십시오. AWS KMS key
   - 그 외 다른 모든 명령문에서는 다음과 같이 자리 표시자 값을 바꿉니다.
     - *myBucketName*버킷 이름입니다.

- *111122223333*은 AWS 계정의 계정 ID입니다.
- *##*은 Macie를 사용하고 있으며 Macie가 검색 결과를 버킷에 추가하도록 허용하려는 AWS 리전 입니다.

  여러 리전에서 Macie를 사용하고 있으며 Macie가 다른 리전에서도 결과를 버킷에 추가할 수 있도록 허용하려면 각 리전에 `aws:SourceArn` 조건을 추가합니다. 예:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
      "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
      "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
      "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
  ]
  ```

  또는 Macie를 사용하는 모든 리전의 결과를 Macie가 버킷에 추가하도록 할 수도 있습니다. 이렇게 하려면 자리표시자 값을 와일드카드 문자(*)로 바꿉니다. 예:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:*:111122223333:export-configuration:*",
      "arn:aws:macie2:*:111122223333:classification-job/*"
  ]
  ```

- 옵트인 리전에서 Macie를 사용하는 경우 Macie 서비스 주체를 지정하는 각 문의 `Service` 필드 값에 적절한 리전 코드를 추가합니다. 예를 들어 계정이 지역 코드 me-south-1인 중동(바레인) 지역에서 Macie를 사용하는 경우 적용되는 각 스테이트먼트에서 `macie.amazonaws.com`를 `macie.me-south-1.amazonaws.com`으로 바꾸십시오. 현재 Macie를 사용할 수 있는 리전 목록 및 각 리전의 지역 코드는 AWS 일반 참조의 Amazon Macie 엔드포인트 및 할당량을 참조하세요.

예제 정책에는 Macie가 버킷이 어느 리전에 있는지 확인하고(`GetBucketLocation`) 버킷에 객체를 추가할 수 있도록 하는(`PutObject`) 문이 포함되어 있습니다. 이 명령문은 다음 두 개의 IAM 글로벌 조건 키를 사용하는 조건을 정의합니다.

- aws: SourceAccount — 이 조건을 통해 Macie는 민감한 데이터 검색 결과를 사용자 계정의 버킷에만 추가할 수 있습니다. 이렇게 하면 Macie가 다른 계정의 검색 결과를 버킷에 추가할 수 없게 됩니다. 좀 더 구체적으로 설명하면 `aws:SourceArn` 조건으로 지정된 리소스 및 작업에 대해 버킷을 사용할 수 있는 계정을 결정합니다.

  버킷에 다른 계정의 결과를 저장하려면 이 조건에 각 계정의 계정 ID를 추가합니다. 예:

```
"aws:SourceAccount": [111122223333,444455556666]
```

- aws: SourceArn — 이 조건은 버킷에 추가되는 객체의 소스를 기반으로 버킷에 대한 액세스를 제한합니다. 다른 AWS 서비스 사람이 버킷에 객체를 추가하는 것을 방지합니다. 또한 계정에서 다른 작업을 수행하는 동안 Macie가 버킷에 객체를 추가하지 못하도록 합니다. 보다 구체적으로 말하자면, Macie는 객체가 민감한 데이터 검색 결과이고 결과가 지정된 지역의 지정된 계정으로 생성된 자동화된 민감한 데이터 검색 또는 민감한 데이터 검색 작업에 대한 결과인 경우에만 버킷에 객체를 추가할 수 있도록 허용합니다.

  Macie가 다른 계정에서도 지정된 작업을 수행할 수 있도록 하려면 각 계정의 ARN을 이 조건에 추가합니다. 예:

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
    "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
]
```

  `aws:SourceAccount` 및 `aws:SourceArn` 조건에 지정된 계정이 일치해야 합니다.

  이러한 조건은 Amazon S3와의 거래에서 Macie가 혼동된 대리자로 사용되는 것을 방지하는 데 도움이 됩니다. 권장하지는 않지만 버킷 정책에서 이러한 조건을 직접 삭제할 수 있습니다.

8. 버킷 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

이제 Macie에서 리포지토리 설정을 구성할 수 있습니다.

Macie에서 리포지토리 설정을 구성하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 결과 찾기를 선택합니다.
3. 민감한 데이터 검색 결과에 대한 리포지토리에서 기존 버킷을 선택합니다.
4. 버킷 선택에서는 검색 결과를 저장할 버킷을 선택합니다.
5. (선택 사항) 버킷의 위치 경로에 사용할 접두사를 지정하려면 고급 섹션을 확장합니다. 그런 다음 데이터 검색 결과 접두사에 사용할 접두사를 입력합니다.

값을 입력하면 Macie는 상자 아래의 예를 업데이트하여 검색 결과를 저장할 버킷의 위치 경로를 표시합니다.

6. 암호화 설정에서 Macie가 결과를 암호화하는 데 사용하려는 AWS KMS key 를 지정합니다.

   - 자신의 계정에 있는 키를 사용하려면 내 계정에서 키 선택을 선택합니다. 그런 다음 AWS KMS key목록에서 사용할 키를 선택합니다. 목록에는 계정의 고객 관리형 대칭 암호화 KMS 키가 표시됩니다.
   - 다른 계정이 소유한 키를 사용하려면 다른 계정에 있는 키의 ARN 입력을 선택합니다. 그런 다음 AWS KMS key ARN 상자에 사용할 키의 Amazon 리소스 이름(ARN)을 입력합니다(예: **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**).

7. 규칙에 대한 설정 입력을 마치면 저장를 선택합니다.

   Macie는 설정이 올바른지 테스트합니다. 설정이 올바르지 않으면 Macie는 문제 해결에 도움이 되는 오류 메시지를 표시합니다.

리포지토리 설정을 저장하면 Macie는 이전 90일 동안의 기존 검색 결과를 리포지토리에 추가합니다. 또한 Macie는 새 검색 결과를 리포지토리에 추가하기 시작합니다.

> **Note**
>
> 나중에 데이터 검색 결과 접두사 설정을 변경하는 경우 Amazon S3의 버킷 정책도 업데이트합니다. 이전 경로를 지정하는 정책 문은 새로운 경로를 지정해야 합니다. 그러지 않으면 Macie는 검색 결과를 버킷에 추가할 수 없습니다.

> **Tip**
>
> 또한 서버 측 암호화 비용을 줄이려면 S3 버킷 키를 사용하도록 S3 버킷을 구성하고 민감한 데이터 검색 결과를 암호화하도록 구성한 AWS KMS key 것을 지정하십시오. S3 버킷 키를 사용하면 호출 횟수가 AWS KMS줄어들어 AWS KMS 요청 비용을 줄일 수 있습니다. KMS 키가 외부 키 저장소에 있는 경우 S3 버킷 키를 사용하면 키 사용으로 인한 성능 영향을 최소화할 수도 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 버킷 키를 사용하여 SSE-KMS 비용 절감을 참조하세요.

Amazon Macie에서 지원하는 스토리지 클래스 및 형식

Amazon Simple Storage Service(S3) 데이터 자산에서 민감한 데이터를 검색할 수 있도록 Amazon Macie는 대부분의 Amazon S3 스토리지 클래스와 다양한 파일 및 스토리지 형식을 지원합니다. 이 지원은 관리형 데이터 식별자와 사용자 지정 데이터 식별자를 사용하여 S3 객체를 분석하는 데 적용됩니다.

Macie가 S3 객체를 분석하려면 지원되는 스토리지 클래스를 사용하여 객체를 Amazon S3 범용 버킷에 저장해야 합니다. 또한 객체는 지원되는 파일 또는 스토리지 형식을 사용해야 합니다. 이 섹션의 주제에서는 현재 Macie가 지원하는 스토리지 클래스와 파일 및 스토리지 형식을 설명합니다.

> **Tip**
>
> Macie는 Amazon S3에 최적화되어 있지만, 이를 사용하여 현재 다른 곳에 저장하고 있는 리소스에서 민감한 데이터를 검색할 수 있습니다. 데이터를 Amazon S3로 임시 또는 영구적으로 이동하여 이 작업을 수행할 수 있습니다. 예를 들어 Amazon 관계형 데이터베이스 서비스 또는 Amazon Aurora 스냅샷을 Apache Parquet 형식으로 Amazon S3로 내보낼 수 있습니다. 또는 Amazon DynamoDB 표를 Amazon S3로 내보냅니다. 그런 다음 민감한 데이터 검색 작업을 생성하여 Amazon S3에서 데이터를 분석할 수 있습니다.

주제

지원되는 Amazon S3 스토리지 클래스

민감한 데이터 검색을 위해 Amazon Macie는 다음과 같은 Amazon S3 스토리지 클래스를 지원합니다.

- 중복성 감소(RRS)
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering
- S3 One Zone-Infrequent Access(S3 One Zone-IA)
- S3 Standard
- S3 Standard-Infrequent Access(S3 Standard-IA)

Macie는 S3 Glacier Deep Archive 또는 S3 Express One Zone과 같은 다른 Amazon S3 스토리지 클래스를 사용하는 S3 객체는 분석하지 않습니다. 또한 Macie는 S3 디렉터리 버킷에 저장된 객체를 분석하지 않습니다.

지원되는 Amazon S3 스토리지 클래스를 사용하지 않는 S3 객체를 분석하도록 민감한 데이터 검색 작업을 구성하더라도 Macie는 작업 실행 시 해당 객체를 건너뜁니다. Macie는 해당 객체에서 데이터를 검색하거나 분석하려고 시도하지 않으며, 해당 객체는 분류할 수 없는 객체로 취급됩니다. 분류할 수 없는 객체란 지원되는 스토리지 클래스나 지원되는 파일 또는 스토리지 형식을 사용하지 않는 객체를 말합니다. Macie는 지원되는 스토리지 클래스와 지원되는 파일 또는 스토리지 형식을 사용하는 객체만 분석합니다.

마찬가지로 민감한 데이터를 자동으로 검색하도록 Macie를 구성하더라도 분류할 수 없는 객체는 선택 및 분석에 대상에 포함되지 않습니다. Macie는 지원되는 스토리지 클래스와 지원되는 파일 또는 Amazon S3 스토리지 형식을 사용하는 객체만 분석합니다.

분류할 수 없는 객체를 저장하는 S3 버킷을 식별하기 위해 S3 버킷 인벤토리를 필터링할 수 있습니다. 인벤토리의 각 버킷에는 버킷에 있는 분류할 수 없는 객체의 수와 총 스토리지 크기를 보고하는 필드가 있습니다.

Amazon S3에서 제공하는 스토리지 클래스에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 스토리지 클래스 사용을 참조하십시오.

지원되는 파일 및 스토리지 형식

Amazon Macie가 S3 객체를 분석할 때 Macie는 Amazon S3에서 객체의 최신 버전을 검색한 다음 객체의 콘텐츠에 대한 심층 검사를 수행합니다. 이 검사는 데이터의 파일 또는 스토리지 형식을 고려합니다. Macie는 일반적으로 사용되는 압축 및 아카이브 형식을 포함하여 다양한 형식의 데이터를 분석할 수 있습니다.

Macie가 압축 또는 아카이브 파일의 데이터를 분석할 때 전체 파일과 파일의 내용을 모두 검사합니다. 파일 내용을 검사하기 위해 Macie는 파일의 압축을 푼 다음 지원되는 형식을 사용하는 추출된 각 파일을 검사합니다. Macie는 최대 1,000,000개의 파일 및 최대 10레벨의 중첩 깊이에 대해 이 작업을 수행할 수 있습니다. 민감한 데이터 검색에 적용되는 추가 할당량에 대한 자세한 내용은 Amazon Macie 할당량을 참조하십시오.

다음 표에서는 Macie가 민감한 데이터를 검색하기 위해 분석할 수 있는 파일 유형 및 스토리지 형식을 설명합니다. 표에는 지원되는 각 유형과 해당 파일 이름 확장자도 함께 나와 있습니다.

파일 또는 스토리지 유형	설명	파일 이름 확장자
빅 데이터	Apache Avro 객체 컨테이너 및 Apache Parquet 파일	.avro, .parquet
압축 또는 아카이브	GNU Zip 압축 아카이브, TAR 아카이브 및 ZIP 압축 아카이브	.gz, .gzip, .tar, .zip
문서	Adobe Portable Document Format 파일, Microsoft Excel 통합 문서 및 Microsoft Word 문서	.doc, .docx, .pdf, .xls, .xlsx
이메일 메시지	내용이 전자 메일 메시지에 대해 IETF RFC에서 지정한 요구 사항(예: RFC 2822)을 준수하는 전자 메일 파일	.eml
텍스트	쉼표로 구분된 값 (CSV) 파일, 하이퍼텍스트 마크업 언어 (HTML) 파일, JavaScript 객체 표기법 (JSON) 파일, JSON 라인 파일, 일반 텍스트 문서, 탭으로 구분된 값 (TSV) 파일, 확장 가능한 마크업 언어 (XML) 파일과 같은 바이너리가 아닌 텍스트 파일	.csv, .htm, .html, .json, .jsonl, .tsv, .txt, . 및 기타(비이진 텍스트 파일 유형에 따라 다름)

Macie는 이미지, 오디오, 비디오 및 기타 유형의 멀티미디어 콘텐츠에 있는 데이터를 분석하지 않습니다.

지원되는 파일 또는 스토리지 형식을 사용하지 않는 S3 객체를 분석하도록 민감한 데이터 검색 작업을 구성하더라도 Macie는 작업 실행 시 해당 객체를 건너뜁니다. Macie는 해당 객체에서 데이터를 검색하거나 분석하려고 시도하지 않으며, 해당 객체는 분류할 수 없는 객체로 취급됩니다. 분류할 수 없는 객체란 지원되는 스토리지 클래스나 지원되는 파일 또는 Amazon S3 스토리지 형식을 사용하지 않는 객체를 말합니다. Macie는 지원되는 스토리지 클래스와 지원되는 파일 또는 스토리지 형식을 사용하는 객체만 분석합니다.

마찬가지로 민감한 데이터를 자동으로 검색하도록 Macie를 구성하더라도 분류할 수 없는 객체는 선택 및 분석에 대상에 포함되지 않습니다. Macie는 지원되는 스토리지 클래스와 지원되는 파일 또는 Amazon S3 스토리지 형식을 사용하는 객체만 분석합니다.

분류할 수 없는 객체를 저장하는 S3 버킷을 식별하기 위해 S3 버킷 인벤토리를 필터링할 수 있습니다. 인벤토리의 각 버킷에는 버킷에 있는 분류할 수 없는 객체의 수와 총 스토리지 크기를 보고하는 필드가 있습니다.

Amazon Macie 조사 결과 분석

Amazon Macie는 Amazon Simple Storage Service (Amazon S3) 범용 버킷의 보안 또는 개인 정보 보호와 관련된 잠재적 정책 위반 또는 문제를 탐지하거나 S3 객체에서 민감한 데이터를 탐지할 때 결과를 생성합니다. 조사 결과는 Macie가 발견한 잠재적 문제 또는 민감한 데이터에 대한 자세한 보고서입니다. 각 조사 결과는 심각도 등급, 영향을 받는 리소스에 대한 정보, Macie가 문제 또는 데이터를 발견한 시기와 방법 같은 추가 세부 정보를 제공합니다. Macie는 정책과 민감한 데이터 조사 결과를 90일 동안 저장합니다.

조사 결과는 다음과 같은 방법으로 검토, 분석 및 관리할 수 있습니다.

Amazon Macie 콘솔

Amazon Macie 콘솔의 조사 결과 페이지에는 조사 결과가 나열되고 개별 조사 결과에 대한 세부 정보가 제공됩니다. 또한 이 페이지는 조사 결과를 그룹화, 필터링 및 정렬하고 억제 규칙을 생성 및 관리하기 위한 옵션을 제공합니다. 억제 규칙을 사용하면 조사 결과 분석을 간소화할 수 있습니다.

Amazon Macie API

Amazon Macie API를 사용하면 AWS 명령줄 도구 또는 AWS SDK를 사용하거나 HTTPS 요청을 Macie에 직접 전송하여 결과 데이터를 쿼리하고 검색할 수 있습니다. 데이터를 쿼리하려면 Amazon Macie API에 요청을 제출하고 지원되는 파라미터를 사용하여 검색하려는 조사 결과를 지정합니다. 요청을 제출한 후, Macie는 결과를 JSON 응답으로 반환합니다. 그런 다음 분석, 장기 저장 또는 보고 기능을 향상시키기 위해 결과를 다른 서비스나 애플리케이션에 전달할 수 있습니다. 자세한 내용을 알아보려면 Amazon Macie API 참조를 참조하세요.

아마존 EventBridge

모니터링 또는 이벤트 관리 시스템과 같은 다른 서비스 및 시스템과의 통합을 추가로 지원하기 위해 Macie는 조사 결과를 이벤트로 EventBridge Amazon에 게시합니다. EventBridge이전의 Amazon CloudWatch Events는 자체 애플리케이션, 서비스형 소프트웨어 (SaaS) 애플리케이션 및 Macie와 같은 애플리케이션으로부터 실시간 데이터 스트림을 전송할 수 있는 서버리스 이벤트 버스 서비스입니다. AWS 서비스 추가 자동 처리를 위해 해당 데이터를 AWS Lambda 함수, Amazon 단순 알림 서비스 주제, Amazon Kinesis 스트림과 같은 대상으로 라우팅할 수 있습니다. EventBridge 또한 를 사용하면 결과 데이터를 장기간 보존할 수 있습니다. 자세한 EventBridge 내용은 Amazon EventBridge 사용 설명서를 참조하십시오.

Macie는 새로운 결과를 얻기 EventBridge 위해 이벤트를 자동으로 게시합니다. 또한 이후에 기존 정책 조사 결과가 발생할 경우, 이벤트를 자동으로 게시합니다. 결과 데이터는 EventBridge 이

벤트로 구조화되므로 다른 서비스 및 도구를 사용하여 결과를 보다 쉽게 모니터링, 분석하고 이에 따라 조치를 취할 수 있습니다. 예를 들어 특정 유형의 새로운 검색 결과를 함수에 자동으로 보내고, AWS Lambda 함수가 데이터를 처리하여 SIEM (보안 사고 및 이벤트 관리) 시스템으로 전송하는 데 사용할 EventBridge 수 있습니다. AWS 사용자 알림을 Macie와 통합하는 경우, 이벤트를 사용하여 지정한 전송 채널을 통해 자동으로 조사 결과에 대한 알림을 받을 수도 있습니다. EventBridge 이벤트를 사용하여 결과를 모니터링하고 처리하는 방법에 대한 자세한 내용은 을 참조하십시오Amazon Macie, Amazon EventBridge와 통합.

AWS Security Hub

조직의 보안 태세에 대한 추가적이고 광범위한 분석을 위해 조사 결과를 AWS Security Hub에 게시할 수도 있습니다. Security Hub는 지원되는 보안 솔루션으로부터 AWS 서비스 AWS Partner Network 보안 데이터를 수집하여 AWS 환경 전반의 보안 상태를 포괄적으로 파악하는 서비스입니다. Security Hub를 사용하면 소속된 환경에서 보안 업계 표준 및 모범 사례를 준수하는지 확인할 수 있습니다. 에 대한 자세한 내용은 AWS Security Hub 사용 설명서를 참조하세요. Security Hub를 사용하여 조사 결과를 모니터링하고 처리하는 방법에 대한 자세한 내용은 Amazon Macie와 통합 AWS Security Hub 섹션을 참조하세요.

조사 결과 외에도, Macie는 민감한 데이터를 발견하기 위해 분석하는 S3 개체에 대한 민감한 데이터 검색 결과를 생성합니다. 민감한 데이터 검색 결과는 객체 분석에 대한 세부 정보를 기록하는 레코드입니다. Macie가 민감한 데이터를 찾지 못해서 조사 결과가 생성되지 않는 객체와 Macie가 오류나 문제로 인해 분석할 수 없는 객체가 여기에 포함됩니다. 민감한 데이터 검색 결과에는 데이터 프라이버시 및 보호 감사 또는 조사에 도움이 될 수 있는 분석 기록이 표시됩니다. 민감한 데이터 검색 결과는 Amazon Macie 콘솔이나 Amazon Macie API를 사용하여 직접 액세스할 수는 없습니다. 대신 Macie를 구성하여 결과를 S3 버킷에 저장할 수 있습니다. 그런 다음 선택적으로 해당 버킷의 결과에 액세스하고 쿼리할 수 있습니다. 결과를 저장하도록 Macie를 구성하는 방법에 대해 알아보려면 민감한 데이터 검색 결과 저장 및 유지 섹션을 참조하세요.

주제

- Amazon Macie의 조사 결과 유형
- Amazon Macie에서 샘플 조사 결과 다루기
- Amazon Macie 콘솔에서 조사 결과 검토
- Amazon Macie 조사 결과 필터링
- Amazon Macie의 조사 결과를 통한 민감한 데이터 조사
- Amazon Macie 조사 결과 안 보이게 하기
- Amazon Macie 조사 결과에 대한 심각도 점수

Amazon Macie의 조사 결과 유형

Amazon Macie는 정책 조사 결과와 민감한 데이터 조사 결과라는 두 가지 범주의 결과를 생성합니다. 정책 결과는 Amazon Simple Storage Service (Amazon S3) 범용 버킷의 보안 또는 개인 정보 보호 관련 잠재적 정책 위반 또는 문제에 대한 자세한 보고서입니다. Macie는 보안 및 액세스 제어를 위해 범용 버킷을 평가하고 모니터링하기 위한 지속적인 활동의 일환으로 정책 조사 결과를 생성합니다. 민감한 데이터 결과는 Macie가 S3 객체에서 감지한 민감한 데이터에 대한 상세 보고서입니다. Macie는 민감한 데이터 검색 작업을 실행하거나 민감한 데이터 자동 검색을 수행할 때 수행하는 활동의 일환으로 민감한 데이터 검색 결과를 생성합니다.

각 범주에는 특정 유형이 있습니다. 조사 결과 유형은 Macie가 발견한 문제의 본질이나 민감한 데이터에 대한 통찰력을 제공합니다. 조사 결과의 세부 정보에는 심각도 등급, 영향을 받는 리소스에 대한 정보, 추가 정보(예: Macie가 문제 또는 민감한 데이터를 발견한 시기와 방법)가 제공됩니다. 각 조사 결과의 심각도 및 세부 사항은 조사 결과의 유형과 특성에 따라 달라집니다.

주제

- 정책 조사 결과의 유형
- 민감한 데이터 조사 결과의 유형

> **Tip**
>
> Amazon Macie가 생성할 수 있는 다양한 범주와 유형의 조사 결과를 탐색하고 알아보기 위해 샘플 조사 결과를 생성할 수 있습니다. 샘플 조사 결과는 예제 데이터와 자리 표시자 값을 사용하여 각 조사 결과에 포함될 수 있는 정보의 종류를 보여줍니다.

정책 조사 결과의 유형

Amazon Macie는 S3 범용 버킷의 정책 또는 설정이 버킷 및 버킷 객체의 보안 또는 개인 정보 보호를 약화시키는 방식으로 변경되는 시기를 찾는 정책을 생성합니다. Macie가 이러한 변경 사항을 감지하는 방법에 대한 정보는 Macie가 Amazon S3 데이터 보안을 모니터링하는 방법을(를) 참조하십시오.

Macie는 사용자가 AWS 계정에 대해 Macie를 사용하도록 설정한 후 변경된 경우에만 정책 조사 결과를 생성합니다. 예를 들어, Macie를 활성화한 후 S3 버킷에 대한 퍼블릭 액세스 차단 설정이 비활성화된 경우 Macie는 해당 버킷에 대해 BlockPublicAccessDisabled정책:IAmuser/S3 찾기 정책을 생성합니다. Macie를 활성화했을 때 버킷에 대한 공개 액세스 차단 설정이 비활성화되었는데도 계속 비

활성화되어 있는 경우 Macie는 해당 버킷에 대해 정책:IAmuser/S3 찾기 기능을 생성하지 않습니다. BlockPublicAccessDisabled

Macie가 기존 정책 검색 결과의 후속 발생을 감지하면 Macie는 후속 조사 결과에 대한 세부 정보를 추가하고 발생 횟수를 늘려 기존 조사 결과를 업데이트합니다. Macie는 정책 조사 결과를 90일 동안 저장합니다.

Macie는 S3 범용 버킷에 대해 다음과 같은 유형의 정책 결과를 생성할 수 있습니다.

Policy:IAMUser/S3BlockPublicAccessDisabled

버킷에 대한 모든 버킷 수준 퍼블릭 액세스 차단 설정이 비활성화되었습니다. 버킷에 대한 액세스는 계정의 퍼블릭 액세스 설정 차단, 액세스 제어 목록(ACL) 및 버킷의 버킷 정책에 의해 제어됩니다.

Amazon S3 버킷에 대한 퍼블릭 액세스 설정 차단에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서의 Amazon S3 Storage에 대한 퍼블릭 액세스 차단을 참조하세요.

Policy:IAMUser/S3BucketEncryptionDisabled

버킷의 기본 암호화 설정이 Amazon S3 관리 키를 사용하여 새 객체를 자동으로 암호화하는 기본 Amazon S3 암호화 동작으로 재설정되었습니다.

2023년 1월 5일부터 Amazon S3가 Amazon S3 관리형 키를 사용한 서버 측 암호화 (SSE-S3) 를 버킷에 추가되는 객체의 암호화의 기본 수준으로 자동 적용합니다. 선택적으로 키를 사용한 서버 측 암호화 (SSE-KMS) 또는 AWS KMS 키를 사용한 이중 레이어 서버 측 암호화 (DSSE-KMS) 를 대신 사용하도록 버킷의 기본 암호화 설정을 구성할 수 있습니다. AWS KMS S3 버킷의 기본 암호화 설정 및 옵션에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서의 S3 버킷에 대한 기본 서버 측 암호화 동작 설정을 참조하세요.

Macie가 2023년 1월 5일 이전에 이러한 유형의 조사 결과를 생성한 경우 해당 조사 결과는 영향을 받는 버킷에 대해 기본 암호화 설정이 비활성화되었음을 알 수 있습니다. 즉, 버킷 설정에는 새 객체에 대한 기본 서버 측 암호화 동작이 지정되지 않았습니다. Amazon S3에서는 버킷의 기본 암호화 설정을 비활성화하는 기능을 더 이상 지원하지 않습니다.

Policy:IAMUser/S3BucketPublic

익명 사용자 또는 모든 인증 (IAM) ID를 통한 액세스를 허용하도록 버킷의 ACL 또는 버킷 정책이 변경되었습니다. AWS Identity and Access Management

S3 버킷에 대한 ACL 및 버킷 정책에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서의 Amazon S3의 ID 및 액세스 관리를 참조하세요.

Policy:IAMUser/S3BucketReplicatedExternally

복제가 활성화되고 버킷의 객체를 조직 외부 (일부가 아닌) 의 버킷으로 복제하도록 구성되었습니다. AWS 계정 조직은 Macie 초대를 통해 AWS Organizations 또는 Macie의 초대를 통해 관련 계정 그룹으로 중앙에서 관리되는 Macie 계정 집합입니다.

특정 상황에서 Macie는 객체를 외부 버킷에 복제하도록 구성되지 않은 버킷에 대해 이러한 유형의 검색 결과를 생성할 수 있습니다. AWS 계정이는 Macie가 일일 새로 고침 주기의 일부로 Amazon S3에서 버킷 및 객체 메타데이터를 검색한 후 이전 24시간 AWS 리전 동안 다른 버킷에서 대상 버킷을 생성한 경우 발생할 수 있습니다. 조사 결과를 조사하려면 먼저 인벤토리 데이터를 새로 고치는 것으로 시작합니다. 그런 다음 버킷의 세부 정보를 검토합니다. 세부 정보는 버킷이 객체를 다른 버킷에 복제하도록 구성되었는지 여부를 나타냅니다. 이렇게 하도록 버킷을 구성한 경우 세부 정보에는 대상 버킷을 소유한 각 계정의 계정 ID가 포함됩니다.

S3 버킷의 복제 설정에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서의 객체 복제를 참조하세요.

Policy:IAMUser/S3BucketSharedExternally

버킷의 ACL 또는 버킷 정책이 조직 외부 (소속이 아닌) 와 버킷을 공유할 수 있도록 변경되었습니다. AWS 계정 조직은 Macie 초대를 통해 AWS Organizations 또는 Macie 초대를 통해 관련 계정 그룹으로 중앙에서 관리되는 Macie 계정 집합입니다.

경우에 따라 Macie는 외부 AWS 계정과 공유되지 않는 버킷에 대해 이러한 유형의 조사 결과를 생성할 수 있습니다. 이는 Macie가 버킷 정책의 `Principal` 요소와 정책의 `Condition` 요소의 특정 AWS 글로벌 조건 컨텍스트 키 또는 Amazon S3 조건 키 간의 관계를 완전히 평가할 수 없는 경우 발생할 수 있습니다. 적용 가능한 조건 키는`aws:PrincipalAccount`,,,`aws:PrincipalArn`,`aws:PrincipalOrgID`,,`aws:PrincipalOrgPat` `aws:SourceIp` `aws:SourceVpc` `aws:SourceVpceaws:userid`, `s3:DataAccessPointAccount` 및 입니다. `s3:DataAccessPointArn` 버킷 정책을 검토하여 이러한 액세스가 의도적이고 안전한지 판단하는 것이 좋습니다.

S3 버킷에 대한 ACL 및 버킷 정책에 대해 알아보려면 Amazon Simple Storage Service 사용 설명서의 Amazon S3의 ID 및 액세스 관리를 참조하세요.

Policy:IAMUser/S3BucketSharedWithCloudFront

버킷의 버킷 정책은 Amazon CloudFront 원본 액세스 ID (OAI), CloudFront 원본 액세스 제어 (OAC) 또는 CloudFront OAI 및 OAC 모두와 버킷을 공유할 수 있도록 변경되었습니다. CloudFront CloudFront OAI 또는 OAC를 사용하면 사용자가 하나 이상의 지정된 배포를 통해 버킷의 객체에 액세스할 수 있습니다. CloudFront

CloudFront OAI 및 OAC에 대해 자세히 알아보려면 Amazon 개발자 안내서의 Amazon S3 오리진에 대한 액세스 제한을 참조하십시오. CloudFront

> **Note**
>
> 경우에 따라 Macie는 버킷에 대해 정책:IAmuser/S3 검색 대신 BucketSharedExternally 정책:IAmuser/S3 검색 결과를 생성합니다. BucketSharedWithCloudFront 이러한 경우는 다음과 같습니다.
>
> - 버킷은 OAI 또는 OAC 외에도 조직 외부의 AWS 계정 다른 사람과 공유됩니다. CloudFront
> - 버킷 정책은 OAI의 Amazon 리소스 이름 (ARN) 대신 표준 사용자 ID를 지정합니다. CloudFront
>
> 그러면 버킷에 대해 더 높은 심각도의 정책 조사 결과가 생성됩니다.

민감한 데이터 조사 결과의 유형

Macie는 S3 객체에서 민감한 데이터를 탐지하면 민감한 데이터를 생성하여 민감한 데이터 조사 결과를 생성합니다. 여기에는 민감한 데이터 검색 작업을 실행하거나 민감한 데이터 자동 검색을 수행할 때 Macie가 수행하는 분석이 포함됩니다.

예를 들어 민감한 데이터 검색 작업을 생성하여 실행할 때 Macie가 S3 객체에서 은행 계좌 번호를 감지하면 Macie는 해당 객체에 SensitiveData 대해:S3Object/재무 검색 결과를 생성합니다. 마찬가지로 Macie는 자동화된 민감한 데이터 검색 주기 동안 분석하는 S3 객체에서 은행 계좌 번호를 감지하면 해당 객체에 대한:S3Object/Financial 검색 결과를 생성합니다. SensitiveData

Macie는 후속 작업 실행 또는 자동화된 민감한 데이터 검색 주기 중에 동일한 S3 객체에서 민감한 데이터를 감지하면 해당 객체에 대한 새로운 민감한 데이터 조사 결과를 생성합니다. 정책 조사 결과와는 달리 민감한 데이터 조사 결과는 모두 새로운(고유한) 것으로 취급됩니다. Macie는 민감한 데이터 조사 결과를 90일 동안 저장합니다.

Macie는 S3 객체에 대해 다음과 같은 유형의 민감한 데이터 조사 결과를 생성할 수 있습니다.

SensitiveData:S3Object/Credentials

객체에는 비밀 액세스 키나 개인 키와 같은 민감한 자격 증명 데이터가 포함되어 있습니다. AWS

SensitiveData:S3Object/CustomIdentifier

객체에는 하나 이상의 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 텍스트가 포함되어 있습니다. 객체에는 두 가지 이상의 민감한 데이터 유형이 포함될 수 있습니다.

SensitiveData:S3Object/Financial

객체에는 은행 계좌 번호나 신용 카드 번호와 같은 민감한 금융 정보가 포함되어 있습니다.

SensitiveData:S3Object/Multiple

객체에는 두 가지 이상의 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 자격 증명 데이터, 금융 정보, 개인 정보 또는 텍스트의 조합을 비롯한 여러 범주의 민감한 데이터가 포함되어 있습니다.

SensitiveData:S3Object/Personal

객체에는 여권 번호나 운전면허 식별 번호와 같은 개인 식별 정보(PII), 건강 보험 또는 의료 식별 번호와 같은 개인 건강 정보(PHI) 또는 PII와 PHI의 조합 등 민감한 개인 정보가 포함되어 있습니다.

Macie가 기본 제공 기준 및 기술을 사용하여 탐지할 수 있는 민감한 데이터 유형에 대한 자세한 내용은 관리형 데이터 식별자 사용을(를) 참조하십시오. Macie에서 분석할 수 있는 S3 객체 유형에 대한 자세한 내용은 지원하는 스토리지 클래스 및 형식을(를) 참조하십시오.

Amazon Macie에서 샘플 조사 결과 다루기

Amazon Macie가 생성할 수 있는 다양한 유형의 조사 결과를 탐색하고 알아보기 위해 샘플 조사 결과를 생성할 수 있습니다. 샘플 조사 결과는 예제 데이터와 자리 표시자 값을 사용하여 각 조사 결과에 포함될 수 있는 정보의 종류를 보여줍니다.

예를 들어 Policy:IAMUser/S3BucketPublic 샘플 조사 결과에는 가상의 Amazon Simple Storage Service(S3) 버킷에 대한 세부 정보가 포함되어 있습니다. 조사 결과의 세부 정보에는 버킷의 액세스 제어 목록(ACL)을 변경하고 버킷을 공개적으로 액세스할 수 있게 한 행위자 및 작업에 대한 예제 데이터가 포함됩니다. 마찬가지로 SensitiveData:S3Object/Multiple 샘플 조사 결과에는 가상의 Microsoft Excel 통합 문서에 대한 세부 정보가 포함되어 있습니다. 조사 결과의 세부 정보에는 통합 문서에 있는 민감한 데이터의 유형 및 위치에 대한 예제 데이터가 포함됩니다.

다양한 유형의 조사 결과에 포함될 수 있는 정보를 숙지하는 것 외에도 샘플 조사 결과를 사용하여 다른 응용 프로그램, 서비스 및 시스템과의 통합을 테스트할 수 있습니다. 계정에 대한 억제 규칙에 따라 Macie는 샘플 결과를 Amazon EventBridge에 이벤트로 게시할 수 있습니다. 샘플 조사 결과의 예제 데이터를 사용하여 이러한 이벤트를 모니터링하고 처리하는 자동화된 솔루션을 개발하고 테스트할 수 있습니다. 사용자 계정의 게시 설정에 따라 Macie는 샘플 조사 결과를 AWS Security Hub에 게시할 수

도 있습니다. 즉, 샘플 조사 결과를 사용하여 Security Hub에서 Macie 조사 결과를 모니터링하고 처리하기 위한 솔루션을 개발하고 테스트할 수도 있습니다. 이러한 서비스에 결과를 게시하는 방법에 대한 자세한 내용은 결과 모니터링 및 처리을 참조하세요.

주제

- 샘플 조사 결과 생성
- 샘플 조사 결과를 검토합니다.
- 샘플 조사 결과 보이지 않기

샘플 조사 결과 생성

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 샘플 조사 결과를 생성할 수 있습니다. 콘솔을 사용하는 경우 Macie는 Macie가 지원하는 각 검색 유형에 대해 하나의 샘플 조사 결과를 자동으로 생성합니다. API를 사용하는 경우 각 유형별로 샘플을 만들거나 지정한 특정 유형에만 샘플을 만들 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 샘플 조사 결과를 생성하려면 다음 단계를 수행하세요.

샘플 조사 결과를 만들려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 샘플 조사 결과아래에서, 조사 결과 생성을 선택합니다.

API

프로그래밍 방식으로 샘플 조사 결과를 생성하려면 Amazon Macie API의 CreateSampleFindings 작업을 사용하세요. 요청을 제출할 때, 선택적으로 `findingTypes` 파라미터를 사용하여 생성할 샘플 조사 결과의 특정 유형만 지정하세요. 모든 유형의 샘플을 자동으로 생성하려면, 요청에 이 파라미터를 포함하지 마세요.

AWS Command Line Interface(AWS CLI)를 사용하여 샘플 조사 결과를 만들려면 create-sample-find 명령을 실행합니다. 모든 유형의 조사 결과에 대한 샘플을 자동으로 만들려면 `finding-types` 파라미터를 포함하지 마세요. 특정 유형의 조사 결과만 포함하는 샘플을 만들려면 이 파라미터를 포함하고 생성할 샘플 조사 결과 유형을 지정하세요. 예:

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/
Multiple" "Policy:IAMUser/S3BucketPublic"
```

여기서 *SensitiveData:S3Object/Multiple*은 생성해야 할 민감한 데이터 조사 결과의 한 유형이고 *Policy:IAMUser/S3BucketPublic*은 생성해야 할 조사 결과의 일종입니다.

이 명령이 성공적으로 실행되면 Macie는 비어 있는 응답을 반환합니다.

샘플 조사 결과를 검토합니다.

생성한 샘플 조사 결과를 쉽게 식별할 수 있도록 Macie는 각 샘플 조사 결과의 샘플 필드 값을 True로 설정합니다. 또한 영향을 받는 S3 버킷의 이름은 모든 샘플 결과에 대해 macie-sample-finding-bucket으로 동일합니다. Amazon Macie 콘솔의 조사 결과 페이지를 사용하여 샘플 조사 결과를 검토하는 경우 Macie는 각 샘플 조사 결과에 대한 조사 결과 유형 필드에 [SAMPLE] 접두사도 표시합니다.

Console

Amazon Macie 콘솔을 사용하여 샘플 조사 결과를 검토하려면 다음 단계를 따르세요.

샘플 조사 결과를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. 조사 결과 페이지에서 다음 중 하나를 수행합니다.
   - 조사 결과 유형 열에서 다음 이미지와 같이 유형이 [SAMPLE]로 시작하는 조사 결과를 찾습니다.

Severity	Finding type	Resources affected
Low	[SAMPLE] Policy:IAMUser/S3BucketEncryptionDisabled	macie-sample-finding-bucket
High	[SAMPLE] SensitiveData:S3Object/CustomIdentifier	macie-sample-finding-bucket/
Low	[SAMPLE] SensitiveData:S3Object/Personal	macie-sample-finding-bucket/
High	[SAMPLE] Policy:IAMUser/S3BucketPublic	macie-sample-finding-bucket
Medium	[SAMPLE] Policy:IAMUser/S3BucketSharedWithCloudFront	macie-sample-finding-bucket
High	[SAMPLE] Policy:IAMUser/S3BucketSharedExternally	macie-sample-finding-bucket
High	[SAMPLE] SensitiveData:S3Object/Financial	macie-sample-finding-bucket/
High	[SAMPLE] Policy:IAMUser/S3BucketReplicatedExternally	macie-sample-finding-bucket
High	[SAMPLE] SensitiveData:S3Object/Credentials	macie-sample-finding-bucket/
High	[SAMPLE] SensitiveData:S3Object/Multiple	macie-sample-finding-bucket/
High	[SAMPLE] Policy:IAMUser/S3BlockPublicAccessDisabled	macie-sample-finding-bucket

- 표 위의 필터 기준 상자를 사용하여, 표본 결과만 표시되도록 표를 필터링하세요. 이렇게 하려면 상자에 커서를 놓으세요. 나타나는 필드 목록에서 샘플을 선택합니다. True를 선택한 후 적용을 선택합니다. 그러면 테이블에 다음과 같은 필터 조건이 추가됩니다.

4. 특정 샘플 조사 결과의 세부 정보를 검토하려면 조사 결과를 선택합니다. 세부 정보 패널에 조사 결과의 정보가 표시됩니다.

하나 이상의 샘플 조사 결과의 세부 정보를 JSON 파일로 다운로드하여 저장할 수도 있습니다. 이렇게 하려면 다운로드하고 저장할 각 샘플 조사 결과의 확인란을 선택합니다. 그런 다음 조사 결과 페이지 상단의 작업 메뉴에서 내보내기(JSON)를 선택합니다. 나타나는 창에서 다운로드를 선택합니다. 조사 결과에 포함될 수 있는 JSON 필드에 대한 자세한 설명은 Amazon Macie API 참조의 조사 결과를 참조하세요.

API

샘플 조사 결과를 프로그래밍 방식으로 검토하려면 먼저 Amazon Macie API의 ListFinders 작업을 사용하여 생성한 각 샘플 조사 결과에 대한 고유 식별자(`findingId`)를 검색하세요. 그런 다음 GetFinding 작업을 사용하여 해당 검색의 세부 정보를 검색합니다.

ListFindings요청을 제출할 때 조사 결과에 샘플 조사 결과만 포함하도록 필터 기준을 지정할 수 있습니다. 이렇게 하려면 `sample` 필드 값이 `true`인 곳에 필터 조건을 추가하세요. AWS CLI를 사용하는 경우 list-findings 명령을 실행하고 `finding-criteria` 파라미터를 사용하여 필터 조건을 지정하세요. 예:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"sample\":{\"eq\":
[\"true\"]}}}
```

요청이 성공하면 Macie는 `findingIds` 배열을 반환합니다. 배열에는 현재 AWS 리전 계정에서 찾은 각 샘플의 고유 식별자가 나열됩니다.

그런 다음 샘플 조사 결과의 세부 정보를 검색하려면, GetFindings 요청 시 또는 AWS CLI에 대해, get-findings 명령을 실행할 때 이러한 고유 식별자를 지정하세요.

샘플 조사 결과 보이지 않기

다른 조사 결과와 마찬가지로, Macie는 샘플 조사 결과를 90일 동안 저장합니다. 샘플 검토 및 실험을 마친 후에는 선택적으로 억제 규칙을 생성하여 샘플을 보관할 수 있습니다. 이렇게 하면 샘플 조사 결과가 콘솔에 기본적으로 표시되지 않고 상태가 보관됨으로 변경됩니다.

Amazon Macie 콘솔을 사용하여 샘플 조사 결과를 보관하려면 Sample 필드 값이 True인 조사 결과를 보관하도록 규칙을 구성하세요. Amazon Macie API를 사용하여 샘플 조사 결과를 보관하려면 `sample` 필드 값이 `true`이 있는 위치에 결과를 보관하도록 규칙을 구성하세요.

Amazon Macie 콘솔에서 조사 결과 검토

Amazon Macie는 AWS 환경을 모니터링하고 Amazon Simple Storage Service (Amazon S3) 범용 버킷의 보안 또는 개인 정보 보호와 관련된 잠재적 정책 위반 또는 문제가 감지되면 정책 결과를 생성합니다. Macie는 S3 객체에서 민감한 데이터를 탐지하면 민감한 데이터 조사 결과를 생성합니다. Macie는 정책과 민감한 데이터 조사 결과를 90일 동안 저장합니다.

각 조사 결과는 조사 결과 유형 및 심각도 등급을 지정합니다. 추가 세부 정보에는 영향을 받는 리소스에 대한 정보, Macie가 문제를 발견한 시기와 방법 또는 조사 결과로 보고된 민감한 데이터에 대한 정보가 포함됩니다. 각 조사 결과의 심각도 및 세부 사항은 조사 결과의 유형과 특성에 따라 달라집니다.

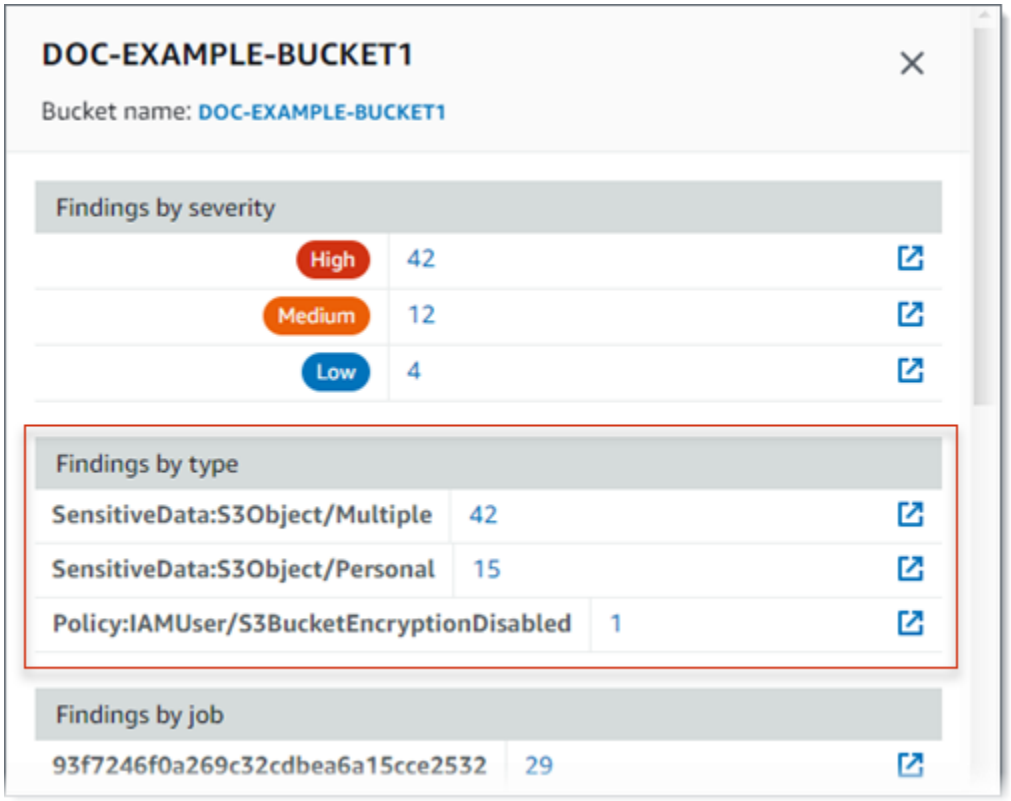
Amazon Macie 콘솔을 사용하면 조사 결과를 검토 및 분석하고 개별 조사 결과의 세부 정보에 액세스할 수 있습니다. 하나 이상의 조사 결과를 JSON 파일로 내보낼 수도 있습니다. 분석을 간소화하는 데

도움이 되도록 콘솔은 조사 결과에 대한 사용자 지정 보기를 구축할 수 있는 몇 가지 옵션을 제공합니다.

사전 정의된 그룹화 사용

특정 페이지를 사용하여 영향을 받는 S3 버킷, 조사 결과 유형 또는 민감한 데이터 검색 작업과 같은 기준별로 그룹화된 조사 결과를 검토할 수 있습니다. 이 페이지에서는 심각도별 조사 결과 수와 같은 각 그룹에 대한 집계된 통계를 검토할 수 있습니다. 또한 드릴다운하여 그룹 내 개별 조사 결과의 세부 정보를 검토하고 필터를 적용하여 분석을 세분화할 수 있습니다.

예를 들어 모든 조사 결과를 S3 버킷별로 그룹화하고 특정 버킷에 정책 위반이 있음을 확인하면 해당 버킷에 대한 민감한 데이터 조사 결과도 있는지 빠르게 확인할 수 있습니다. 이렇게 하려면 탐색 창(조사 결과 아래)에서 버킷별을 선택한 다음 버킷을 선택합니다. 표시되는 세부 정보 패널의 유형별 조사 결과 섹션에는 다음 이미지와 같이 버킷에 적용되는 조사 결과 유형이 나열됩니다.



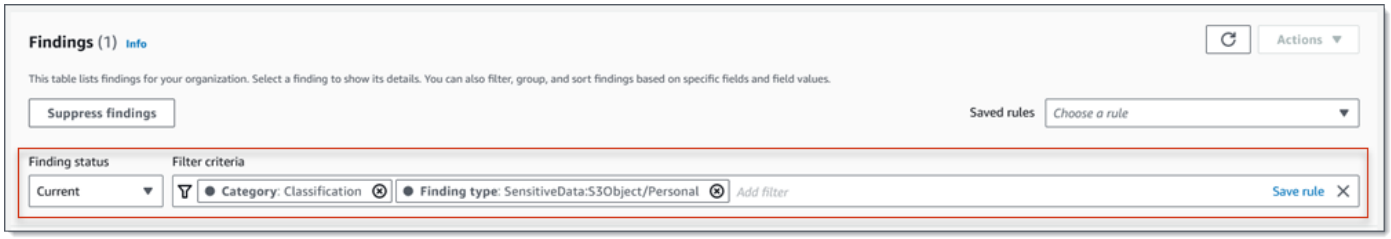
특정 유형을 조사하려면 해당 유형의 번호를 선택하세요. Macie는 선택한 유형과 일치하고 S3 버킷에 적용되는 모든 결과를 표로 표시합니다. 결과를 구체화하려면 테이블을 필터링하세요.

필터 생성 및 적용

특정 찾기 속성을 사용하여 조사 결과 테이블에 특정 조사 결과를 포함하거나 제외할 수 있습니다. 조사 결과 속성은 유형, 심각도 또는 영향을 받는 S3 버킷의 이름과 같은 조사 결과에 대한 특정 데

이터를 저장하는 필드입니다. 테이블을 필터링하면 특정 특징이 있는 조사 결과를 더 쉽게 식별할 수 있습니다. 그런 다음 드릴다운하여 해당 조사 결과의 세부 정보를 검토할 수 있습니다.

예를 들어, 민감한 데이터 조사 결과를 모두 검토하려면 범주 필드에 필터 기준을 추가하세요. 결과를 세분화하고 특정 유형의 민감한 데이터 조사 결과만 포함하려면 조사 결과 유형 필드에 필터 기준을 추가하세요. 예:



그런 다음 특정 조사 결과에 대한 세부 정보를 검토하려면 해당 결과를 선택합니다. 세부 정보 패널에 조사 결과의 정보가 표시됩니다.

조사 결과를 특정 필드를 기준으로 오름차순 또는 내림차순으로 정렬할 수도 있습니다. 이렇게 하려면 필드의 열 제목을 선택합니다. 정렬 순서를 변경하려면 열 제목을 다시 선택합니다.

콘솔에서 조사 결과를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다. 조사 결과 페이지에는 Macie가 지난 90일 AWS 리전 동안 현재 계정에 대해 생성하거나 업데이트한 결과가 표시됩니다. 기본적으로 억제 규칙에 의해 안 보이게 된 조사 결과는 여기 포함되지 않습니다.
3. 미리 정의된 논리 그룹을 기준으로 피벗하여 결과를 검토하려면 탐색창(조사 결과 아래)에서 버킷별, 유형별 또는 작업별을 선택합니다. 그런 다음 표에서 항목을 선택합니다. 디테일 패널에서 피벗할 필드의 링크를 선택합니다.
4. 조사 결과를 특정 기준으로 필터링하려면 표 위의 필터 옵션을 사용하세요.

   - 억제 규칙에 의해 억제된 조사 결과를 표시하려면 조사 결과 상태 메뉴를 사용하세요. 억제된 조사 결과와 억제되지 않은 조사 결과를 모두 표시하려면 모두를 선택하고, 억제된 조사 결과만 표시하려면 보관됨을 선택합니다. 그런 다음 억제된 조사 결과를 다시 숨기려면 현재를 선택합니다.
   - 특정 속성을 가진 조사 결과만 표시하려면 필터 기준 상자를 사용하세요. 상자에 커서를 놓고 속성에 대한 필터 조건을 추가합니다. 결과를 더 구체화하려면 추가 속성에 대한 조건을 추가하세요. 그런 다음 조건을 제거하려면 제거할 조건의 조건 제거 아이콘

( ) 을 선택합니다.

조사 결과 필터링에 대한 자세한 내용은 조사 결과에 필터 생성 및 적용 섹션을 참조하세요.

5. 검색 결과를 특정 필드별로 정렬하려면 해당 필드의 열 제목을 선택합니다. 정렬 순서를 변경하려면 열 제목을 다시 선택합니다.
6. 특정 조사 결과의 세부 정보를 검토하려면 조사 결과를 선택합니다. 세부 정보 패널에 조사 결과의 정보가 표시됩니다.

> **Tip**
>
> 세부 정보 패널을 사용하여 특정 필드를 피벗하고 드릴다운할 수 있습니다.
>
> 
>
> 필드에 대해 동일한 값을 가진 조사 결과를 표시하려면 해당 필드를 선택하세요. 또는 필드에 다른 값이 있는 조사 결과를 표시하도록  를 선택할 수도 있습니다.
>
> 민감한 데이터 조사 결과의 경우 세부 정보 패널을 사용하여 Macie가 영향을 받는 S3 객체에서 발견한 민감한 데이터를 조사할 수도 있습니다.
>
> - 특정 유형의 민감한 데이터가 발생한 위치를 찾으려면 필드에서 해당 유형의 데이터에 대한 숫자 링크를 선택하세요. Macie는 Macie가 데이터를 찾은 위치에 대한 정보(JSON 형식)를 표시합니다. 자세한 정보는 민감한 데이터 위치 찾기을 참조하세요.
> - Macie가 찾은 민감한 데이터의 샘플을 검색하려면 샘플 공개 필드에서 검토를 선택합니다. 자세한 정보는 민감한 데이터 샘플 검색을 참조하세요.
> - 해당하는 민감한 데이터 조사 결과를 탐색하려면 세부 결과 위치 필드에서 링크를 선택하세요. Macie는 Amazon S3 콘솔을 열고 조사 결과가 포함된 파일 또는 폴더를 표시합니다. 자세한 정보는 민감한 데이터 검색 결과 저장 및 유지을 참조하세요.

하나 이상의 조사 결과의 세부 정보를 JSON 파일로 다운로드하여 저장할 수도 있습니다. 이렇게 하려면 다운로드하고 저장할 각 조사 결과의 확인란을 선택합니다. 그런 다음 조사 결과 페이지 상단의 작업 메뉴에서 내보내기(JSON)를 선택합니다. 나타나는 창에서 다운로드를 선택합니다. 조사 결과에 포함될 수 있는 JSON 필드에 대한 자세한 설명은 Amazon Macie API 참조의 조사 결과를 참조하세요.

Amazon Macie 조사 결과 필터링

표적 분석을 수행하고 조사 결과를 보다 효율적으로 분석하기 위해 Amazon Macie 조사 결과를 필터링할 수 있습니다. 필터를 사용하면 조사 결과에 대한 사용자 정의 보기 및 쿼리를 작성하여 특정 특징이 있는 조사 결과를 식별하고 이에 초점을 맞추는 데 도움이 될 수 있습니다. Amazon Macie 콘솔을 사용하여 조사 결과를 필터링하거나 Amazon Macie API를 사용하여 프로그래밍 방식으로 쿼리를 제출합니다.

필터를 생성할 때는 특정 조사 결과 속성을 사용하여 보기 또는 쿼리 결과에서 조사 결과를 포함하거나 제외하는 기준을 정의합니다. 조사 결과 속성은 심각도, 유형 또는 조사 결과가 적용되는 S3 버킷의 이름과 같이 조사 결과에 대한 특정 데이터를 저장하는 필드입니다.

Macie에서 필터는 하나 이상의 조건으로 구성됩니다. 기준이라고도 하는 각 조건은 다음과 같은 세 부분으로 구성됩니다.

- 심각도또는 검색 유형과 같은 속성 기반 필드
- equals 또는 not equals와 같은 연산자.
- 하나 이상의 값. 값의 유형과 개수는 선택한 필드와 연산자에 따라 달라집니다.

다시 사용하려는 필터를 생성하는 경우, 해당 내용을 필터 규칙으로 저장할 수 있습니다. 필터 규칙은 Amazon Macie 콘솔에서 조사 결과를 검토할 때 다시 적용하기 위해 생성하고 저장하는 필터 기준 세트입니다.

필터를 금지 규칙으로 저장할 수도 있습니다. 안 보이게 하기 규칙은 규칙의 기준과 일치하는 조사 결과를 자동으로 보관하기 위해 생성하고 저장하는 일련의 필터 기준의 집합입니다. 금지 규칙 작성에 대해 알아보려면 조사 결과 안 보이게 하기(을)를 참조하세요.

주제

조사 결과 필터링의 기초

필터를 생성할 때는 다음 기능과 지침을 주의하세요. 또한 필터링된 결과는 이전 90일 및 현재 AWS 리전(으)로 제한된다는 점에 유의하세요. Amazon Macie는 AWS 리전마다 조사 결과를 90일 동안 저장합니다.

주제

필터에서 다수의 조건 사용

필터에는 조건을 하나 이상 포함할 수 있습니다. 기준이라고도 하는 각 조건은 다음과 같은 세 부분으로 구성됩니다.

- 심각도또는 검색 유형과 같은 속성 기반 필드 사용할 수 있는 필드 목록은 조사 결과 필터링 필드(을)를 참조하세요.
- equals 또는 not equals와 같은 연산자. 사용할 수 있는 연산자 목록은 조건에서·연산자 사용(을)를 참조하세요.
- 하나 이상의 값. 값의 유형과 개수는 선택한 필드와 연산자에 따라 달라집니다.

필터에 여러 개의 조건이 있으면 Macie는 AND 로직을 사용하여 조건을 결합하고 필터 기준을 평가합니다. 즉, 조사 결과는 필터의 모든 조건과 일치하는 경우에만 필터 기준과 일치합니다.

예를 들어, 높은 심각도의 조사 결과만 포함하도록 조건을 추가하고 민감한 데이터 조사 결과만 포함하도록 다른 조건을 추가하면 Macie는 높은 심각도의 민감한 데이터 조사 결과를 모두 반환합니다. 즉, Macie는 모든 정책 조사 결과와 중간 심각도 및 낮은 심각도의 민감한 데이터 조사 결과를 모두 제외합니다.

필터는 한 번만 필드를 사용할 수 있습니다. 그러나, 다수의 필드에 다수의 값을 지정할 수 있습니다.

예를 들어, 어떤 조건에서 심각도 필드를 사용하여 높은 심각도의 조사 결과만 포함하는 경우 다른 조건의 심각도 필드를 사용하여 중간 심각도 또는 낮은 심각도의 조사 결과를 포함할 수 없습니다. 대신 기존 조건에 여러 값을 지정하거나 기존 조건에 다른 연산자를 사용하세요. 예를 들어, 중간 심각도 또

는 높은 심각도의 조사 결과를 모두 포함하려면 심각도가 중간, 높음 상태와 같음 조건을 추가하거나 심각도가 낮음 상태와 같지 않음 조건을 추가합니다.

필드 값 지정

필드 값을 지정할 때, 값은 필드의 기본 데이터 유형을 준수해야 합니다. 필드에 따라 다음 유형의 값 중 하나를 지정할 수 있습니다.

텍스트 배열(문자열)

필드의 텍스트(문자열) 값 목록을 지정합니다. 각 문자열은 필드의 사전 정의된 값 또는 기존 값과 상관 관계가 있습니다. 예를 들어, 심각도 필드의 경우 높음, 찾기 유형 필드의 경우 SensitiveData:S3Object/Financial, S3 버킷 이름 필드의 경우 S3 버킷 이름과 상호 연관됩니다.

배열을 사용하는 경우 다음 사항에 유의하세요.

- 값은 대소문자를 구분합니다.
- 부분 값을 지정하거나 값의 와일드카드 문자를 사용할 수 없습니다. 이러한 필드에 대해 완전하고 유효한 값을 지정해야 합니다.

예를 들어, my-S3-bucket이라는 이름의 S3 버킷에 대한 조사 결과를 필터링하려면 S3 버킷 이름 필드에 값으로 **`my-S3-bucket`**를 입력합니다. **`my-s3-bucket`** 또는 **`my-S3`**와 같은 다른 값을 입력하면 Macie는 버킷에 대한 조사 결과를 반환하지 않습니다.

각 필드의 유효한 값 목록은 조사 결과 필터링 필드(을)를 참조하세요.

배열에 최대 50개의 값을 지정할 수 있습니다. 값을 지정하는 방법은 필드에 대한 여러 값 지정에서 설명한 대로 Amazon Macie 콘솔을 사용하는지 아니면 Amazon Macie API를 사용하는지에 따라 다릅니다.

부울

필드에 대해 상호 배타적인 두 값 중 하나를 지정합니다.

Amazon Macie 콘솔을 사용하여 이 유형의 값을 지정하는 경우 콘솔은 선택할 수 있는 값 목록을 제공합니다. Amazon Macie API를 사용하는 경우 값에 `true` 또는 `false` 를 지정하세요.

날짜/시간(및 시간 범위)

필드의 절대 날짜 및 시간을 지정합니다. 이 유형의 값을 지정하는 경우 날짜와 시간을 모두 지정해야 합니다.

Amazon Macie 콘솔에서 날짜 및 시간 값은 현지 시간대를 기준으로 하며 24시간 표기법을 사용합니다. 다른 모든 상황에서는 이러한 값이 협정 세계시(UTC) 및 확장 ISO 8601 형식으로 표시됩니다(예: `2020-09-01T14:31:13Z` 2020년 9월 1일 오후 2:31:13 UTC).

필드에 날짜/시간 값이 저장되는 경우 필드를 사용하여 고정 또는 상대 시간 범위를 정의할 수 있습니다. 예를 들어, 두 특정 날짜와 시간 사이에 생성된 해당 조사 결과만 포함하거나 특정 날짜 및 시간 이전 또는 이후에 생성된 해당 조사 결과만 포함할 수 있습니다. 시간 범위를 정의하고 적용하는 방법은 Amazon Macie 콘솔을 사용하는지 아니면 Amazon Macie API를 사용하는지에 따라 다릅니다.

- 콘솔에서 날짜 선택기를 사용하거나 시작 및 종료 상자에 직접 텍스트를 입력합니다.
- API를 사용하여 범위의 첫 번째 날짜 및 시간을 지정하는 조건을 추가하여 고정 시간 범위를 정의하고 범위의 마지막 날짜 및 시간을 지정하는 다른 조건을 추가합니다. 이렇게 하면 Macie는 AND 로직을 사용하여 조건을 결합합니다. 상대 시간 범위를 정의하려면 범위의 첫 번째 또는 마지막 날짜와 시간을 지정하는 조건을 하나 추가하세요. 값을 밀리초 단위의 Unix 타임스탬프로 지정합니다(예: 2020년 11월 5일 22:49:32 UTC의 경우 `1604616572653`).

콘솔에서는 시간 범위가 포함됩니다. API를 사용하면 선택하는 연산자에 따라 시간 범위를 포함하거나 제외할 수 있습니다.

숫자(및 숫자 범위)

필드에 긴 정수를 지정합니다.

필드에 숫자 값이 저장되는 경우 필드를 사용하여 고정 또는 상대 숫자 범위를 정의할 수 있습니다. 예를 들어, S3 객체에서 50~90건의 민감한 데이터를 보고하는 해당 조사 결과만 포함할 수 있습니다. 필터·조건을 정의하고·적용하는 방법은 Amazon Macie 콘솔을 사용하는지 아니면 Amazon Macie API를 사용하는지에 따라 다릅니다.

- 콘솔에서 시작 및 종료 상자를 사용하여 범위의 가장 낮은 숫자와 가장 높은 숫자를 각각 입력합니다.
- API를 사용하여 범위에서 가장 낮은 숫자를 지정하는 조건을 추가하여 고정된 숫자 범위를 정의하고 범위에서 가장 높은 숫자를 지정하는 다른 조건을 추가합니다. 이렇게 하면 Macie는 AND 로직을 사용하여 조건을 결합합니다. 상대적 숫자 범위를 정의하려면 범위에서 가장 낮거나 가장 높은 숫자를 지정하는 조건을 하나 추가하세요.

콘솔에서는 숫자 범위가 포함됩니다. API를 사용하면 선택하는 연산자에 따라 숫자 범위를 포함하거나 제외할 수 있습니다.

텍스트(문자열)

필드의 단일 텍스트(문자열) 값을 지정합니다. 문자열은 필드의 사전 정의된 값 또는 기존 값과 상관 관계가 있습니다. 예를 들어, 심각도 필드에 대한 높음, S3 버킷 이름 필드에 대한 S3 버킷의 이름, 또는 작업 ID 필드에 대한 민감한 데이터 검색 작업의 고유 식별자 등이 있습니다.

단일 텍스트 문자열을 지정하는 경우, 다음을 유의하세요.

- 값은 대소문자를 구분합니다.
- 값에 부분 값이나 와일드카드 문자를 사용할 수 없습니다. 이러한 필드에 대해 완전하고 유효한 값을 지정해야 합니다.

예를 들어, my-S3-bucket이라는 이름의 S3 버킷에 대한 조사 결과를 필터링하려면 S3 버킷 이름 필드에 값으로 **`my-S3-bucket`**를 입력합니다. **`my-s3-bucket`** 또는 **`my-S3`**와 같은 다른 값을 입력하면 Macie는 버킷에 대한 조사 결과를 반환하지 않습니다.

각 필드의 유효한 값 목록은 조사 결과 필터링 필드(을)를 참조하세요.

필드에 대한 여러 값 지정

특정 필드와 연산자를 사용하여 필드에 대한 여러 값을 지정할 수 있습니다. 이렇게 하면 Macie는 OR 로직을 사용하여 값을 결합하고 필터 기준을 평가합니다. 즉, 해당 필드에 대한 값이 하나라도 있으면 조사 결과가 해당 기준과 일치한다는 뜻입니다.

예를 들어, 조사 결과 유형 필드의 값이 SensitiveData:S3Object/Financial, SensitiveData:S3Object/Personal과 같은 조사 결과를 포함하도록 조건을 추가하면, Macie는 재무 정보만 포함된 S3 객체와 개인 정보만 포함된 S3 객체에 대한 민감한 데이터 조사 결과를 반환합니다. 즉, Macie는 모든 정책 조사 결과를 제외합니다. 또한 Macie는 다른 유형의 민감한 데이터나 여러 유형의 민감한 데이터가 포함된 객체에 대한 모든 민감한 데이터 조사 결과를 제외합니다.

예외사항은 eqExactMatch 연산자를 사용하는 조건입니다. 이 연산자의 경우, Macie는 AND 로직을 사용하여 값을 결합하고 필터 기준을 평가합니다. 즉, 해당 필드에 대한 모든 값과 필드에 대해 오직 해당 값만 포함하는 경우에만 조사 결과가 기준과 일치합니다. 이 연산자에 대해 자세히 알아보려면 조건에서·연산자 사용(을)를 참조하세요.

필드에 여러 값을 지정하는 방법은 Amazon Macie API를 사용하는지, Amazon Macie 콘솔을 사용하는지에 따라 다릅니다. API를 사용할 경우, 사용자는 값을 나열하는 배열을 사용합니다.

콘솔에서는 사용자가 일반적으로 목록에서 값을 선택합니다. 하지만, 일부 필드의 경우 각 값에 고유한 조건을 추가해야 합니다. 예를 들어, Macie가 특정 사용자 정의 데이터 식별자를 사용하여 탐지한 데이터에 대한 조사 결과를 포함하려면 다음과 같이 하세요.

1. 필터 기준 상자에 커서를 놓고 사용자 정의 데이터 식별자 이름 필드를 선택합니다. 사용자 정의 데이터 식별자의 이름을 입력한 다음 적용을 선택합니다.
2. 필터에 지정하려는 각 추가 사용자 정의 데이터 식별자에 대해 이전 단계를 반복합니다.

이 작업을 수행해야 하는 필드 목록은 조사 결과 필터링 필드(을)를 참조하세요.

조건에서·연산자 사용

개별 조건에서 다음과 같은 유형의 연산자를 사용할 수 있습니다.

같음(eq)

필드에 지정된 모든 값과 일치합니다(=). 텍스트 배열(문자열), 부울, 날짜/시간, 숫자, 텍스트(문자열) 등의 값 유형에는 같음 연산자를 사용할 수 있습니다.

대부분의 필드에서 이 연산자를 사용하여 필드에 최대 50개의 값을 지정할 수 있습니다. 이렇게 하면 Macie는 OR 로직을 사용하여 값을 결합합니다. 즉, 필드에 지정된 값 중 어느 하나라도 있는 경우 조사 결과가 기준과 일치합니다.

예:

- 재무 정보, 개인 정보 또는 금융 정보와 개인 정보 모두의 발생을 보고하는 조사 결과를 포함하려면 민감한 데이터 범주 필드와 이 연산자를 사용하는 조건을 추가하고 금융 정보와 개인 정보를 필드 값으로 지정하세요.
- 신용 카드 번호, 우편 주소 또는 신용 카드 번호와 우편 주소 모두의 발생을 보고하는 조사 결과를 포함하려면, 민감한 데이터 검색 유형 필드에 대한 조건을 추가하고, 이 연산자를 사용한 다음, 필드에 대한 값으로 CREDIT_CARD_NUMBER 및 ADDRESS(을)를 지정합니다.

Amazon Macie API를 사용하여 이 연산자를 날짜/시간 값과 함께 사용하는 조건을 정의하는 경우 값을 밀리초 단위의 Unix 타임스탬프로 지정하세요(예: 2020년 11월 5일 22:49:32 UTC의 경우 1604616572653).

정확히 일치하는 항목(eqExactMatch)과 같음

필드에 지정된 모든 값을 배타적으로 일치시킵니다. 선택한 필드 세트를 사용해 정확히 일치하는 항목과 같음 연산자를 사용할 수 있습니다.

이 연산자를 사용하고 필드에 여러 값을 지정하는 경우 Macie는 AND 로직을 사용하여 값을 결합합니다. 즉, 필드에 지정된 모든 값과 오직 필드에 대한 해당 값만 있는 경우에만 조사 결과가 기준과 일치합니다. 필드에 최대 50개의 값을 지정할 수 있습니다.

예:

- 신용 카드 번호 발생 및 다른 유형의 민감한 데이터가 없음을 보고하는 조사 결과를 포함하려면, 민감한 데이터 탐지 유형 필드에 대한 조건을 추가하고, 이 연산자를 사용한 다음, 필드에 대한 유일한 값으로 CREDIT_CARD_NUMBER(을)를 지정하세요.
- 신용 카드 번호와 우편 주소(다른 유형의 민감한 데이터는 제외됨)가 모두 발생했다고 보고하는 조사 결과를 포함하려면, 민감한 데이터 탐지 유형 필드에 조건을 추가하고, 이 연산자를 사용한 다음, 필드에 대한 값으로 CREDIT_CARD_NUMBER 및 ADDRESS(을)를 지정합니다.

Macie는 AND 로직을 사용하여 필드 값을 결합하므로 동일한 필드에 대해 이 연산자를 다른 연산자와 조합하여 사용할 수 없습니다. 즉, 한 조건의 필드를 포함하는 정확히 일치하는 항목과 같음 연산자를 사용하는 경우, 동일한 필드를 사용하는 다른 모든 조건에서도 이 연산자를 사용해야 합니다.

다른 연산자와 마찬가지로, 필터에 있는 두 가지 이상의 조건에서 정확히 일치하는 항목과 같음 연산자를 사용할 수 있습니다. 이렇게 하면 Macie는 AND 로직을 사용하여 조건을 결합하고 필터를 평가합니다. 즉, 필터의 모든 조건을 통해 지정된 모든 값이 있는 경우에만 조사 결과가 필터 기준과 일치합니다.

예를 들어, 특정 시간 이후에 생성된 조사 결과를 포함시키고, 신용 카드 번호 발생 횟수는 보고하고, 다른 유형의 민감한 데이터는 보고하지 않으려면 다음과 같이 하세요.

1. 생성 시간 필드를 사용하고, 보다 큼 연산자를 사용하고, 필터 시작 날짜 및 시간을 지정하는 조건을 추가합니다.
2. 민감한 데이터 검색 유형 필드를 사용하고, 정확히 일치하는 항목과 같음 연산자를 사용하고, 필드의 유일한 값으로 CREDIT_CARD_NUMBER(을)를 지정하는 다른 조건을 추가합니다.

다음 필드를 통해 정확히 일치하는 항목과 같음 연산자를 사용할 수 있습니다.

- 사용자 정의 데이터 식별자 ID(`customDataIdentifiers.detections.arn`)
- 사용자 정의 데이터 식별자 이름(`customDataIdentifiers.detections.name`)
- S3 버킷 태그 키(`resourcesAffected.s3Bucket.tags.key`)
- S3 버킷 태그 값(`resourcesAffected.s3Bucket.tags.value`)
- S3 객체 태그 키(`resourcesAffected.s3Object.tags.key`)
- S3 객체 태그 값(`resourcesAffected.s3Object.tags.value`)
- 민감한 데이터 탐지 유형(`sensitiveData.detections.type`)
- 민감한 데이터 범주(`sensitiveData.category`)

위 목록에서, 괄호 안의 이름은 점 표기법을 사용하여 조사 결과 및 Amazon Macie API를 JSON으로 표현한 필드 이름을 나타냅니다.

보다 큼(gt)

필드에 지정된 값보다 큽니다(>). 숫자 및 날짜/시간 값과 함께 보다 큼 연산자를 사용할 수 있습니다.

예를 들어, S3 객체에서 민감한 데이터가 90회를 초과해 발생했다고 보고하는 해당 조사 결과만 포함하려면 민감한 데이터 총 개수 필드와 이 연산자를 사용하는 조건을 추가하고 필드 값으로 90을 지정하세요. Amazon Macie 콘솔에서 이 작업을 수행하려면 시작 상자에 **91**(을)를 입력하고 종료 상자에는 값을 입력하지 않고, 적용을 선택합니다. 콘솔에는 숫자 및 시간 기반 비교내용이 포함됩니다.

Amazon Macie API를 사용하여 이 연산자를 사용하는 시간 범위를 정의하는 경우 날짜/시간 값을 밀리초 단위의 Unix 타임스탬프로 지정해야 합니다(예: 2020년 11월 5일 22:49:32 UTC의 경우 1604616572653).

보다 크거나 같음(gte)

필드에 지정된 값보다 크거나 이와 같습니다(>=). 숫자 및 날짜/시간 값과 함께 보다 크거나 같음 연산자를 사용할 수 있습니다.

예를 들어, S3 객체에서 민감한 데이터가 90회 이상 발생했다고 보고하는 해당 조사 결과만 포함하려면 민감한 데이터 총 개수 필드와 이 연산자를 사용하는 조건을 추가하고 필드 값으로 90을 지정하세요. Amazon Macie 콘솔에서 이 작업을 수행하려면 시작 상자에 **90**(을)를 입력하고 종료 상자에는 값을 입력하지 않고, 적용을 선택합니다.

Amazon Macie API를 사용하여 이 연산자를 사용하는 시간 범위를 정의하는 경우 날짜/시간 값을 밀리초 단위의 Unix 타임스탬프로 지정해야 합니다(예: 2020년 11월 5일 22:49:32 UTC의 경우 1604616572653).

보다 작음(lt)

필드에 지정된 값보다 작습니다(<). 숫자 및 날짜/시간 값과 함께 보다 작음 연산자를 사용할 수 있습니다.

예를 들어, S3 객체에서 민감한 데이터가 90회 미만 발생했다고 보고하는 해당 조사 결과만 포함하려면 민감한 데이터 총 개수 필드와 이 연산자를 사용하는 조건을 추가하고 필드 값으로 90을 지정하세요. Amazon Macie 콘솔에서 이 작업을 수행하려면 종료 상자에 **89**(을)를 입력하고 시작 상자에는 값을 입력하지 않고, 적용을 선택합니다. 콘솔에는 숫자 및 시간 기반 비교내용이 포함됩니다.

Amazon Macie API를 사용하여 이 연산자를 사용하는 시간 범위를 정의하는 경우 날짜/시간 값을 밀리초 단위의 Unix 타임스탬프로 지정해야 합니다(예: 2020년 11월 5일 22:49:32 UTC의 경우 1604616572653).

보다 작거나 같음(lte)

필드에 지정된 값과 같보다 작거나 이와 같습니다(<=). 숫자 및 날짜/시간 값과 함께 보다 작거나 같음 연산자를 사용할 수 있습니다.

예를 들어, S3 객체에서 민감한 데이터가 90회 이하로 발생했다고 보고하는 해당 조사 결과만 포함하려면 민감한 데이터 총 개수 필드와 이 연산자를 사용하는 조건을 추가하고 필드 값으로 90을 지정하세요. Amazon Macie 콘솔에서 이 작업을 수행하려면 종료 상자에 **90**(을)를 입력하고 시작 상자에는 값을 입력하지 않고, 적용을 선택합니다.

Amazon Macie API를 사용하여 이 연산자를 사용하는 시간 범위를 정의하는 경우 날짜/시간 값을 밀리초 단위의 Unix 타임스탬프로 지정해야 합니다(예: 2020년 11월 5일 22:49:32 UTC의 경우 1604616572653).

같지 않음(neq)

필드에 지정된 어떤 값과도 일치하지 않습니다(≠). 텍스트 배열(문자열), 부울, 날짜/시간, 숫자, 텍스트(문자열) 등의 값 유형에는 같지 않음 연산자를 사용할 수 있습니다.

대부분의 필드에서 이 연산자를 사용하여 필드에 최대 50개의 값을 지정할 수 있습니다. 이렇게 하면 Macie는 OR 로직을 사용하여 값을 결합합니다. 즉, 필드에 지정된 값 중 어느 하나라도 없는 경우 조사 결과가 기준과 일치합니다.

예:

- 재무 정보, 개인 정보 또는 금융 정보와 개인 정보 모두의 발생을 보고하는 조사 결과를 제외하려면 민감한 데이터 범주 필드와 이 연산자를 사용하는 조건을 추가하고 금융 정보와 개인 정보를 필드 값으로 지정하세요.
- 신용 카드 번호 발생을 보고하는 조사 결과를 포함하려면, 민감한 데이터 탐지 유형 필드에 대한 조건을 추가하고, 이 연산자를 사용한 다음, 필드에 대한 값으로 CREDIT_CARD_NUMBER(을)를 지정하세요.
- 신용 카드 번호, 우편 주소 또는 신용 카드 번호와 우편 주소 모두의 발생을 보고하는 조사 결과를 제외하려면, 민감한 데이터 검색 유형 필드에 대한 조건을 추가하고, 이 연산자를 사용한 다음, 필드에 대한 값으로 CREDIT_CARD_NUMBER 및 ADDRESS(을)를 지정합니다.

Amazon Macie API를 사용하여 이 연산자를 날짜/시간 값과 함께 사용하는 조건을 정의하는 경우 값을 밀리초 단위의 Unix 타임스탬프로 지정하세요(예: 2020년 11월 5일 22:49:32 UTC의 경우 1604616572653).

조사 결과에 필터 생성 및 적용

특정 특성을 가진 조사 결과를 식별하고 집중하기 위해 Amazon Macie 콘솔과 Amazon Macie API를 사용하여 프로그래밍 방식으로 제출하는 쿼리에서 조사 결과를 필터링할 수 있습니다. 필터를 생성할 때는 특정 조사 결과 속성을 사용하여 보기 또는 쿼리 결과에서 조사 결과를 포함하거나 제외하는 기준을 정의합니다. 조사 결과 속성은 심각도, 유형 또는 조사 결과가 적용되는 S3 버킷의 이름과 같이 조사 결과에 대한 특정 데이터를 저장하는 필드입니다.

Macie에서 필터는 하나 이상의 조건으로 구성됩니다. 기준이라고도 하는 각 조건은 다음과 같은 세 부분으로 구성됩니다.

- 심각도또는 검색 유형과 같은 속성 기반 필드
- equals 또는 not equals와 같은 연산자.
- 하나 이상의 값. 값의 유형과 개수는 선택한 필드와 연산자에 따라 달라집니다.

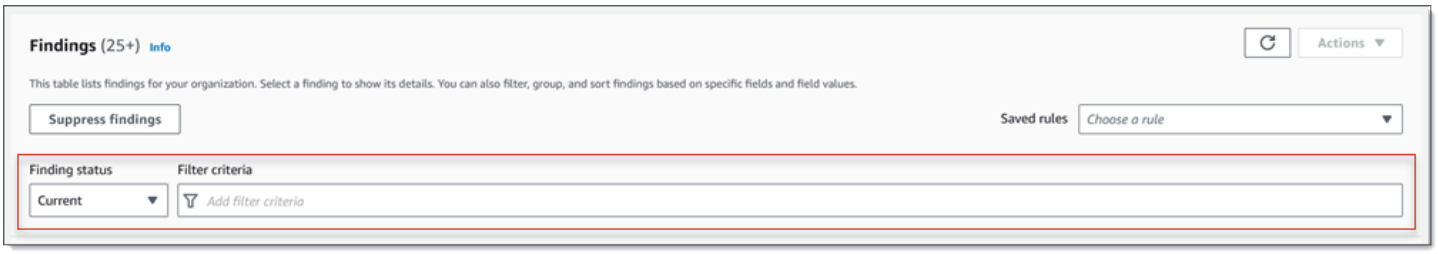
필터 조건을 정의하고 적용하는 방법은 Amazon Macie 콘솔을 사용하는지 아니면 Amazon Macie API를 사용하는지에 따라 다릅니다.

주제

- Amazon Macie 콘솔에서 조사 결과 필터링
- Amazon Macie API를 사용하여 프로그래밍 방식으로 조사 결과 필터링

Amazon Macie 콘솔에서 조사 결과 필터링

Amazon Macie 콘솔을 사용하여 조사 결과를 필터링하는 경우, Macie는 개별 조건에 대한 필드, 연산자, 값을 선택하는 데 도움이 되는 옵션을 제공합니다. 다음 이미지와 같이 조사 결과 페이지의 필터 설정을 사용하여 이러한 옵션에 액세스할 수 있습니다.



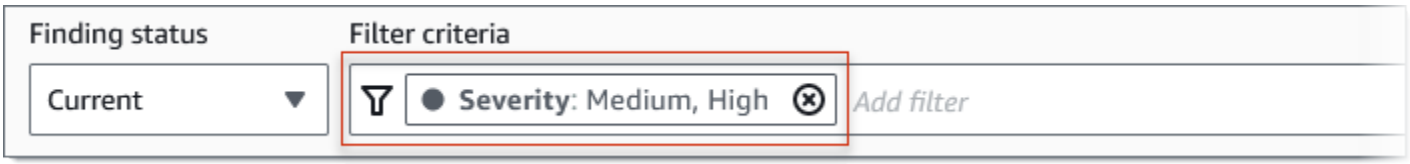
결과 상태 메뉴를 사용하여 안 보이게 하기 규칙에 의해 숨김 처리(자동 보관)된 검색 결과를 포함할지 여부를 지정할 수 있습니다. 필터 기준 상자를 사용하여 필터 조건을 입력할 수 있습니다.

필터 기준 상자에 커서를 놓으면, Macie는 필터 조건에서 사용할 수 있는 필드 목록을 표시합니다. 필드는 논리적 범주별로 구성되어 있습니다. 예를 들어, 일반 필드 범주에는 모든 유형의 조사 결과에 적용되는 필드가 포함되고, 분류 필드 범주에는 민감한 데이터 조사 결과에만 적용되는 필드가 포함됩니다. 필드는 각 범주 내에서 알파벳순으로 정렬됩니다.

조건을 추가하려면 먼저 목록에서 필드를 선택합니다. 필드를 찾으려면 전체 목록을 찾아보거나 필드 이름의 일부를 입력하여 필드 목록의 범위를 좁힙니다.

선택한 필드에 따라 Macie는 다른 옵션을 표시합니다. 옵션은 선택한 필드의 유형과 특성을 반영합니다. 예를 들어 심각도 필드를 선택하면, Macie는 낮음, 중간, 높음 중에서 선택할 수 있는 값 목록을 표시합니다. S3 버킷 이름 필드를 선택하면 Macie는 버킷 이름을 입력할 수 있는 텍스트 상자를 표시합니다. 어떤 필드를 선택하든 Macie는 필드에 필요한 설정이 포함된 조건을 추가하는 단계를 안내합니다.

조건을 추가하면, 다음 이미지와 같이 Macie는 조건에 대한 기준을 적용하고 필터 기준 상자의 필터 토큰에 조건을 추가합니다.



이 예시에서는 중간 심각도 및 높은 심각도 조사 결과를 모두 포함하고, 낮은 심각도 조사 결과는 모두 제외하도록 조건이 구성되어 있습니다. 심각도 필드의 값이 중간 또는 높음과 동일한 조사 결과를 반환합니다.

> **Tip**
>
> 대부분의 필드에서 조건의 필터 토큰에서 등호 아이콘 (●) 을 선택하여 조건의 연산자를 같음에서 같지 않음으로 변경할 수 있습니다. 이렇게 하면, Macie에서 연산자를 같지 않음으로 변경하고 토큰에 같지 않음 아이콘 (⦸) 을 표시됩니다. 같음 연산자로 다시 전환하려면 같지 않음 아이콘을 선택합니다.

조건을 더 추가하면, Macie는 조건을 적용하고 필터 기준 상자의 토큰에 조건을 추가합니다. 언제든지 상자를 참조하여 어떤 기준을 적용했는지 확인할 수 있습니다. 조건을 제거하려면 조건에 대한 토큰에서 조건 제거 아이콘

(⊗)
을 선택합니다.

콘솔을 사용하여 조사 결과를 필터링하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. (선택 사항) 먼저 미리 정의된 논리 그룹을 기준으로 피벗하여 결과를 검토하려면 패널조사 결과 아래)에서 버킷별, 유형별 또는 작업별을 선택합니다. 그런 다음 표에서 항목을 선택합니다. 디테일 패널에서 피벗할 필드의 링크를 선택합니다.
4. (선택 사항) 안 보이게 하기 규칙으로 숨김 처리된 조사 결과를 표시하려면, 상태 필터링 설정을 변경합니다. 숨김 처리된 조사 결과만 표시하려면, 보관됨을 선택하고, 숨김 처리된 결과와 숨김 처리되지 않은 결과를 모두 표시하려면 모두를 선택합니다. 안 보이게 한 조사 결과를 다시 숨기려면 현재를 선택합니다.
5. 필터 조건을 추가하려면:

   a. 필터 기준 상자에 커서를 놓고, 조건에 사용할 필드를 선택합니다. 사용할 수 있는 필드에 대한 자세한 내용은 조사 결과 필터링 필드을 참조하십시오.

   b. 필드에 적절한 유형의 값을 입력합니다. 다양한 유형의 값에 대한 자세한 내용은 필드 값 지정을 참조하십시오.

      텍스트 배열(문자열)

      이 유형의 값에 대해 Macie는 선택할 수 있는 값 목록을 제공하는 경우가 많습니다. 이 경우 조건에 사용할 각 값을 선택합니다.

      Macie에서 값 목록을 제공하지 않는 경우, 필드에 완전하고 유효한 값을 입력합니다. 필드에 추가 값을 지정하려면 적용을 선택한 다음, 각 추가 값에 대해 다른 조건을 추가합니다.

      와 는 대소문자를 구분합니다. 또한 값에 부분 값이나 와일드카드 문자를 사용할 수 없습니다. 예를 들어, my-S3-bucket이라는 이름의 S3 버킷에 대한 조사 결과를 필터링하려면 S3 버킷 이름 필드에 값으로 **`my-S3-bucket`**를 입력합니다. **`my-s3-bucket`** 또는 **`my-S3`**와 같은 다른 값을 입력하면 Macie는 버킷에 대한 조사 결과를 반환하지 않습니다.

      부울

      이 유형의 값에 대해 Macie는 선택할 수 있는 값 목록을 제공합니다. 조건에 사용할 값을 선택합니다

날짜/시간 (시간 범위)

이 유형의 값의 경우, 시작 및 종료 상자를 사용하여 포함된 시간 범위를 정의합니다.

- 고정된 시간 범위를 정의하려면, 시작 및 종료 상자를 사용하여 범위의 첫 번째 날짜 및 시간과 마지막 날짜 및 시간을 각각 지정합니다.
- 특정 날짜와 시간에 시작하여 현재 시간에 끝나는 상대적인 시간 범위를 정의하려면, 시작 상자에 시작 날짜와 시간을 입력하고 종료 상자의 모든 텍스트를 삭제합니다.
- 특정 날짜 및 시간에 종료되는 상대적 시간 범위를 정의하려면, 종료 상자에 종료 날짜 및 시간을 입력하고 시작 상자의 모든 텍스트를 삭제합니다.

참고로 시간 값은 24시간 표기법을 사용합니다. 날짜 선택기를 사용하여 날짜를 선택하는 경우, 시작 및 종료 상자에 직접 텍스트를 입력하여 값을 조정할 수 있습니다.

숫자(숫자 범위)

이 유형의 값의 경우, 시작 및 종료 상자를 사용하여 포함, 고정 또는 상대 숫자 범위를 정의하는 정수를 하나 이상 입력합니다.

텍스트(문자열) 값

이 유형의 값에는 필드에 대해 완전하고 유효한 값을 입력합니다.

와 는 대소문자를 구분합니다. 또한 값에 부분 값이나 와일드카드 문자를 사용할 수 없습니다. 예를 들어, my-S3-bucket이라는 이름의 S3 버킷에 대한 조사 결과를 필터링하려면 S3 버킷 이름 필드에 값으로 **`my-S3-bucket`**를 입력합니다. **`my-s3-bucket`** 또는 **`my-S3`**와 같은 다른 값을 입력하면 Macie는 버킷에 대한 조사 결과를 반환하지 않습니다.

c. 필드에 값을 모두 추가했으면 적용을 선택합니다. Macie는 필터 기준을 적용하고 필터 기준 상자의 필터 토큰에 조건을 추가합니다.

6. 추가하려는 각 조건에 대해 5단계를 반복합니다
7. 조건을 제거하려면 조건에 대한 토큰에서 조건 제거 아이콘 ( ) 을 선택합니다.
8. 조건을 변경하려면 조건에 대한 필터 토큰에서 조건 제거 아이콘 ( ) 을 선택하여 조건을 제거합니다. 그런 다음 5단계를 반복하여 올바른 설정이 포함된 조건을 추가합니다.

이후에 이 조건 집합을 다시 사용하려면 해당 조건 집합을 필터 규칙으로 저장하면 됩니다. 이렇게 하려면 필터 기준 상자에서 규칙 저장을 선택합니다. 규칙의 이름을 입력하고, 선택적으로 설명을 입력합니다. 마쳤으면 저장을 선택합니다.

Amazon Macie API를 사용하여 프로그래밍 방식으로 조사 결과 필터링

프로그래밍 방식으로 조사 결과를 필터링하려면 Amazon Macie API의 ListFindings 또는 GetFindingStatistics 작업을 사용하여 제출하는 쿼리에 필터 기준을 지정합니다. 이 ListFindings작업은 필터 기준과 일치하는 각 조사 결과에 대해 하나의 ID씩 조사 결과 ID 배열을 반환합니다. 이 GetFindingStatistics 작업은 필터 기준과 일치하는 모든 조사 결과에 대한 집계된 통계 데이터를 요청에서 지정한 필드별로 그룹화하여 반환합니다.

ListFindings 및 GetFindingStatistics 연산은 조사 결과를 안 보이게 하는 데 사용하는 연산과 다릅니다. 필터 기준도 지정하는 안 보이게 하는 작업과 달리, ListFindings 및 GetFindingStatistics 작업은 조사 결과 데이터만 쿼리합니다. 필터 기준과 일치하는 조사 결과에 대해서는 어떠한 작업도 수행하지 않습니다. 조사 결과를 안 보이게 하려면, Amazon Macie API의 CreateFindingsFilter 작업을 사용하면 됩니다.

쿼리에서 필터 기준을 지정하려면 요청에 필터 조건 맵을 포함합니다. 각 조건에 대해 필드, 연산자, 하나 이상의 필드 값을 지정합니다. 값의 유형과 개수는 선택한 필드와 연산자에 따라 달라집니다. 조건에 사용할 수 있는 필드, 연산자 및 값 유형에 대한 자세한 내용은 조사 결과 필터링 필드, 조건에서·연산자 사용 및 필드 값 지정 을 참조하십시오.

다음 예제는 AWS Command Line Interface(AWS CLI)를 사용하여 제출하는 쿼리에 필터 기준을 지정하는 방법을 보여줍니다. 최신 버전의 다른 AWS 명령줄 도구 또는 AWS SDK를 사용하거나 Macie에 직접 HTTPS 요청을 보냄으로써 이 작업을 수행할 수도 있습니다. AWS도구와 SDK에 대한 자세한 내용은, AWS 기반의 도구를 참조하세요.

예시

- 예 1: 심각도를 기준으로 조사 결과 필터링
- 예 2: 민감한 데이터 범주를 기준으로 조사 결과 필터링
- 예 3: 고정된 시간 범위를 기준으로 조사 결과 필터링
- 예 4: 숨김 처리 상태를 기준으로 조사 결과 필터링
- 예 5: 여러 필드 및 값 유형을 기준으로 조사 결과 필터링

이 예시에서는 list-findings 명령을 사용합니다. 예제가 성공적으로 실행되면 Macie는 `findingIds` 배열을 반환합니다. 배열에는 다음 예시와 같이 필터 기준과 일치하는 각 조사 결과의 고유 식별자가 표시됩니다.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

필터 기준과 일치하는 조사 결과가 없는 경우 Macie는 빈 `findingIds` 배열을 반환합니다.

```
{
    "findingIds": []
}
```

예 1: 심각도를 기준으로 조사 결과 필터링

이 예시에서는 list-findings 명령을 사용하여 현재 AWS 리전에서 모든 높은 심각도 및 중간 심각도 검색 결과에 대한 조사 결과 ID를 검색합니다.

Linux, macOS 또는 Unix의 경우:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

Microsoft Windows의 경우:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":
{\"severity.description\":{\"eq\":[\"High\",\"Medium\"]}}}
```

위치:

- *severity.description*은 심각도 필드의 JSON 이름을 지정합니다.
- *eq*는 등호 연산자를 지정합니다,
- *##* 및 *##*은 심각도 필드에 열거된 값의 배열입니다.

예 2: 민감한 데이터 범주를 기준으로 조사 결과 필터링

이 예시에서는 list-findings 명령을 사용하여 현재 리전에 있는 모든 민감한 데이터 조사 결과에 대한 조사 결과 ID를 검색하고 S3 객체에 있는 금융 정보(다른 민감한 데이터 범주는 제외)의 발생을 보고합니다.

Linux, macOS 또는 Unix의 경우, 가독성을 높이기 위해 백슬래시 (\) 줄 연속 문자를 사용합니다.

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

Microsoft Windows의 경우 캐럿(^) 줄 연속 문자를 사용하여 가독성을 개선합니다.

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"FINANCIAL_INFORMATION\"]}}}
```

위치:

- *classificationDetails.result.sensitiveData.category*는 민감한 데이터 범주 필드의 JSON 이름을 지정합니다.
- *eqExactMatch*는 동일 완전 일치 연산자를 지정합니다.
- *FINANCIAL_INFORMATION*은 민감한 데이터 범주 필드의 열거형 값입니다.

예 3: 고정된 시간 범위를 기준으로 조사 결과 필터링

이 예시에서는 list-findings 명령을 사용하여 현재 리전에 있고 2020년 10월 5일 07:00 UTC부터 2020년 11월 5일 07:00 UTC(포함) 사이에 생성된 모든 조사 결과에 대한 조사 결과 ID를 검색합니다.

Linux, macOS 또는 Unix의 경우:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":
{"gte":1601881200000,"lte":1604559600000}}}'
```

Microsoft Windows의 경우:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"createdAt\":
{\"gte\":1601881200000,\"lte\":1604559600000}}}
```

위치:

- *createdAt*은 생성 위치 필드의 JSON 이름을 지정합니다.
- *gte*는 크거나 같음 연산자를 지정합니다.
- *1601881200000*은 시간 범위의 첫 번째 날짜 및 시간(밀리초 단위의 유닉스 타임스탬프)입니다.
- *lte*는 작거나 같음 연산자를 지정합니다.
- *1604559600000*은 시간 범위의 마지막 날짜 및 시간(밀리초 단위의 유닉스 타임스탬프)입니다.

예 4: 숨김 처리 상태를 기준으로 조사 결과 필터링

이 예시에서는 list-findings 명령을 사용하여 현재 리전에 있고 안 보이게 하기 규칙에 의해 숨김 처리(자동 보관)된 모든 조사 결과에 대한 조사 결과 ID를 검색합니다.

Linux, macOS 또는 Unix의 경우:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":
["true"]}}}'
```

Microsoft Windows의 경우:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"archived\":{\"eq\":
[\"true\"]}}}
```

위치:

- *###*은 보관된 필드의 JSON 이름을 지정합니다.
- *eq*는 등호 연산자를 지정합니다,
- *true*는 보관된 필드의 부울 값입니다.

예 5: 여러 필드 및 값 유형을 기준으로 조사 결과 필터링

이 예시에서는 list-findings 명령을 사용하여 현재 리전에 있고 다음 기준과 일치하는 모든 민감한 데이터 조사 결과의 조사 결과 ID를 검색합니다: 2020년 10월 5일 07:00 UTC부터 2020년 11월 5일 07:00

UTC(제외) 사이에 생성, S3 객체에 있는 금융 데이터의 발생을 보고하고 그 외 다른 범주의 민감한 데이터는 제외, 안 보이게 하기 규칙에 의해 숨김 처리(자동 보관)되지 않음.

Linux, macOS 또는 Unix의 경우, 가독성을 높이기 위해 백슬래시 (\) 줄 연속 문자를 사용합니다.

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":1601881200000,"lt":1604559600000},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

Microsoft Windows의 경우 캐럿(^) 줄 연속 문자를 사용하여 가독성을 개선합니다.

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"createdAt\":{\"gt\":1601881200000,
\"lt\":1604559600000},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}
```

위치:

- *createdAt*은 생성 위치 필드의 JSON 이름을 지정합니다. 그리고:
  - *gt*는 크거나 같음 연산자를 지정합니다.
  - *1601881200000*은 시간 범위의 첫 번째 날짜 및 시간(밀리초 단위의 유닉스 타임스탬프)입니다.
  - *lt*는 작거나 같음 연산자를 지정합니다.
  - *1604559600000*은 시간 범위의 마지막 날짜 및 시간(밀리초 단위의 유닉스 타임스탬프)입니다.
- *classificationDetails.result.sensitiveData.category*는 민감한 데이터 범주 필드의 JSON 이름을 지정합니다. 그리고:
  - *eqExactMatch*는 동일 완전 일치 연산자를 지정합니다.
  - *FINANCIAL_INFORMATION*은 필드에 대한 열거형 값입니다.
- *archived*은 보관된 필드의 JSON 이름을 지정합니다. 그리고:
  - *eq*는 등호 연산자를 지정합니다,
  - *false*는 필드의 부울 값입니다.

조사 결과에 대한 필터 규칙 생성 및 관리

필터 규칙은 Amazon Macie 콘솔에서 조사 결과를 검토할 때 다시 사용하기 위해 생성하고 저장하는 일련의 필터 기준의 집합입니다. 필터 규칙을 사용하면 특정 특성이 있는 결과를 일관되게 분석할 수

있습니다. 예를 들어, 암호화되지 않은 객체가 포함된 S3 버킷에 대한 모든 심각도 높은 정책 조사 결과를 분석하는 필터 규칙을 하나 만들고, 특정 유형의 민감한 데이터를 보고하는 모든 심각도 높은 민감한 데이터 조사 결과를 분석하는 필터 규칙을 하나 더 만들 수 있습니다.

필터 규칙은 안 보이게 하기 규칙과 다릅니다. 안 보이게 하기 규칙은 규칙의 기준과 일치하는 조사 결과를 자동으로 보관하기 위해 생성하고 저장하는 일련의 필터 기준의 집합입니다. 두 가지 유형의 규칙 모두 필터 기준을 저장하고 적용하지만, 필터 규칙은 규칙의 기준과 일치하는 조사 결과에 대해 아무런 작업도 수행하지 않습니다. 대신 필터 규칙은 규칙을 적용한 후에 콘솔에 표시되는 조사 결과만 결정합니다. 안 보이게 하기 규칙에 대한 자세한 내용은 조사 결과 안 보이게 하기을 참조하세요.

필터 규칙을 생성하고 관리하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 다음 주제에서는 방법을 설명합니다. API의 경우 항목에는 AWS Command Line Interface(AWS CLI) 를 사용하여 이러한 작업을 수행하는 방법에 대한 예가 포함되어 있습니다. 또한 최신 버전의 또 다른 AWS 명령줄 도구 또는 AWS SDK를 사용하거나 Macie에 직접 HTTPS 요청을 보냄으로써 이 작업을 수행할 수도 있습니다. AWS도구와 SDK에 대한 자세한 내용은, AWS 기반의 도구를 참조하세요.

주제

필터 규칙 생성

필터 규칙을 생성할 때는 필터 기준, 이름, 규칙 설명(선택 사항)을 지정합니다. Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 필터 규칙을 생성할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 필터 규칙을 생성하려면 다음 단계를 따르세요.

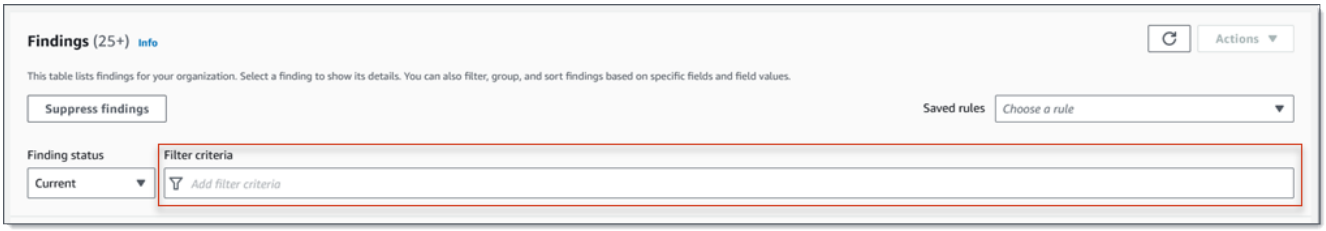
필터 규칙을 생성하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.

> **Tip**
>
> 기존 필터 규칙을 시작점으로 사용하려면 저장된 규칙 목록에서 규칙을 선택합니다.

사전 정의된 논리 그룹별로 조사 결과를 피벗하고 드릴다운하여 규칙을 간편하게 생성할 수 있습니다. 이렇게 하면 Macie가 적절한 필터 조건을 자동으로 만들어 적용하므로 규칙을 만들 때 유용한 출발점이 될 수 있습니다. 이렇게 하려면 탐색 창(조사 결과 아래)에서 버킷별, 유형별 또는 작업별을 선택한 다음 테이블에서 항목을 선택합니다. 디테일 패널에서 피벗할 필드의 링크를 선택합니다.

3. 필터 기준 상자에서 규칙의 필터 기준을 정의하는 조건을 추가합니다.



필터 조건을 추가하는 방법을 알아보려면 조사 결과에 필터 생성 및 적용을 참조하십시오.

4. 규칙에 대한 필터 기준을 정의한 후에는 필터 기준 상자에서 규칙 저장을 선택합니다.

5. 필터 규칙아래에 이름을 입력하고, 선택 사항으로 규칙에 대한 설명을 입력합니다.
6. 저장을 선택합니다.

API

프로그래밍 방식으로 필터 규칙을 생성하려면 Amazon Macie API의 CreateFindingsFilter 작업을 사용하고 필수 매개 변수에 적절한 값을 지정하십시오.

- `action`매개 변수의 경우, Macie가 규칙 기준과 일치하는 결과를 억제(자동 보관)하지 않도록 `NOOP`를 지정하십시오.
- `criterion` 파라미터의 경우, 규칙의 필터 기준을 정의하는 조건 맵을 지정하세요.

  맵에서 각 조건은 필드, 연산자 및 필드에 대한 하나 이상의 값을 지정해야 합니다. 값의 유형과 개수는 선택한 필드와 연산자에 따라 달라집니다. 조건에 사용할 수 있는 필드, 연산자 및 값 유형에 대한 자세한 내용은 조사 결과 필터링 필드, 조건에서·연산자 사용 및 필드 값 지정 을 참조하십시오.

AWS CLI를 사용하여 규칙을 만들려면 create-findings-filter 명령을 실행하고 필수 매개 변수에 적절한 값을 지정합니다. 다음 예제에서는 S3 객체에 있는 개인 정보(기타 민감한 데이터 유형은 제외)의 현재 AWS 리전 및 보고서 발생에 있는 모든 민감한 데이터 조사 결과를 반환하는 필터 규칙을 생성합니다.

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

```
$ aws macie2 create-findings-filter \
--action NOOP \
--name my_filter_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["PERSONAL_INFORMATION"]}}}'
```

이 예제는 Microsoft Windows용으로 포맷되었으며 가독성을 높이기 위해 캐럿(^) 줄 연속 문자를 사용합니다.

```
C:\> aws macie2 create-findings-filter ^
--action NOOP ^
--name my_filter_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"PERSONAL_INFORMATION\"]}}}
```

위치:

- *my_filter_rule*은 규칙의 사용자 지정 이름입니다.
- criterion 규칙의 필터 조건 맵입니다.
  - *classificationDetails.result.sensitiveData.detections.type*은Sensitive data detection type필드의 JSON 이름입니다.
  - *eqExactMatch*는 동일 완전 일치 연산자를 지정합니다.
  - *PERSONAL_INFORMATION*은 민감한 데이터 범주 필드의 열거형 값입니다.

이 명령이 성공적으로 실행되면 다음과 비슷한 출력이 표시됩니다.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
```

```
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

여기서 `arn`은 생성된 필터 규칙의 Amazon 리소스 이름(ARN)이며, `id`는 규칙의 고유 식별자입니다.

필터 기준의 추가 예는 Amazon Macie API를 사용하여 프로그래밍 방식으로 조사 결과 필터링을 참조하세요.

필터 규칙 적용

필터 규칙을 적용하면 Amazon Macie는 규칙의 기준을 사용하여 콘솔의 조사 결과 보기에 어떤 결과를 포함시키고 제외할지 결정합니다. Macie는 또한 어떤 기준을 적용했는지 확인할 수 있도록 기준을 표시합니다.

필터 규칙은 Amazon Macie 콘솔과 함께 사용하도록 설계되었습니다. Amazon Macie API를 사용하여 프로그래밍 방식으로 제출하는 쿼리에는 직접 사용할 수 없습니다. 하지만 API를 사용하여 조사 결과를 쿼리하는 경우, GetFindingsFilter 작업을 사용하여 규칙에 대한 필터 기준을 검색할 수 있습니다. 그런 다음 쿼리에 기준을 추가할 수 있습니다. 쿼리에서 필터 기준을 지정하는 방법에 대한 자세한 내용은 조사 결과에 필터 생성 및 적용을 참조하십시오.

필터 규칙을 적용하여 콘솔에서 조사 결과를 필터링하려면 다음 단계를 수행합니다.

필터 규칙을 적용하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. 저장된 규칙 목록에서 적용할 규칙을 선택합니다. Macie는 규칙의 기준을 적용하고 필터 기준 상자에 기준을 표시합니다.
4. (선택 사항) 기준을 세분화하려면 필터 기준 상자를 사용하여 필터 조건을 추가하거나 제거합니다. 이렇게 하면 변경 내용이 규칙 설정에 영향을 미치지 않습니다. 사용자가 명시적으로 새 규칙으로 저장하지 않는 한 Macie는 변경 사항을 저장하지 않습니다.
5. 다른 필터 규칙을 적용하려면 3단계를 반복합니다.

필터 규칙을 적용한 후에는 필터 기준 상자에서 X를 선택하여 보기에서 해당 필터 기준을 모두 빠르게 제거할 수 있습니다.

필터 규칙 변경

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 언제든지 규칙의 설정을 변경할 수 있습니다. 규칙에 태그를 지정하고 관리할 수도 있습니다.

태그는 사용자가 정의하여 특정 유형의 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별, 분류, 관리하는 데 도움이 됩니다. 자세한 내용은 Amazon Macie에 리소스 태그 지정(을)를 참조하세요.

Console

Amazon Macie 콘솔을 사용하여 기존의 필터 설정을 변경하려면 다음 단계를 따르십시오.

필터 규칙을 변경하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. 저장된 규칙 목록에서 변경하려는 규칙 옆에 있는 편집 아이콘 ( ) 을 선택합니다.
4. 다음을 수행하세요.
   - 규칙의 필터 기준을 변경하려면 필터 기준 상자를 사용하여 원하는 기준에 대한 조건을 입력합니다. 자세한 방법은 조사 결과에 필터 생성 및 적용 섹션을 참조하세요.
   - 규칙 이름을 변경하려면 필터 규칙 아래에 있는 이름 상자에 새 이름을 입력합니다.
   - 규칙의 설명을 변경하려면 필터 규칙 아래에 있는 설명 상자에 새 설명을 입력합니다.
   - 규칙에 태그를 지정, 검토 또는 편집하려면 필터 규칙 아래에 있는 태그 관리를 선택합니다. 그런 다음 필요에 따라 태그를 검토하고 변경합니다. 규칙은 최대 50개의 태그를 가질 수 있습니다.
5. 변경 작업을 마치면, 저장을 선택합니다.

API

필터 규칙을 프로그래밍 방식으로 변경하려면 Amazon Macie API의 UpdateFindingsFilter작업을 사용하십시오. 요청을 제출할 때 지원되는 파라미터를 사용하여 변경하려는 각 설정에 대해 새 값을 지정하세요.

id매개 변수의 경우, 변경할 규칙의 고유 식별자를 지정하십시오. ListFindingsFilter 작업을 사용하여 계정에 대한 필터 및 안 보이게 하기 필터 규칙 목록을 검색하면 이 식별자를 얻을 수 있습니다. AWS CLI를 사용하는 경우, list-findings-filters 명령을 실행하여 이 목록을 검색하십시오.

AWS CLI를 사용하여 필터 규칙을 변경하려면 update-findings-filter 명령을 실행하고 지원되는 매개 변수를 사용하여 변경하려는 각 설정에 대해 새 값을 지정합니다. 예를 들어, 다음 명령은 기존 필터 규칙의 이름을 변경합니다.

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --
name personal_information_only
```

위치:

- *9b2b4508-aa2f-4940-b347-d1451example*는 규칙에 대한 고유 식별자입니다.
- *personal_information_only*는 규칙의 새 이름입니다.

이 명령이 성공적으로 실행되면 다음과 비슷한 출력이 표시됩니다.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

여기서 arn은 변경된 규칙의 Amazon 리소스 이름(ARN)이며, id는 규칙의 고유 식별자입니다.

마찬가지로, 다음 예제에서는 action 매개 변수 값을 ARCHIVE에서 NOOP로 변경하여 필터 규칙을 안 보이게 하기 규칙으로 변환합니다.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action NOOP
```

위치:

- *8a1c3508-aa2f-4940-b347-d1451example*는 규칙에 대한 고유 식별자입니다.
- *NOOP*은 Macie가 규칙의 기준과 일치하는 조사 결과에 대해 수행하는 새로운 작업(조사 결과를 안 보이게하지 않음)입니다.

이 명령이 성공적으로 실행되면, 다음과 비슷한 출력이 표시됩니다.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

여기서 `arn`은 변경된 규칙의 Amazon 리소스 이름(ARN)이며, `id`는 규칙의 고유 식별자입니다.

필터 규칙 삭제

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 언제든지 필터 규칙을 삭제할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 필터 규칙을 삭제하려면 다음 단계를 따르세요.

필터 규칙을 삭제하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. 저장된 규칙 목록에서 변경하려는 필터 규칙 옆에 있는 편집 아이콘 ( ) 을 선택합니다.
4. 필터 규칙에서 삭제를 선택합니다.

API

필터 규칙을 프로그래밍 방식으로 삭제하려면 Amazon Macie API의 DeleteFindingsFilter 작업을 사용하십시오. `id`매개 변수의 경우, 삭제할 규칙의 고유 식별자를 지정하십시오. ListFindingsFilter 작업을 사용하여 계정에 대한 필터 및 안 보이게 하기 필터 규칙 목록을 검색하면 이 식별자를 얻을 수 있습니다. AWS CLI를 사용하는 경우, list-findings-filters 명령을 실행하여 이 목록을 검색하십시오.

AWS CLI를 사용하여 필터 규칙을 삭제하려면 delete-findings-filter 명령을 실행합니다. 예:

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

*9b2b4508-aa2f-4940-b347-d1451example*는 필터 규칙에 대한 고유 식별자입니다.

명령이 성공적으로 실행되면, Macie는 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Macie는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

조사 결과 필터링 필드

조사 결과를 더 효율적으로 분석할 수 있도록 Amazon Macie 콘솔과 Amazon Macie API는 조사 결과를 필터링하기 위한 여러 필드 세트에 대한 액세스를 제공합니다.

- 일반 필드 — 이 필드는 모든 유형의 조사 결과에 적용되는 데이터를 저장합니다. 이들은 심각도, 조사 결과 유형, 조사 결과 ID와 같은 조사 결과의 일반적인 속성과 상관관계가 있습니다.
- 영향을 받는 리소스 필드 - 이 필드에는 영향을 받는 S3 버킷 또는 객체의 이름, 태그, 암호화 설정 등 조사 결과가 적용되는 리소스에 대한 데이터가 저장됩니다.
- 정책 필드 - 이 필드에는 조사 결과를 생성한 작업, 작업을 수행한 주체 등 정책 조사 결과와 관련된 데이터가 저장됩니다.
- 민감한 데이터 분류 필드 - 이 필드에는 Macie가 영향을 받는 S3 객체에서 찾은 민감한 데이터의 범주 및 유형과 같이 민감한 데이터 조사 결과와 관련된 데이터가 저장됩니다.

필터는 이전 세트의 필드 조합을 사용할 수 있습니다.

이 섹션의 항목에서는 조사 결과를 필터링하는 데 사용할 수 있는 개별 필드를 나열하고 설명합니다. 필드 간 관계를 포함하여 이러한 필드에 대한 추가 세부 정보는 Amazon Macie API 참조의 조사 결과를 참조하세요.

주제

공통 필드

다음 테이블은 일반적인 조사 결과 속성을 기반으로 조사 결과를 필터링하는 데 사용할 수 있는 필드를 나열하고 설명합니다. 이 필드에는 모든 유형의 조사 결과에 적용되는 데이터가 저장됩니다.

테이블에서 필드 열은 Amazon Macie 콘솔의 필드 이름을 나타냅니다. JSON 필드 열은 점 표기법을 사용하여 조사 결과를 JSON으로 표현한 필드 이름과 Amazon Macie API를 나타냅니다. 설명 열에는

필드에 저장하는 데이터에 대한 간략한 설명과 필터 값에 대한 요구 사항이 표시됩니다. 테이블은 필드를 기준으로, 그 다음에는 JSON 필드를 기준으로 알파벳 오름차순으로 정렬됩니다.

필드	JSON 필드	설명
계정 ID*	`accountId`	조사 결과가 적용되는 AWS 계정의 고유 식별자입니다. 일반적으로 영향을 받는 리소스를 소유하는 계정입니다.
—	`archived`	조사 결과가 금지 규칙에 의해 금지(자동 보관)되었는지를 지정하는 부울 값입니다. 콘솔의 필터에서 이 필드를 사용하려면 조사 결과 상태 메뉴에서 보관됨(숨김만), 현재(숨김 해제만) 또는 모두(숨김 및 표시 안 함) 중 원하는 옵션을 선택합니다.
범주	`category`	조사 결과 범주 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. API에서, 유효한 값은 민감한 데이터 검색의 경우 `CLASSIFICATION` , 정책 조사 결과의 경우 `POLICY`입니다.
—	`count`	조사 결과가 발생한 총 수입니다. 민감한 데이터 조사 결과의 경우, 이 값은 항상 `1`입니다. 모든 민감한 데이터 조사 결과는 고유한 것으로 간주됩니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다. API

필드	JSON 필드	설명
		를 사용하면 이 필드를 사용하여 필터의 숫자 범위를 정의할 수 있습니다.
생성 시간	`createdAt`	Macie가 조사 결과를 생성한 날짜 및 시간입니다. 이 필드를 사용하여 필터의 시간 범위를 정의할 수 있습니다.
조사 결과 ID*	`id`	조사 결과의 고유 식별자입니다. 이 문자열은 Macie가 조사 결과를 만들 때 생성하여 조사 결과에 할당하는 임의의 문자열입니다.
조사 결과 유형*	`type`	조사 결과 유형(예: `SensitiveData:S3Object/Personal` 또는 `Policy:IAMUser/S3BucketPublic`) 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. API의 유효한 값 목록은 Amazon Macie API 레퍼런스를 참조하십시오 FindingType.
리전	`region`	AWS 리전Macie가 찾은 조사 결과(예: `us-east-1` 또는 `ca-central-1`).

필드	JSON 필드	설명
Sample	`sample`	조사 결과가 샘플 조사 결과인지를 지정하는 부울 값입니다. 샘플 조사 결과는 예제 데이터와 자리 표시자 값을 사용하여 조사 결과에 포함될 수 있는 정보를 설명하는 조사 결과입니다. 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다.
심각도(Severity)	`severity.description`	조사 결과의 심각도에 대한 질적 표현 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. API에서 유효 값은 `Low`, `Medium` 및 `High`입니다.
업데이트된 시간	`updatedAt`	조사 결과가 마지막으로 업데이트된 날짜 및 시간입니다. 민감한 데이터 조사 결과의 경우 이 값은 생성 시간 필드의 값과 동일합니다. 모든 민감한 데이터 조사 결과는 새로운 것(고유한 것)으로 간주됩니다. 이 필드를 사용하여 필터의 시간 범위를 정의할 수 있습니다.

* 콘솔에서 이 필드에 여러 값을 지정하려면 필드를 사용하고 필터에 고유한 값을 지정하는 조건을 추가한 다음 각 추가 값에 대해 해당 단계를 반복합니다. API를 사용하여 이 작업을 수행하려면 필터에 사용할 값이 나열된 배열을 사용하세요.

영향을 받는 리소스 필드

다음 항목에서는 조사 결과가 적용되는 리소스를 기준으로 조사 결과를 필터링하는 데 사용할 수 있는 필드를 나열하고 설명합니다. 주제는 리소스 유형별로 구성됩니다.

주제

- S3 버킷
- S3 객체

S3 버킷

다음 표는 조사 결과가 적용되는 S3 버킷의 특성을 기반으로 조사 결과를 필터링하는 데 사용할 수 있는 필드를 나열하고 설명합니다.

테이블에서 필드 열은 Amazon Macie 콘솔의 필드 이름을 나타냅니다. JSON 필드 열은 점 표기법을 사용하여 조사 결과를 JSON으로 표현한 필드 이름과 Amazon Macie API를 나타냅니다. (긴 JSON 필드 이름은 가독성을 높이기 위해 줄 바꿈 문자 시퀀스(\n)를 사용합니다.) 설명 열에는 필드에 저장하는 데이터에 대한 간략한 설명과 필터 값에 대한 요구 사항이 표시됩니다. 테이블은 필드를 기준으로, 그 다음에는 JSON 필드를 기준으로 알파벳 오름차순으로 정렬됩니다.

필드	JSON 필드	설명
—	`resourcesAffected.s3Bucket.createdAt`	영향을 받는 버킷이 생성된 날짜 및 시간, 또는 버킷 정책 편집 등의 변경 사항이 가장 최근에 영향을 받은 버킷에 적용된 날짜 및 시간입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다. API를 사용하면 이 필드를 사용하여 필터의 시간 범위를 정의할 수 있습니다.
S3 버킷 기본 암호화	`resourcesAffected.s3Bucket.defaultSe`	영향을 받는 버킷에 추가된 객체를 암호화하는 데 기본적으

필드	JSON 필드	설명
	`rverSideEncryption.encryptionType`	로 사용되는 서버 측 암호화 알고리즘입니다. 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. API의 유효한 값 목록은 Amazon Macie API 레퍼런스를 참조하십시오 EncryptionType.
S3 버킷 암호화 KMS 키 ID*	`resourcesAffected.s3Bucket.defaultServerSideEncryption.kmsMasterKeyId`	영향을 받는 버킷에 추가되는 객체를 암호화하는 데 기본적으로 사용되는 AWS KMS key에 대한 Amazon 리소스 이름(ARN) 또는 고유 식별자(키 ID)
버킷 정책에 필요한 S3 버킷 암호화	`resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads`	객체가 버킷에 추가될 때 영향을 받는 버킷의 버킷 정책에 객체의 서버 측 암호화가 필요한지를 지정합니다. 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. API의 유효한 값 목록은 Amazon Macie API 레퍼런스의 S3Bucket을 참조하세요.
S3 버킷 이름*	`resourcesAffected.s3Bucket.name`	영향을 받는 버킷의 전체 이름입니다.
S3 버킷 소유자 표시 이름*	`resourcesAffected.s3Bucket.owner.displayName`	영향을 받는 버킷을 소유한 AWS 사용자의 표시 이름.

필드	JSON 필드	설명
S3 버킷 공개 액세스 권한	`resourcesAffected.s3Bucket.publicAccess.effectivePermission`	버킷에 적용되는 권한 설정의 조합을 기반으로 영향을 받는 버킷에 공개적으로 액세스할 수 있는지를 지정합니다. 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. API의 유효한 값 목록은 Amazon Macie API 레퍼런스를 참조하십시오 BucketPublicAccess.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n  accountLevelPermissions.blockPublicAccess.blockPublicAcls`	Amazon S3가 영향을 받는 버킷 및 버킷의 객체에 대해 공개 액세스 제어 목록(ACL)을 차단하는지를 지정하는 부울 값입니다. 이는 버킷에 대한 계정 수준의 공개 액세스 차단 설정입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n  accountLevelPermissions.blockPublicAccess.blockPublicPolicy`	Amazon S3가 영향을 받는 버킷에 대한 공개 버킷 정책을 차단할지를 지정하는 부울 값입니다. 이는 버킷에 대한 계정 수준의 공개 액세스 차단 설정입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.

필드	JSON 필드	설명
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.ignorePublicAcls`	Amazon S3가 영향을 받는 버킷 및 버킷의 객체에 대한 공개 ACL을 무시할지를 지정하는 부울 값입니다. 이는 버킷에 대한 계정 수준의 공개 액세스 차단 설정입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.restrictPublicBuckets`	Amazon S3가 영향을 받는 버킷에 대한 공개 버킷 정책을 제한할지를 지정하는 부울 값입니다. 이는 버킷에 대한 계정 수준의 공개 액세스 차단 설정입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicReadAccess`	영향을 받는 버킷의 버킷 수준 ACL이 일반 대중에게 해당 버킷에 대한 읽기 액세스 권한을 부여할지를 지정하는 부울 값입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.

필드	JSON 필드	설명
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicWriteAccess`	영향을 받는 버킷의 버킷 수준 ACL이 일반 대중에게 해당 버킷에 대한 쓰기 액세스 권한을 부여할지를 지정하는 부울 값입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicAcls`	Amazon S3가 해당 버킷과 버킷의 객체에 대한 공개 ACL을 차단할지를 지정하는 부울 값입니다. 이는 버킷에 대한 버킷 수준의 공개 액세스 차단 설정입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicPolicy`	Amazon S3가 영향을 받는 버킷에 대한 공개 버킷 정책을 차단할지를 지정하는 부울 값입니다. 이는 버킷에 대한 버킷 수준의 공개 액세스 차단 설정입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.

필드	JSON 필드	설명
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.ignorePublicAcls`	Amazon S3가 영향을 받는 버킷 및 버킷의 객체에 대한 공개 ACL을 무시할지를 지정하는 부울 값입니다. 이는 버킷에 대한 버킷 수준의 공개 액세스 차단 설정입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets`	Amazon S3가 영향을 받는 버킷에 대한 공개 버킷 정책을 제한할지를 지정하는 부울 값입니다. 이는 버킷에 대한 버킷 수준의 공개 액세스 차단 설정입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess`	영향을 받는 버킷의 정책에서 일반 대중이 버킷에 대한 읽기 액세스 권한을 갖도록 허용할지를 지정하는 부울 값입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.

필드	JSON 필드	설명

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess`
		영향을 받는 버킷의 정책에서 일반 대중이 버킷에 대한 쓰기 권한을 갖도록 허용할지를 지정하는 부울 값입니다.
		
		이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.

S3 버킷 태그 키*	`resourcesAffected.s3Bucket.tags.key`	영향을 받는 버킷과 연결된 태그 키입니다.
S3 버킷 태그 값*	`resourcesAffected.s3Bucket.tags.value`	영향을 받는 버킷과 연결된 태그 값입니다.

* 콘솔에서 이 필드에 여러 값을 지정하려면 필드를 사용하고 필터에 고유한 값을 지정하는 조건을 추가한 다음 각 추가 값에 대해 해당 단계를 반복합니다. API를 사용하여 이 작업을 수행하려면 필터에 사용할 값이 나열된 배열을 사용하세요.

S3 객체

다음 테이블에는 조사 결과가 적용되는 S3 객체의 특성을 기반으로 조사 결과를 필터링하는 데 사용할 수 있는 필드가 나열되고 설명되어 있습니다.

테이블에서 필드 열은 Amazon Macie 콘솔의 필드 이름을 나타냅니다. JSON 필드 열은 점 표기법을 사용하여 조사 결과를 JSON으로 표현한 필드 이름과 Amazon Macie API를 나타냅니다. 설명 열에는 필드에 저장하는 데이터에 대한 간략한 설명과 필터 값에 대한 요구 사항이 표시됩니다. 테이블은 필드를 기준으로, 그 다음에는 JSON 필드를 기준으로 알파벳 오름차순으로 정렬됩니다.

필드	JSON 필드	설명
S3 객체 암호화 KMS 키 ID*	`resourcesAffected.s3Object.serverSid`	영향을 받는 객체를 암호화하는 데 사용된 AWS KMS key

필드	JSON 필드	설명
	`eEncryption.kmsMas terKeyId`	에 대한 Amazon 리소스 이름(ARN) 또는 고유 식별자(키 ID) 입니다.
S3 객체 암호화 유형	`resourcesAffected. s3Object.serverSid eEncryption.encryp tionType`	영향을 받는 객체를 암호화하는 데 사용된 서버 측 암호화 알고리즘. 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. API의 유효한 값 목록은 Amazon Macie API 레퍼런스를 참조하십시오 EncryptionType.
—	`resourcesAffected. s3Object.extension`	영향을 받는 객체의 파일 이름 확장명. 파일 이름 확장명이 없는 객체의 경우, 필터에 대한 값으로 ""(을)를 지정합니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`resourcesAffected. s3Object.lastModif ied`	영향 받는 객체가 생성되거나 마지막으로 변경된 날짜 및 시간입니다(둘 중 가장 늦은 날짜). 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다. API를 사용하면 이 필드를 사용하여 필터의 시간 범위를 정의할 수 있습니다.

필드	JSON 필드	설명
S3 객체 키*	`resourcesAffected.s3Object.key`	해당하는 경우 객체의 접두사를 포함하여 영향을 받는 객체의 전체 이름(키).
—	`resourcesAffected.s3Object.path`	영향을 받는 버킷 이름 및 객체 이름(키)을 포함한 영향 받는 객체의 전체 경로. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
S3 객체 공개 액세스	`resourcesAffected.s3Object.publicAccess`	객체에 적용되는 권한 설정의 조합을 기반으로 영향을 받는 객체에 공개적으로 액세스할 수 있는지를 지정하는 부울 값입니다. 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다.
S3 객체 태그 키*	`resourcesAffected.s3Object.tags.key`	영향을 받는 객체와 연결된 태그 키입니다.
S3 객체 태그 값*	`resourcesAffected.s3Object.tags.value`	영향을 받는 객체와 연결된 태그 값입니다.

* 콘솔에서 이 필드에 여러 값을 지정하려면 필드를 사용하고 필터에 고유한 값을 지정하는 조건을 추가한 다음 각 추가 값에 대해 해당 단계를 반복합니다. API를 사용하여 이 작업을 수행하려면 필터에 사용할 값이 나열된 배열을 사용하세요.

정책 필드

다음 테이블에는 정책 조사 결과를 필터링하는 데 사용할 수 있는 필드가 나열되고 설명되어 있습니다. 이 필드에는 정책 조사 결과와 관련된 데이터가 저장됩니다.

테이블에서 필드 열은 Amazon Macie 콘솔의 필드 이름을 나타냅니다. JSON 필드 열은 점 표기법을 사용하여 조사 결과를 JSON으로 표현한 필드 이름과 Amazon Macie API를 나타냅니다. (긴 JSON 필드 이름은 가독성을 높이기 위해 줄 바꿈 문자 시퀀스(\n)를 사용합니다.) 설명 열에는 필드에 저장하는 데이터에 대한 간략한 설명과 필터 값에 대한 요구 사항이 표시됩니다. 테이블은 필드를 기준으로, 그 다음에는 JSON 필드를 기준으로 알파벳 오름차순으로 정렬됩니다.

필드	JSON 필드	설명
작업 유형	`policyDetails.action.actionType`	조사 결과를 생성한 작업 유형. 이 필드의 유일한 유효 값은 `AWS_API_CALL` 입니다.
API 호출 이름*	`policyDetails.action.apiCallDetails.api`	가장 최근에 호출되어 조사 결과를 생성한 작업의 이름(예: `PutBucketPublicAccessBlock`).
API 서비스 이름*	`policyDetails.action.apiCallDetails.apiServiceName`	호출되어 조사 결과를 생성한 작업을 제공하는 AWS 서비스의 URL(예: `s3.amazonaws.com`).
—	`policyDetails.action.apiCallDetails.firstSeen`	작업이 호출되어 조사 결과를 생성한 첫 번째 날짜 및 시간입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다. API를 사용하면 이 필드를 사용하여 필터의 시간 범위를 정의할 수 있습니다.

필드	JSON 필드	설명
—	`policyDetails.action.apiCallDetails.lastSeen`	지정된 작업(API 호출 이름 또는 api)이 호출되어 조사 결과를 생성한 가장 최근 날짜 및 시간입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다. API를 사용하면 이 필드를 사용하여 필터의 시간 범위를 정의할 수 있습니다.
—	`policyDetails.actor.domainDetails.domainName`	작업을 수행하는 데 사용된 장치의 도메인 이름. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
IP 도시*	`policyDetails.actor.ipAddressDetails.ipCity.name`	작업을 수행하는 데 사용된 장치의 IP 주소에 대한 발신 도시 이름.
IP 국가*	`policyDetails.actor.ipAddressDetails.ipCountry.name`	작업을 수행하는 데 사용된 장치의 IP 주소의 발신 국가 이름(예:). `United States`
—	`policyDetails.actor.ipAddressDetails.ipOwner.asn`	작업을 수행하는 데 사용된 장치의 IP 주소가 포함된 자율 시스템의 ASN(자율 시스템 번호). 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
IP 소유자 ASN 조직*	`policyDetails.actor.ipAddressDetails.ipOwner.asnOrg`	작업을 수행하는 데 사용된 장치의 IP 주소를 포함하는 자율 시스템용 ASN과 연결된 조직 식별자입니다.

필드	JSON 필드	설명
IP 소유자는 SP*	`policyDetails.actor.ipAddressDetails.ipOwner.isp`	작업을 수행하는 데 사용된 장치의 IP 주소를 소유한 인터넷 서비스 공급자(ISP)의 이름.
IP V4 주소*	`policyDetails.actor.ipAddressDetails.ipAddressV4`	작업을 수행하는 데 사용된 장치의 IPv4(인터넷 프로토콜 버전 4) 주소입니다.
—	`policyDetails.actor.userIdentity.assumedRole.accessKeyId`	AWS STS API의 `AssumeRole` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 자격 증명을 식별하는 AWS 액세스 키 ID입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
사용자 ID 수임 역할 계정 ID*	`policyDetails.actor.userIdentity.assumedRole.accountId`	AWS STS API의 `AssumeRole` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 자격 증명을 가져오는 데 사용된 엔티티를 소유하는AWS 계정에 대한 고유 식별자입니다.
사용자 ID로 위임된 역할 보안 주체 ID*	`policyDetails.actor.userIdentity.assumedRole.principalId`	AWS STS API의 `AssumeRole` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 자격 증명을 가져오는 데 사용된 주체의 고유 식별자입니다.

필드	JSON 필드	설명
사용자 ID 역할 수임 세션 ARN*	`policyDetails.actor.userIdentity.assumedRole.arn`	AWS STS API의 `AssumeRole` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 자격 증명을 가져오는 데 사용된 소스 계정, IAM 사용자 또는 역할의 Amazon 리소스 이름(ARN).

—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n`
	
	`sessionIssuer.type`
		AWS STS API의 `AssumeRole` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 임시 보안 자격 증명의 출처(예: `Root`, `IAMUser` 또는 `Role`).
		
		이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.

—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n`
	
	`sessionIssuer.userName`
		AWS STS API의 `AssumeRole` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우 세션을 생성한 사용자 또는 역할의 이름 또는 별칭입니다. 단, 별칭이 없는 루트 계정에서 자격 증명을 가져온 경우 이 값은 무효입니다.
		
		이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.

사용자 ID AWS 계정 계정 ID*	`policyDetails.actor.userIdentity.awsAccount.accountId`	다른 AWS 계정의 자격 증명을 사용하여 수행한 작업의 경우, 해당 계정의 고유 식별자입니다.

필드	JSON 필드	설명
사용자 ID AWS 계정 보안 주체 ID*	`policyDetails.actor.userIdentity.awsAccount.principalId`	다른 AWS 계정의 자격 증명을 사용하여 수행한 작업의 경우, 해당 작업을 수행한 주체의 고유 식별자입니다.
사용자 ID AWS 서비스 호출자	`policyDetails.actor.userIdentity.awsService.invokedBy`	AWS 서비스에 속하는 계정으로 수행한 작업의 경우, 서비스 이름입니다.
—	`policyDetails.actor.userIdentity.federatedUser.accessKeyId`	AWS STS API의 `GetFederationToken` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 자격 증명을 식별하는 AWS 액세스 키 ID입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
사용자 ID 연동 세션 ARN*	`policyDetails.actor.userIdentity.federatedUser.arn`	AWS STS API의 `GetFederationToken` 작업을 통해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 자격 증명을 가져오는 데 사용된 주체의 ARN입니다.
사용자 ID 연동 사용자 계정 ID*	`policyDetails.actor.userIdentity.federatedUser.accountId`	AWS STS API의 `GetFederationToken` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 자격 증명을 가져오는 데 사용된 엔티티를 소유하는AWS 계정에 대한 고유 식별자입니다.

필드	JSON 필드	설명
사용자 ID 연동 사용자 보안 주체 ID*	`policyDetails.actor.userIdentity.federatedUser.principalId`	AWS STS API의 `GetFederationToken` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 자격 증명을 가져오는 데 사용된 주체의 고유 식별자입니다.
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.type`	AWS STS API의 `GetFederationToken` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우, 임시 보안 자격 증명의 출처(예: `Root`, `IAMUser` 또는 `Role`). 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.userName`	AWS STS API의 `GetFederationToken` 작업을 사용해 획득한 임시 보안 자격 증명으로 수행한 작업의 경우 세션을 생성한 사용자 또는 역할의 이름 또는 별칭입니다. 단, 별칭이 없는 루트 계정에서 자격 증명을 가져온 경우 이 값은 무효입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
사용자 ID IAM 계정 ID*	`policyDetails.actor.userIdentity.iamUser.accountId`	IAM 사용자의 자격 증명을 사용하여 수행한 작업의 경우, 작업을 수행한 IAM 사용자와 관련된 AWS 계정에 대한 고유 식별자입니다.

필드	JSON 필드	설명
사용자 ID IAM 보안 주체 ID*	`policyDetails.actor.userIdentity.iamUser.principalId`	IAM 사용자의 자격 증명을 사용하여 수행한 작업의 경우, 작업을 수행한 IAM 사용자에 대한 고유 식별자입니다.
사용자 ID IAM 사용자 이름*	`policyDetails.actor.userIdentity.iamUser.userName`	IAM 사용자의 자격 증명을 사용하여 수행한 작업의 경우, 작업을 수행한 IAM 사용자의 사용자 이름입니다.
사용자 ID 루트 계정 ID*	`policyDetails.actor.userIdentity.root.accountId`	사용자의 AWS 계정에 대한 자격 증명을 사용하여 수행한 작업의 경우, 해당 계정의 고유 식별자입니다.
사용자 ID 루트 보안 주체 ID*	`policyDetails.actor.userIdentity.root.principalId`	사용자의 AWS 계정에 대한 자격 증명을 사용하여 수행한 작업의 경우, 해당 작업을 수행한 엔티티의 고유 식별자입니다.
사용자 ID 유형	`policyDetails.actor.userIdentity.type`	조사 결과를 생성한 작업을 수행한 엔티티의 유형입니다. 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. API의 유효한 값 목록은 Amazon Macie API 레퍼런스를 참조하십시오 UserIdentityType.

* 콘솔에서 이 필드에 여러 값을 지정하려면 필드를 사용하고 필터에 고유한 값을 지정하는 조건을 추가한 다음 각 추가 값에 대해 해당 단계를 반복합니다. API를 사용하여 이 작업을 수행하려면 필터에 사용할 값이 나열된 배열을 사용하세요.

민감한 데이터 분류 필드

다음 테이블에는 민감한 데이터 조사 결과를 필터링하는 데 사용할 수 있는 필드가 나열되고 설명되어 있습니다. 이 필드에는 민감한 데이터 조사 결과와 관련된 데이터가 저장됩니다.

테이블에서 필드 열은 Amazon Macie 콘솔의 필드 이름을 나타냅니다. JSON 필드 열은 점 표기법을 사용하여 조사 결과를 JSON으로 표현한 필드 이름과 Amazon Macie API를 나타냅니다. 설명 열에는 필드에 저장하는 데이터에 대한 간략한 설명과 필터 값에 대한 요구 사항이 표시됩니다. 테이블은 필드를 기준으로, 그 다음에는 JSON 필드를 기준으로 알파벳 오름차순으로 정렬됩니다.

필드	JSON 필드	설명
사용자 정의 데이터 식별자 ID*	`classificationDetails.result.customDataIdentifiers.detections.arn`	데이터를 탐지하고 조사 결과를 생성한 사용자 정의 데이터 식별자의 고유 식별자입니다.
사용자 정의 데이터 식별자 이름*	`classificationDetails.result.customDataIdentifiers.detections.name`	데이터를 탐지하고 조사 결과를 생성한 사용자 정의 데이터 식별자의 이름입니다.
사용자 정의 데이터 식별자 총 수입니다.	`classificationDetails.result.customDataIdentifiers.detections.count`	사용자 정의 데이터 식별자로 탐지되어 조사 결과를 생성한 총 데이터 발생 횟수입니다. 이 필드를 사용하여 필터의 숫자 범위를 정의할 수 있습니다.
작업 ID*	`classificationDetails.jobId`	조사 결과를 생성한 민감한 데이터 검색 작업의 고유 식별자입니다.
오리진 유형	`classificationDetails.originType`	Macie가 조사 결과를 생성한 민감한 데이터를 발견한 방법: `AUTOMATED_SENSITIVE_DATA_DISCOVERY` 또는 `SENSITIVE_DATA_DISCOVERY_JOB` .

필드	JSON 필드	설명
—	`classificationDetails.result.mimeType`	조사 결과가 적용되는 콘텐츠 유형(예: CSV 파일의 경우 `text/csv` 또는 Adobe Portable Document Format 파일의 경우 `application/pdf`)을 나타내는 MIME 유형입니다. 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다.
—	`classificationDetails.result.sizeClassified`	조사 결과가 적용되는 S3 객체의 총 스토리지 크기(바이트) 이 필드는 콘솔에서 필터 옵션으로 사용할 수 없습니다. API를 사용하면 이 필드를 사용하여 필터의 숫자 범위를 정의할 수 있습니다.

필드	JSON 필드	설명
결과 상태 코드*	`classificationDetails.result.status.code`	조사 결과의 상태입니다. 유효한 값은 다음과 같습니다. • `COMPLETE` - Macie가 객체 분석을 완료했습니다. • `PARTIAL`— Macie가 객체의 데이터 부분집합만 분석했습니다. 예를 들어, 객체는 지원되지 않는 형식의 파일을 포함하는 아카이브 파일입니다. • `SKIPPED`— Macie는 객체를 분석할 수 없었습니다. 예를 들어, 객체는 형식이 잘못된 파일입니다.
민감한 데이터 범주	`classificationDetails.result.sensitiveData.category`	탐지되어 조사 결과를 생성한 민감한 데이터의 범주입니다. 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. API에서 유효 값은 `CREDENTIALS` , `FINANCIAL_INFORMATION` 및 `PERSONAL_INFORMATION` 입니다.

필드	JSON 필드	설명
민감한 데이터 탐지 유형	`classificationDetails.result.sensitiveData.detections.type`	탐지되어 조사 결과를 생성한 민감한 데이터의 유형입니다. 콘솔은 이 필드를 필터에 추가할 때 선택할 수 있는 값 목록을 제공합니다. 콘솔과 API의 유효한 값 목록을 보려면 민감한 데이터 탐지 유형(을)를 참조하세요.
민감한 데이터 총 수	`classificationDetails.result.sensitiveData.detections.count`	탐지되어 조사 결과를 생성한 민감한 데이터가 발생한 총 횟수입니다. 이 필드를 사용하여 필터의 숫자 범위를 정의할 수 있습니다.

* 콘솔에서 이 필드에 여러 값을 지정하려면 필드를 사용하고 필터에 고유한 값을 지정하는 조건을 추가한 다음 각 추가 값에 대해 해당 단계를 반복합니다. API를 사용하여 이 작업을 수행하려면 필터에 사용할 값이 나열된 배열을 사용하세요.

민감한 데이터 탐지 유형

다음 항목에는 필터의 민감한 데이터 탐지 유형 필드에 지정할 수 있는 값이 나열되어 있습니다. (이 필드의 JSON 이름은 `classificationDetails.result.sensitiveData.detections.type`입니다.) 항목은 Macie가 관리형 데이터 식별자를 사용하여 탐지할 수 있는 민감한 데이터 범주별로 구성됩니다.

카테고리

- 보안 인증
- 금융 정보
- 개인 정보: 개인 건강 정보(PHI)
- 개인 정보: 개인 식별 정보(PII)

특정 유형의 민감한 데이터에 대한 관리형 데이터 식별자에 대한 자세한 내용은 상세 참조: Amazon Macie 관리형 데이터 식별자(을)를 참조하세요.

보안 인증

다음 값을 지정하여 S3 객체의 자격 증명 데이터 발생을 보고하는 조사 결과를 필터링할 수 있습니다.

민감한 데이터 유형	필터 값
AWS 비밀 액세스 키	AWS_CREDENTIALS
Google Cloud API 키	GCP_API_KEY
HTTP Basic Authorization 헤더	HTTP_BASIC_AUTH_HEADER
JSON Web Token(JWT)	JSON_WEB_TOKEN
OpenSSH 프라이빗 키	OPENSSH_PRIVATE_KEY
PGP 프라이빗 키	PGP_PRIVATE_KEY
퍼블릭 키 암호화 표준(PKCS) 프라이빗 키	PKCS
PuTTY 프라이빗 키	PUTTY_PRIVATE_KEY
Stripe API 키	STRIPE_CREDENTIALS

금융 정보

다음 값을 지정하여 S3 객체의 재무 정보 발생을 보고하는 조사 결과를 필터링할 수 있습니다.

민감한 데이터 유형	필터 값
은행 계좌 번호	BANK_ACCOUNT_NUMBER (캐나다 및 미국의 경우)
기본 은행 계좌 번호(BBAN)	국가 또는 리전에 따라 다름: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BA

민감한 데이터 유형	필터 값
	NK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
신용 카드 유효 기간	CREDIT_CARD_EXPIRATION
신용 카드 마그네틱 스트립 데이터	CREDIT_CARD_MAGNETIC_STRIPE
신용 카드 번호	CREDIT_CARD_NUMBER (키워드에 근접한 신용 카드 번호의 경우), CREDIT_CARD_NUMBER_(NO_KEYWORD) (키워드에 근접하지 않은 신용 카드 번호의 경우)
신용 카드 인증 코드	CREDIT_CARD_SECURITY_CODE

민감한 데이터 유형	필터 값
국제 은행 계좌 번호(IBAN)	국가 또는 리전에 따라 다름: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER,

민감한 데이터 유형	필터 값
	MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (영국령 버진 아일랜드의 경우)

개인 정보: 개인 건강 정보(PHI)

다음 값을 지정하여 S3 객체에서 발생하는 개인 건강 정보(PHI)를 보고하는 조사 결과를 필터링할 수 있습니다.

민감한 데이터 유형	필터 값
마약단속국(DEA) 등록 번호	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
건강 보험 청구 번호(HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
건강 보험 또는 의료 식별 번호	국가 또는 리전에 따라 다름: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER
Healthcare Common Procedure Coding System(HCPCS) 코드	USA_HEALTHCARE_PROCEDURE_CODE
국가 의약품 코드(NDC)	USA_NATIONAL_DRUG_CODE
국가 공급자 식별자(NPI)	USA_NATIONAL_PROVIDER_IDENTIFIER
고유 디바이스 식별자(UDI)	MEDICAL_DEVICE_UDI

개인 정보: 개인 식별 정보(PII)

다음 값을 지정하여 S3 객체에서 발생하는 개인 식별 정보(PII)를 보고하는 조사 결과를 필터링할 수 있습니다.

민감한 데이터 유형	필터 값
생년월일	DATE_OF_BIRTH
운전면허증 식별 번호	국가 또는 리전에 따라 다름: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_D

민감한 데이터 유형	필터 값
	RIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (미국의 경우), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
선거인단 번호	UK_ELECTORAL_ROLL_NUMBER
전체 이름	NAME
위성 항법 시스템(GPS) 좌표	LATITUDE_LONGITUDE
HTTP 쿠키	HTTP_COOKIE

민감한 데이터 유형	필터 값
우편 주소	ADDRESS, BRAZIL_CEP_CODE
국적 식별 번호	국가 또는 리전에 따라 다름: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
National Insurance Number(NINO)	UK_NATIONAL_INSURANCE_NUMBER
여권 번호	국가 또는 리전에 따라 다름: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
영주권 번호	CANADA_NATIONAL_IDENTIFICATION_NUMBER
전화번호	국가 또는 리전에 따라 다름: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (캐나다 및 미국의 경우), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
Social Insurance Number(SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
사회 보장 번호(SSN)	국가 또는 리전에 따라 다름: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

민감한 데이터 유형	필터 값
납세자 식별 번호 또는 참조 번호	국가 또는 리전에 따라 다름: AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER
차량 식별 번호(VIN)	VEHICLE_IDENTIFICATION_NUMBER

Amazon Macie의 조사 결과를 통한 민감한 데이터 조사

민감한 데이터 검색 작업을 실행하거나 Amazon Macie가 민감한 데이터 자동 검색을 수행하는 경우 Macie는 Amazon Simple Storage Service(S3) 객체에서 찾은 민감한 데이터의 각 발생 위치에 대한 세부 정보를 캡처합니다. 여기에는 Macie가 관리형 데이터 식별자를 사용하여 탐지한 민감한 데이터와 작업 또는 Macie가 사용하도록 구성한 사용자 지정 데이터 식별자의 기준과 일치하는 데이터가 포함됩니다.

민감한 데이터 조사 결과를 통해 Macie가 개별 S3 객체에서 발견한 민감한 데이터가 최대 15건인지 등 세부 정보를 검토할 수 있습니다. 세부 정보를 통해 특정 S3 버킷 및 객체에 포함될 수 있는 민감한 데이터의 범주와 유형에 대한 통찰력을 얻을 수 있습니다. 이를 통해 객체에서 발생하는 민감한 데이터를 개별적으로 찾아내고 특정 버킷과 객체에 대해 더 심층적인 조사를 수행할지 여부를 결정할 수 있습니다.

추가로 통찰력을 얻기 위해 Macie가 개별 조사 결과를 보고하는 민감한 데이터의 샘플을 검색하도록 Macie를 구성하고 사용할 수도 있습니다. 샘플을 통해 Macie가 발견한 민감한 데이터의 특성을 확인할 수 있습니다. 또한 영향을 받는 S3 버킷 및 객체에 대한 조사를 맞춤 설정하는 데 도움이 될 수 있습니다. 조사 결과를 얻기 위해 민감한 데이터 샘플 검색을 선택한 경우 Macie는 조사 결과에 있는 데이터를 사용하여 조사 결과에서 보고된 각 유형의 민감한 데이터 중에서 1~10개의 항목을 찾습니다. 그런

다음 Macie는 영향을 받는 객체에서 이러한 민감한 데이터를 추출하여 검토할 수 있도록 데이터를 표시합니다.

S3 객체에 민감한 데이터가 많이 포함되어 있는 경우 조사 결과를 통해 해당 민감한 데이터 조사 결과를 탐색할 수도 있습니다. 민감한 데이터 조사 결과와는 달리, 민감한 데이터 조사 결과는 Macie가 객체에서 발견한 각 유형의 민감한 데이터가 1,000건에 달하는 상세한 위치 데이터를 제공합니다. Macie는 민감한 데이터 조사 결과 및 민감한 데이터 조사 결과의 위치 데이터에 동일한 스키마를 사용합니다. 민감한 데이터 조사 결과에 대한 자세한 내용은 민감한 데이터 검색 결과 저장 및 유지을(를) 참조하세요.

이 섹션의 항목에서는 민감한 데이터 발견으로 보고된 민감한 데이터를 찾고 선택적으로 검색하는 방법을 설명합니다. 또한 Macie가 발견한 민감한 데이터의 개별 발생 위치를 보고하는 데 사용하는 스키마에 대해서도 설명합니다.

주제

- Amazon Macie 조사 결과를 통한 민감한 데이터 위치 찾기
- Amazon Macie 조사 결과를 사용하여 민감한 데이터 샘플 검색
- 민감한 데이터 위치에 대한 JSON 스키마

Amazon Macie 조사 결과를 통한 민감한 데이터 위치 찾기

민감한 데이터 검색 작업을 실행하거나 Amazon Macie가 민감한 데이터 자동 검색을 수행하는 경우, Macie는 분석하는 각 Amazon Simple Storage Service(S3) 객체의 최신 버전을 심층 검사합니다. 각 작업 실행 또는 분석 주기의 경우, Macie는 또한 깊이 우선 검색 알고리즘을 사용하여 Macie가 S3 객체에서 찾은 민감한 데이터의 특정 발생 위치에 대한 세부 정보로 결과적인 조사 결과를 채웁니다. 이러한 발생 사례를 통해 영향을 받는 S3 버킷 및 객체에 포함될 수 있는 민감한 데이터의 범주 및 유형에 대한 통찰력을 얻을 수 있습니다. 세부 정보를 통해 객체의 개별적인 민감한 데이터 발생 위치를 찾아내고 특정 버킷과 객체에 대해 더 심층적인 조사를 수행할지 여부를 결정할 수 있습니다.

민감한 데이터 조사 결과를 통해, Macie가 영향을 받는 S3 객체에서 발견한 민감한 데이터의 위치를 최대 15개까지 파악할 수 있습니다. 여기에는 Macie가 관리형 데이터 식별자를 사용하여 탐지한 민감한 데이터와 작업이나 Macie가 사용하도록 구성한 사용자 지정 데이터 식별자의 기준과 일치하는 데이터가 포함됩니다.

민감한 데이터 조사 결과는 다음과 같은 세부 정보를 제공할 수 있습니다 -

- Microsoft Excel 통합 문서, CSV 파일 또는 TSV 파일에 있는 셀 또는 필드의 열 및 행 번호.

- JSON 또는 JSON 행 파일에 있는 필드 또는 배열의 경로입니다.
- CSV, JSON, JSON 행 또는 TSV 파일이 아닌 비이진 텍스트 파일에 있는 줄의 줄 번호입니다(예: HTML, TXT 또는 XML 파일).
- Adobe 휴대용 문서 형식(PDF) 파일에 있는 페이지의 페이지 번호입니다.
- Apache Avro 객체 컨테이너 또는 Apache Parquet 파일에 있는 레코드의 레코드 인덱스 및 필드 경로.

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 이러한 세부 정보에 액세스할 수 있습니다. Macie가 Amazon EventBridge와 AWS Security Hub 등 다른 AWS 서비스에 게시하는 조사 결과에서도 이러한 세부 정보에 액세스할 수 있습니다. Macie가 이러한 세부 정보를 보고하는 데 사용하는 JSON 구조에 대해 알아보려면 민감한 데이터 위치에 대한 JSON 스키마을(를) 참조하세요. Macie가 다른 AWS 서비스에 게시하는 조사 결과의 세부 정보에 액세스하는 방법을 알아보려면 결과 모니터링 및 처리을(를) 참조하세요.

S3 객체에 민감한 데이터가 많이 포함되어 있는 경우 조사 결과를 사용하여 해당 민감한 데이터 검색 결과를 탐색할 수도 있습니다. 민감한 데이터 조사 결과와 달리, 민감한 데이터 검색 결과는 Macie가 객체에서 발견한 각 유형의 민감한 데이터가 1,000건까지 발생했는지에 대한 상세한 위치 데이터를 제공합니다. S3 객체가 아카이브 파일(예: .tar 또는.zip 파일)인 경우 여기에는 Macie가 아카이브에서 추출한 개별 파일에 있는 민감한 데이터가 포함됩니다. (Macie는 민감한 데이터 조사 결과에 이 정보를 포함시키지 않습니다.) 민감한 데이터 조사 결과에 대한 자세한 내용은 민감한 데이터 검색 결과 저장 및 유지을(를) 참조하세요. Macie는 민감한 데이터 조사 결과 및 민감한 데이터 조사 결과의 위치 데이터에 동일한 스키마를 사용합니다.

민감한 데이터의 발생 위치 찾기

민감한 데이터의 발생 위치를 찾으려면, Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 다음 단계에서는 콘솔을 사용하여 민감한 데이터의 위치를 찾는 방법을 설명합니다.

프로그래밍 방식으로 민감한 데이터의 위치를 찾으려면, Amazon Macie API의 GetFindings 작업을 사용합니다. 조사 결과에 특정 유형의 민감한 데이터가 한 번 이상 발생한 위치에 대한 세부 정보가 포함된 경우, 조사 결과에 포함된 `occurrences` 객체는 이러한 세부 정보를 제공합니다. 자세한 내용은 민감한 데이터 위치에 대한 JSON 스키마 섹션을 참조하세요.

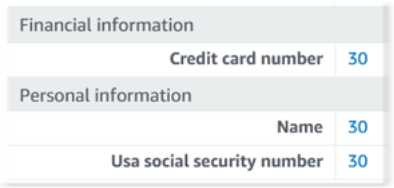
민감한 데이터의 발생 위치를 찾으려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.

> **Tip**
>
> 작업 페이지를 사용하여 특정 민감한 데이터 검색 작업의 모든 조사 결과를 표시할 수 있습니다. 이렇게 하려면, 탐색 창에서 작업을 선택한 다음, 작업 이름을 선택합니다. 세부 정보 패널 상단에서, 결과 표시를 선택한 다음, 조사 결과 표시를 선택합니다.

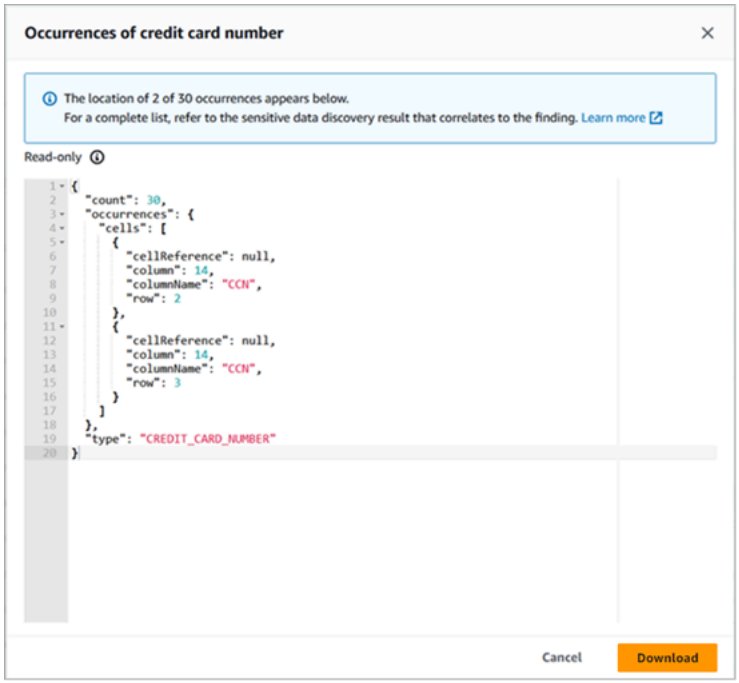
3. 조사 결과 페이지에서 찾으려는 민감한 데이터에 대한 조사 결과를 선택합니다. 세부 정보 패널에 조사 결과의 정보가 표시됩니다.
4. 세부 정보 패널에서 민감한 데이터 섹션으로 스크롤합니다. 이 섹션에서는 Macie가 영향을 받는 S3 객체에서 발견한 민감한 데이터의 범주 및 유형에 대한 정보를 제공합니다. 이 항목은 또한 Macie가 발견한 각 유형의 민감한 데이터 발생 횟수도 나타냅니다.

   예를 들어, 다음 이미지는 신용카드 번호가 30번, 이름이 30번, 미국 사회보장번호가 30번 나왔다는 조사 결과에 대한 세부 정보를 보여줍니다.



   조사 결과에 특정 유형의 민감한 데이터가 한 번 이상 발생한 위치에 대한 세부 정보가 포함된 경우, 발생 횟수는 링크입니다. 링크를 선택하면 세부 정보가 표시됩니다. Macie는 새 창을 열고 세부 정보를 JSON 형식으로 표시합니다.

   예를 들어, 다음 이미지는 영향을 받는 S3 객체에서 신용 카드 번호가 두 번 나오는 위치를 보여줍니다.



세부 정보를 JSON 파일로 저장하려면, 다운로드를 선택한 다음, 파일의 이름과 위치를 지정합니다.

5. (선택 사항) 모든 조사 결과의 세부 정보를 JSON 파일로 저장하려면 세부 정보 패널 상단에서 조사 결과 식별자(조사 결과 ID)를 선택합니다. Macie는 새 창을 열고 모든 세부 정보를 JSON 형식으로 표시합니다. 다운로드를 선택한 다음, 파일의 이름과 위치를 지정합니다.

영향을 받는 객체에서 각 유형의 민감한 데이터가 1,000개나 나오는 위치에 대한 세부 정보에 액세스하려면, 조사 결과에 대한 해당 민감한 데이터 검색 결과를 참조합니다. 이렇게 하려면, 패널의 세부 정보 섹션의 시작 부분으로 스크롤합니다. 그런 다음, 상세 결과 위치 필드에서 링크를 선택합니다. Macie는 Amazon S3 콘솔을 열고 해당 검색 결과가 포함된 파일 또는 폴더를 표시합니다.

Amazon Macie 조사 결과를 사용하여 민감한 데이터 샘플 검색

Amazon Macie가 조사 결과에 보고하는 민감한 데이터의 특성을 확인하기 위해 선택적으로 Macie를 구성하고 사용하여 개별 조사 결과에 의해 보고된 민감한 데이터의 샘플을 검색하고 공개할 수 있습니다. 여기에는 Macie가 관리형 데이터 식별자를 사용하여 탐지한 민감한 데이터와 사용자 지정 데이터 식별자의 기준과 일치하는 데이터가 포함됩니다. 샘플은 영향을 받는 Amazon Simple Storage Service(S3) 객체 및 버킷에 대한 조사를 맞춤 설정하는 데 도움이 될 수 있습니다.

조사 결과의 민감한 데이터 샘플을 검색하고 공개하는 경우 Macie는 다음과 같은 일반적인 작업을 수행합니다.

1. 검색 결과에 민감한 데이터가 개별적으로 나타나는 위치와 해당하는 민감한 데이터 검색 결과의 위치가 지정되어 있는지 확인합니다.
2. 해당하는 민감한 데이터 검색 결과를 평가하여 영향을 받는 S3 객체에 대한 메타데이터의 유효성과 개체 내 민감한 데이터 발생 여부에 대한 위치 데이터를 확인합니다.
3. 는 민감한 데이터 검색 결과의 데이터를 사용하여 검색 결과 보고된 민감한 데이터 중 처음 1~10개를 찾아 영향을 받는 S3 객체에서 각 항목의 처음 1~128자를 추출합니다. 검색 결과 여러 유형의 민감한 데이터가 보고되는 경우 Macie는 최대 100개 유형에 대해 이 작업을 수행합니다.
4. 사용자가 지정한 AWS Key Management Service(AWS KMS) 키를 사용하여 추출된 데이터를 암호화합니다.
5. 암호화된 데이터를 캐시에 임시로 저장하고 검토할 수 있도록 데이터를 표시합니다. 데이터는 전송 및 저장 시 항상 암호화됩니다.
6. 운영 문제 해결을 위해 일시적으로 추가 보존이 필요한 경우를 제외하고 추출 및 암호화 직후 캐시에서 데이터를 영구적으로 삭제합니다.

조사 결과의 민감한 데이터 샘플을 다시 검색하여 공개하도록 선택하면 Macie는 이러한 작업을 반복하여 샘플을 찾고, 추출하고, 암호화하고, 저장하고, 최종적으로는 삭제합니다.

Macie는 사용자 계정의 Macie 서비스 연결 역할을 사용하여 이러한 작업을 수행하지 않습니다. 대신 AWS Identity and Access Management(IAM) ID를 사용하거나 Macie가 계정에서 IAM 역할을 수임하도록 허용합니다. 사용자 또는 역할이 필수 리소스 및 데이터에 액세스할 수 있는 경우 조사 결과의 민감한 데이터 샘플을 검색하고 공개할 수 있으며 필요한 작업을 수행할 수 있습니다. 모든 필수 조치가 로그인AWS CloudTrail되어 있습니다.

> **Important**
>
> 사용자 지정 IAM 정책을 사용하여 이 기능에 대한 액세스를 제한하는 것이 좋습니다. 추가 액세스 제어를 위해서는 검색되는 민감한 데이터 샘플의 암호화 전용 AWS KMS key 서버를 만들고, 민감한 데이터 샘플을 검색하고 공개할 수 있어야 하는 보안 주체만 키 사용을 제한하는 것이 좋습니다.
>
> 이 기능에 대한 액세스를 제어하는 데 사용할 수 있는 권장 사항 및 정책의 예는 AWS보안 블로그의 Amazon Macie를 사용하여 S3 버킷의 민감한 데이터를 미리 보는 방법 블로그 게시물을 참조하세요.

이 섹션의 항목에서는 검색 결과에 대한 중요 데이터 샘플을 검색하고 공개하기 위해 Macie를 구성하고 사용하는 방법을 설명합니다. 아시아 태평양(오사카) 및 이스라엘(텔아비브) 리전을 제외하고 Macie를 현재 이용할 수 있는 모든 AWS 리전 에서 이러한 작업을 수행할 수 있습니다.

주제

- 조사 결과의 민감한 데이터 샘플을 검색하기 위한 구성 옵션 및 요구 사항
- 조사 결과와 함께 민감한 데이터 샘플을 검색하고 공개하도록 Amazon Macie 구성
- 조사 결과를 사용하여 민감한 데이터 샘플 검색 및 공개

조사 결과의 민감한 데이터 샘플을 검색하기 위한 구성 옵션 및 요구 사항

Amazon Macie를 구성하고 사용하여 Macie가 개별 조사 결과에서 보고하는 민감한 데이터의 샘플을 검색하고 공개할 수 있습니다(선택 사항). 조사 결과의 민감한 데이터 샘플을 검색하여 공개하는 경우 Macie는 해당 민감한 데이터 검색 결과의 데이터를 사용하여 영향을 받는 Amazon Simple Storage Service(S3) 객체에서 민감한 데이터의 발생 위치를 찾습니다. 그런 다음, Macie는 영향을 받는 객체에서 해당 사건의 샘플을 추출합니다. Macie는 지정한 AWS Key Management Service(AWS KMS)키로 추출된 데이터를 암호화하고 암호화된 데이터를 캐시에 임시로 저장한 다음, 조사 결과에 대한 결과에서 해당 데이터를 반환합니다. Macie는 운영 문제 해결을 위해 일시적으로 추가 보존이 필요한 경우를 제외하고 추출 및 암호화 직후 캐시에서 데이터를 영구적으로 삭제합니다.

Macie는 사용자 계정의 Macie 서비스 연결 역할을 사용하여 영향을 받는 S3 객체에서 민감한 데이터 샘플을 찾거나, 검색하거나, 암호화하거나, 공개하지 않습니다. 대신 Macie는 사용자가 계정에 구성한 설정과 리소스를 사용합니다. Macie에서 설정을 구성하는 경우 영향을 받는 S3 객체에 액세스하는 방법을 지정하세요. 또한 샘플을 암호화하는 데 사용할 AWS KMS key를 지정합니다. 아시아 태평양(오사카) 및 이스라엘(텔아비브) 리전을 제외하고 현재 Macie를 사용할 수 있는 모든 AWS 리전에서 설정을 구성할 수 있습니다.

영향을 받는 S3 객체에 액세스하고 해당 객체에서 민감한 데이터 샘플을 검색하기 위한 두 가지 옵션이 있습니다. AWS Identity and Access Management(IAM) 사용자 보안 인증을 사용하거나 IAM 역할을 수임하도록 Macie를 구성할 수 있습니다.

- IAM 사용자 보안 인증 사용 - 이 옵션을 통해 계정의 각 사용자는 개별 IAM ID를 사용하여 샘플을 찾고, 검색하고, 암호화하고, 공개합니다. 즉, 사용자가 필수 리소스와 데이터에 액세스하고 필요한 작업을 수행하도록 허용되는 경우 조사 결과의 민감한 데이터 샘플을 검색하고 공개할 수 있습니다.
- IAM 역할 수임 - 이 옵션을 통해 Macie에 액세스 권한을 위임하는 IAM 역할을 생성합니다. 또한 역할에 대한 신뢰 및 권한 정책이 Macie의 역할 수임을 위한 모든 요구 사항을 충족하는지 확인합니다.

그런 다음 Macie는 계정 사용자가 조사 결과의 민감한 데이터 샘플을 찾고, 검색하고, 암호화하고, 공개하기로 선택할 때 해당 역할을 수임합니다.

조직의 위임된 Macie 관리자 계정, 조직의 Macie 멤버 계정, 독립 실행형 Macie 계정 등 모든 Macie 계정 유형의 각 구성을 사용할 수 있습니다.

다음 주제에서는 계정의 설정 및 리소스를 구성하는 방법을 결정하는 데 도움이 되는 옵션, 요구 사항, 고려 사항에 대해 설명합니다. 여기에는 IAM 역할에 연결할 신뢰 및 권한 정책이 포함됩니다. 민감한 데이터 샘플을 검색하고 공개하는 데 사용할 수 있는 추가 권장 사항 및 정책의 예는 AWS 보안 블로그의 How to use Amazon Macie to preview sensitive data in S3 buckets 블로그 게시물을 참조하세요.

주제

사용할 액세스 방법 결정

AWS 환경에 가장 적합한 구성을 결정하는 경우 주요 고려 사항은 중앙에서 조직으로 관리되는 여러 Amazon Macie 계정이 환경에 포함되어 있는지 여부입니다. 조직의 위임된 Macie 관리자인 경우 IAM 역할을 수임하도록 Macie를 구성하면 조직 계정의 영향을 받는 S3 객체에서 민감한 데이터 샘플을 효율적으로 검색할 수 있습니다. 이 접근 방식을 사용하면 관리자 계정에 IAM 역할을 생성할 수 있습니다. 또한 해당하는 각 멤버 계정에 IAM 역할을 생성합니다. 관리자 계정의 역할은 Macie에 액세스 권한을 위임합니다. 멤버 계정의 역할은 관리자 계정의 역할에 크로스 계정 액세스 권한을 위임합니다. 구현되면 역할 체인을 사용하여 멤버 계정의 영향을 받는 S3 객체에 액세스할 수 있습니다.

또한 기본적으로 개별 조사 결과에 직접 액세스할 수 있는 사람이 누구인지도 고려합니다. 조사 결과의 민감한 데이터 샘플을 검색하고 공개하려면 사용자에게 먼저 조사 결과에 대한 액세스 권한이 있어야 합니다.

- 민감한 데이터 검색 작업 – 작업을 생성한 계정만 해당 작업이 생성한 조사 결과에 액세스할 수 있습니다. Macie 관리자 계정인 경우 조직 내 모든 계정의 S3 버킷에 있는 객체를 분석하도록 작업을 구성할 수 있습니다. 따라서 작업을 통해 멤버 계정이 소유한 버킷의 객체에 대한 조사 결과가 생성될 수 있습니다. 멤버 계정이나 독립 실행형 Macie 계정이 있는 경우 해당 계정이 소유한 버킷의 객체만 분석하도록 작업을 구성할 수 있습니다.

- 자동화된 민감한 데이터 검색 – Macie 관리자 계정만 조직의 계정을 대상으로 자동화된 검색이 생성하는 조사 결과에 액세스할 수 있습니다. 멤버 계정은 이러한 조사 결과에 액세스할 수 없습니다. 독립 실행형 Macie 계정인 경우 본인의 계정을 대상으로만 자동 검색이 생성하는 조사 결과에 액세스할 수 있습니다.

IAM 역할을 사용하여 영향을 받는 S3 객체에 액세스하려는 경우 다음 사항도 고려하세요.

- 객체에서 민감한 데이터의 발생 위치를 찾으려면 조사 결과의 해당하는 민감한 데이터 검색 결과를 Macie가 해시 기반 메시지 인증 코드(HMAC) AWS KMS key로 서명한 S3 객체에 저장해야 합니다. Macie는 민감한 데이터 검색 결과의 무결성과 신뢰성을 확인할 수 있어야 합니다. 그러지 않으면 Macie가 민감한 데이터 샘플을 검색하는 IAM 역할을 수임하지 않습니다. 이는 계정의 S3 객체에 있는 데이터에 대한 액세스를 제한하기 위한 추가 가드레일입니다.
- 고객 관리형 AWS KMS key로 암호화된 객체에서 민감한 데이터 샘플을 검색하려면 IAM 역할이 키를 사용하여 데이터를 해독하도록 허용해야 합니다. 더 구체적으로 말하면 키 정책은 역할이 `kms:Decrypt` 작업을 수행할 수 있도록 허용해야 합니다. 다른 서버측 암호화 유형의 경우 영향을 받는 객체를 해독하는 데 추가 권한이나 리소스가 필요하지 않습니다. 자세한 내용은 영향을 받는 S3 객체 암호 해독 섹션을 참조하세요.
- 다른 계정의 객체에서 민감한 데이터 샘플을 검색하려면 현재 해당 AWS 리전의 계정에 대해 위임된 Macie 관리자여야 합니다. 또한 다음과 같습니다.
  - 현재 해당 리전의 멤버 계정에 대해 Macie가 활성화되어 있어야 합니다.
  - 멤버 계정에는 Macie 관리자 계정의 IAM 역할에 크로스 계정 액세스 권한을 위임하는 IAM 역할이 있어야 합니다. 역할의 이름은 Macie 관리자 계정과 멤버 계정에서 동일해야 합니다.
  - 멤버 계정의 IAM 역할에 대한 신뢰 정책에는 구성에 맞는 올바른 외부 ID를 지정하는 조건이 포함되어야 합니다. 이 ID는 Macie 관리자 계정의 설정을 구성한 후 Macie에서 자동으로 생성하는 고유한 영숫자 문자열입니다. 신뢰 정책에서 외부 ID를 사용하는 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서에서 AWS 리소스에 대한 액세스 권한을 타사에 부여할 때 외부 ID를 사용하는 방법을 참조하세요.
  - 멤버 계정의 IAM 역할이 모든 Macie 요구 사항을 충족하는 경우 해당 계정의 객체에서 민감한 데이터 샘플을 검색하기 위해 멤버 계정에서 Macie 설정을 구성하고 활성화할 필요가 없습니다. Macie는 Macie 관리자 계정의 설정 및 IAM 역할과 멤버 계정의 IAM 역할만 사용합니다.

> **Tip**
>
> 계정이 대규모 조직에 속해 있는 경우 AWS CloudFormation 템플릿 및 스택 세트를 사용하여 조직의 멤버 계정에 대한 IAM 역할을 프로비저닝하고 관리하는 것을 고려하세요. 템

> 플릿과 스택 세트를 생성하고 사용하는 방법에 대한 자세한 내용은 AWS CloudFormation 사용 설명서를 참조하세요.
> 시작점으로 사용할 수 있는 CloudFormation 템플릿을 검토하고 선택적으로 다운로드하려면 Amazon Macie 콘솔을 사용하면 됩니다. 콘솔의 탐색 창에 있는 설정에서 샘플 표시를 선택합니다. 편집을 선택한 다음 멤버 역할 권한 및 CloudFormation 템플릿 보기를 선택합니다.

이 섹션의 다음 주제에서는 각 구성 유형의 추가 세부 정보와 고려 사항에 대해 설명합니다. IAM 역할의 경우 여기에는 역할에 연결할 신뢰 및 권한 정책이 포함됩니다. 어떤 유형의 구성이 사용자 환경에 가장 적합한지 잘 모르겠다면 AWS 관리자에게 도움을 요청하세요.

IAM 사용자 보안 인증을 사용하여 영향을 받는 S3 객체에 액세스

IAM 사용자 보안 인증을 사용하여 민감한 데이터 샘플을 검색하도록 Amazon Macie를 구성하는 경우 Macie 계정의 각 사용자는 IAM ID를 사용하여 개별 조사 결과에 대한 샘플을 찾고, 검색하고, 암호화하고, 공개합니다. 즉, 사용자의 IAM ID가 필수 리소스와 데이터에 액세스하고 필요한 작업을 수행하도록 허용된 경우 조사 결과의 민감한 데이터 샘플을 검색하고 공개할 수 있습니다. 모든 필수 조치가 로그인AWS CloudTrail되어 있습니다.

특정 조사 결과의 민감한 데이터 샘플을 검색하고 공개하려면 사용자에게 조사 결과, 해당 민감한 데이터의 검색 결과, 영향을 받은 S3 버킷, 영향을 받은 S3 객체 등의 데이터와 리소스에 액세스할 수 있는 권한이 있어야 합니다. 또한 해당하는 경우 영향을 받는 객체를 암호화하는 데 사용된 AWS KMS key와 민감한 데이터 샘플을 암호화하는 데 사용하도록 Macie를 구성한 AWS KMS key를 사용할 수 있도록 허용해야 합니다. IAM 정책, 리소스 정책 또는 기타 권한 설정이 필수 액세스를 거부하는 경우 사용자는 조사 결과의 샘플을 검색하거나 공개할 수 없습니다.

이러한 유형의 구성을 설정하려면 다음과 같은 일반적인 작업을 완료하세요.

1. 민감한 데이터 검색 결과의 리포지토리를 구성했는지 확인합니다.
2. 민감한 데이터 샘플의 암호화에 AWS KMS key를 사용하도록 구성합니다.
3. Macie에서 설정을 구성하기 위한 권한을 확인합니다.
4. Macie에서 설정을 구성하고 활성화합니다.

이러한 작업 수행에 대한 자세한 내용은 조사 결과와 함께 민감한 데이터 샘플을 검색하고 공개하도록 Amazon Macie 구성 섹션을 참조하세요.

영향을 받는 S3 객체에 액세스하기 위해 IAM 역할 수임

IAM 역할을 수임하여 민감한 데이터 샘플을 검색하도록 Amazon Macie를 구성하려면 먼저 Macie에 액세스 권한을 위임하는 IAM 역할을 만듭니다. 역할에 대한 신뢰 및 권한 정책이 Macie의 역할 수임을 위한 모든 요구 사항을 충족하는지 확인합니다. Macie 계정 사용자가 조사 결과의 민감한 데이터 샘플을 검색하고 공개하도록 선택하면 Macie는 영향을 받은 S3 객체에서 샘플을 검색하는 역할을 수임합니다. Macie는 사용자가 조사 결과의 샘플을 검색하고 공개하도록 선택한 경우에만 역할을 수임합니다. Macie는 역할을 수임하기 위해 AWS Security Token Service(AWS STS) API의 AssumeRole 작업을 사용합니다. 모든 필수 조치가 로그인AWS CloudTrail되어 있습니다.

특정 조사 결과의 민감한 데이터 샘플을 검색하고 공개하려면 사용자가 조사 결과, 해당 민감한 데이터의 검색 결과, 민감한 데이터 샘플을 암호화하는 데 사용하도록 Macie를 구성한 AWS KMS key에 액세스할 수 있어야 합니다. IAM 역할은 Macie가 영향을 받는 S3 버킷 및 영향을 받는 S3 객체에 액세스할 수 있도록 허용해야 합니다. 또한 해당되는 경우 해당 역할은 영향을 받는 객체를 암호화하는 데 사용된 AWS KMS key를 사용할 수 있어야 합니다. IAM 정책, 리소스 정책 또는 기타 권한 설정이 필수 액세스를 거부하는 경우 사용자는 조사 결과의 샘플을 검색하거나 공개할 수 없습니다.

이러한 유형의 구성을 설정하려면 다음과 같은 일반적인 작업을 완료하세요. 조직의 멤버 계정인 경우 Macie 관리자와 함께 계정의 설정 및 리소스 구성 여부와 구성 방법을 결정합니다.

1. 다음을 정의합니다.
   - Macie에 수임할 IAM 역할의 이름 계정이 조직에 속해 있는 경우 이 이름은 위임된 Macie 관리자 계정과 조직의 각 해당 멤버 계정에 대해 동일해야 합니다. 그러지 않으면 Macie 관리자는 해당 멤버 계정의 영향을 받는 S3 객체에 액세스할 수 없습니다.
   - IAM 역할에 연결할 IAM 권한 정책의 이름 계정이 조직에 속해 있는 경우 조직의 각 해당 멤버 계정에 대해 동일한 정책 이름을 사용하는 것이 좋습니다. 이를 통해 멤버 계정의 역할 프로비저닝 및 관리를 간소화할 수 있습니다.
2. 민감한 데이터 검색 결과의 리포지토리를 구성했는지 확인합니다.
3. 민감한 데이터 샘플의 암호화에 AWS KMS key를 사용하도록 구성합니다.
4. Macie에서 IAM 역할을 생성하고 설정을 구성하기 위한 권한을 확인합니다.
5. 조직의 위임된 Macie 관리자이거나 독립 실행형 Macie 계정인 경우:
   a. 계정에 대한 IAM 역할을 생성하고 구성합니다. 역할에 대한 신뢰 및 권한 정책이 Macie의 역할 수임을 위한 모든 요구 사항을 충족하는지 확인합니다. 이러한 요구 사항에 대한 자세한 내용은 다음 주제를 참조하세요.
   b. Macie에서 설정을 구성하고 활성화합니다. 그러면 Macie가 구성을 위한 외부 ID를 생성합니다. 조직의 Macie 관리자인 경우 이 ID를 기록해 두세요. 해당되는 각 멤버 계정의 IAM 역할에 대한 신뢰 정책에 이 ID가 지정되어 있어야 합니다.

6. 조직의 멤버 계정인 경우:

   a. 계정의 IAM 역할에 대한 신뢰 정책에 지정할 외부 ID를 Macie 관리자에게 요청하세요. 또한 생성할 IAM 역할 및 권한 정책의 이름을 확인합니다.

   b. 계정에 대한 IAM 역할을 생성하고 구성합니다. 역할에 대한 신뢰 및 권한 정책이 Macie 관리자가 역할을 수임하는 데 필요한 모든 요구 사항을 충족하는지 확인합니다. 이러한 요구 사항에 대한 자세한 내용은 다음 주제를 참조하세요.

   c. (선택 사항) 사용자 계정의 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색하고 공개하려면 Macie에서 설정을 구성하고 활성화합니다. Macie가 IAM 역할을 수임하여 샘플을 검색하도록 하려면 먼저 계정에서 추가 IAM 역할을 생성하고 구성합니다. 이 추가적인 역할에 대한 신뢰 및 권한 정책이 Macie의 역할 수임을 위한 모든 요구 사항을 충족하는지 확인합니다. 그런 다음 Macie에서 설정을 구성하고 추가 역할의 이름을 지정합니다. 역할의 정책 요구 사항에 대한 자세한 내용은 다음 주제를 참조하세요.

이러한 작업 수행에 대한 자세한 내용은 조사 결과와 함께 민감한 데이터 샘플을 검색하고 공개하도록 Amazon Macie 구성 섹션을 참조하세요.

영향을 받는 S3 객체에 액세스하도록 IAM 역할 구성

IAM 역할을 사용하여 영향을 받는 S3 객체에 액세스하려면 먼저 Amazon Macie에 액세스 권한을 위임하는 역할을 생성하고 구성합니다. 역할에 대한 신뢰 및 권한 정책이 Macie의 역할 수임을 위한 모든 요구 사항을 충족하는지 확인합니다. 이 작업을 수행하는 방법은 보유하고 있는 Macie 계정의 유형에 따라 다릅니다.

다음 섹션에서는 각 Macie 계정 유형의 IAM 역할에 연결할 신뢰 및 권한 정책에 대해 자세히 설명합니다. 보유한 계정 유형에 해당하는 섹션을 선택하세요.

> **Note**
>
> 조직의 멤버 계정인 경우 계정에 2개의 IAM 역할을 생성하고 구성해야 할 수도 있습니다.
>
> - Macie 관리자가 계정의 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색하고 공개할 수 있도록 허용하려면 관리자 계정이 수임할 수 있는 역할을 생성하고 구성합니다. 자세한 내용을 보려면 Macie 멤버 계정 섹션을 선택합니다.
> - 본인 계정의 영향을 받은 S3 객체에서 민감한 데이터 샘플을 검색하고 공개하려면 Macie가 수임할 수 있는 역할을 생성하고 구성합니다. 자세한 내용을 보려면 독립 실행형 Macie 계정 섹션을 선택합니다.

IAM 역할을 생성하고 구성하기 전에 Macie 관리자와 함께 계정에 적합한 구성을 결정합니다.

IAM을 사용하여 역할을 생성하는 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 사용자 지정 신뢰 정책을 사용하여 역할 생성을 참조하세요.

Macie 관리자 계정

조직의 위임된 Macie 관리자인 경우 먼저 IAM 정책 편집기를 사용하여 IAM 역할에 대한 권한 정책을 생성합니다. 정책은 다음과 같아야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "AssumeMacieRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::*:role/IAMRoleName"
        }
    ]
}
```

여기서 *IAMRoleName*은 조직 내 계정의 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색할 때 Macie가 수임할 IAM 역할의 이름입니다. 이 값을 자신의 계정 또는 조직의 해당 멤버 계정에 대해 생성할 계획인 역할의 이름으로 바꿉니다. 이 이름은 Macie 관리자 계정과 해당하는 각 멤버 계정에서 동일해야 합니다.

> **Note**
>
> 앞의 권한 정책에서 첫 번째 문에 있는 `Resource` 요소는 와일드카드 문자(*)를 사용합니다. 이를 통해 연결된 IAM 엔터티는 조직이 소유한 모든 S3 버킷에서 객체를 검색할 수 있습니다. 특정 버킷에 대해서만 이 액세스를 허용하려면 와일드카드 문자를 각 버킷의 Amazon 리소스 이름(ARN)으로 바꿉니다. 예를 들어 DOC-EXAMPLE-BUCKET이라는 버킷의 객체에만 액세스를 허용하려면 요소를 다음과 같이 바꿉니다.
> `"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"`
> 개별 계정의 특정 S3 버킷에 있는 객체에 대한 액세스를 제한할 수도 있습니다. 이렇게 하려면 각 해당 계정의 IAM 역할에 대한 권한 정책에서 `Resource` 요소에 버킷 ARN을 지정합니다. 자세한 내용과 예제는 AWS Identity and Access Management 사용 설명서의 IAM JSON 정책 요소: Resource를 참조하세요.

IAM 역할에 대한 권한 정책을 생성한 후 역할을 생성하고 구성합니다. IAM 콘솔을 사용하여 이 작업을 수행하는 경우 역할에 대한 신뢰할 수 있는 엔터티 유형으로 사용자 지정 신뢰 정책을 선택합니다. 역할에 대해 신뢰할 수 있는 엔터티를 정의하는 신뢰 정책의 경우 다음을 지정합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

여기서 *accountID*는 AWS 계정의 계정 ID입니다. 이 값을 12자리 계정 ID로 바꿉니다.

앞의 신뢰 정책에서:

- `Principal` 요소는 영향을 받는 S3 개체인 `reveal-samples.macie.amazonaws.com`에서 민감한 데이터 샘플을 검색할 때 Macie가 사용하는 서비스 주체를 지정합니다.
- `Action` 요소는 서비스 주체가 수행할 수 있는 작업인 AWS Security Token Service(AWS STS) API의 AssumeRole 작업을 지정합니다.
- `Condition` 요소는 aws:SourceAccount 전역 조건 컨텍스트 키를 사용하는 조건을 정의합니다. 이 조건에 따라 지정된 작업을 수행할 수 있는 계정이 결정됩니다. 이 경우 Macie가 지정된 계정(*`accountID`*)에 대해서만 역할을 수임할 수 있습니다. 이 조건은 Macie가 거래 중에 AWS STS와 혼동된 대리자로 사용되는 것을 방지하는 데 도움이 됩니다.

IAM 역할에 대한 신뢰 정책을 정의한 후 권한 정책을 역할에 연결합니다. 이 권한 정책은 역할 생성을 시작하기 전에 생성한 권한 정책이어야 합니다. 그런 다음 IAM의 나머지 단계를 완료하여 역할 생성 및 구성을 완료합니다. 완료하면 Macie에서 설정을 구성하고 활성화합니다.

Macie 멤버 계정

Macie 멤버 계정이고 Macie 관리자가 계정의 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색하여 공개할 수 있도록 허용하려면 먼저 Macie 관리자에게 다음 정보를 요청합니다.

- 생성하려는 IAM 역할의 이름 사용자 계정의 이름과 조직의 Macie 관리자 계정 이름이 동일해야 합니다.
- 역할에 연결할 IAM 권한 정책의 이름
- 역할에 대한 신뢰 정책에 지정할 외부 ID 이 ID는 Macie 관리자 구성을 위해 Macie에서 생성한 외부 ID여야 합니다.

이 정보를 받은 후 IAM 정책 편집기를 사용하여 역할에 대한 권한 정책을 생성합니다. 정책은 다음과 같아야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
```

```
            ]
        }
    ]
}
```

앞의 권한 정책은 연결된 IAM 엔터티가 계정의 모든 S3 버킷에서 객체를 검색하도록 허용합니다. 이는 정책의 Resource 요소가 와일드카드 문자(*)를 사용하기 때문입니다. 특정 버킷에 대해서만 이 액세스를 허용하려면 와일드카드 문자를 각 버킷의 Amazon 리소스 이름(ARN)으로 바꿉니다. 예를 들어 DOC-EXAMPLE-BUCKET2이라는 버킷의 객체에만 액세스를 허용하려면 요소를 다음과 같이 바꿉니다.

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
```

자세한 내용과 예제는 AWS Identity and Access Management 사용 설명서의 IAM JSON 정책 요소: Resource를 참조하세요.

IAM 역할에 대한 권한 정책을 생성한 후 역할을 생성합니다. IAM 콘솔을 사용하여 역할을 생성하는 경우 역할의 신뢰할 수 있는 엔터티 유형으로 사용자 지정 신뢰 정책을 선택합니다. 역할에 대해 신뢰할 수 있는 엔터티를 정의하는 신뢰 정책의 경우 다음을 지정합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieAdminRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::administratorAccountID:role/IAMRoleName"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "externalID",
                    "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
                }
            }
        }
    ]
}
```

앞의 정책에서 자리 표시자 값을 AWS 환경에 맞는 올바른 값으로 바꿉니다.

- 여기에서 *administratorAccountID*는 Macie 관리자 계정의 12자리 계정 ID입니다.
- *IAMRoleName*은 Macie 관리자 계정의 IAM 역할 이름입니다. 이는 Macie 관리자로부터 받은 이름이어야 합니다.
- *externalID*는 Macie 관리자로부터 받은 외부 ID입니다.

일반적으로 신뢰 정책을 통해 Macie 관리자는 계정의 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색하고 공개하는 역할을 수임할 수 있습니다. `Principal` 요소는 Macie 관리자 계정에 있는 IAM 역할의 ARN을 지정합니다. 이 역할은 Macie 관리자가 조직 내 계정의 민감한 데이터 샘플을 검색하고 공개하는 데 사용하는 역할입니다. `Condition` 블록은 역할을 수임할 수 있는 사람을 추가로 결정하는 2가지 조건을 정의합니다.

- 첫 번째 조건은 조직의 구성에 고유한 외부 ID를 지정합니다. 외부 ID에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 AWS 리소스에 대한 액세스 권한을 타사에 부여할 때 외부 ID를 사용하는 방법을 참조하세요.
- 두 번째 조건은 aws:PrincipalOrgID 전역 조건 컨텍스트 키를 사용합니다. 키 값은 AWS Organizations(`${aws:ResourceOrgID}`)에 있는 조직의 고유 식별자를 나타내는 동적 변수입니다. 이 조건은 AWS Organizations에서 동일한 조직에 속한 계정으로만 액세스를 제한합니다. Macie에서 초대를 수락하여 조직에 가입한 경우 정책에서 이 조건을 제거합니다.

IAM 역할에 대한 신뢰 정책을 정의한 후 권한 정책을 역할에 연결합니다. 이 권한 정책은 역할 생성을 시작하기 전에 생성한 권한 정책이어야 합니다. 그런 다음 IAM의 나머지 단계를 완료하여 역할 생성 및 구성을 완료합니다. Macie에서 역할의 설정을 구성하고 입력하지 마세요.

독립 실행형 Macie 계정

독립 실행형 Macie 계정 또는 Macie 멤버 계정이고 본인 계정의 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색하고 공개하려면 먼저 IAM 정책 편집기를 사용하여 IAM 역할에 대한 권한 정책을 생성합니다. 정책은 다음과 같아야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
```

```
            "Resource": [
                "*"
            ]
        }
    ]
}
```

앞의 권한 정책에서 Resource 요소는 와일드카드 문자(*)를 사용합니다. 이를 통해 연결된 IAM 엔터티는 사용자 계정의 모든 S3 버킷에서 객체를 검색할 수 있습니다. 특정 버킷에 대해서만 이 액세스를 허용하려면 와일드카드 문자를 각 버킷의 Amazon 리소스 이름(ARN)으로 바꿉니다. 예를 들어 DOC-EXAMPLE-BUCKET3이라는 버킷의 객체에만 액세스를 허용하려면 요소를 다음과 같이 바꿉니다.

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET3/*"
```

자세한 내용과 예제는 AWS Identity and Access Management 사용 설명서의 IAM JSON 정책 요소: Resource를 참조하세요.

IAM 역할에 대한 권한 정책을 생성한 후 역할을 생성합니다. IAM 콘솔을 사용하여 역할을 생성하는 경우 역할의 신뢰할 수 있는 엔터티 유형으로 사용자 지정 신뢰 정책을 선택합니다. 역할에 대해 신뢰할 수 있는 엔터티를 정의하는 신뢰 정책의 경우 다음을 지정합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

여기서 *accountID*는 AWS 계정의 계정 ID입니다. 이 값을 12자리 계정 ID로 바꿉니다.

앞의 신뢰 정책에서:

- `Principal` 요소는 영향을 받는 S3 객체인 `reveal-samples.macie.amazonaws.com`에서 민감한 데이터 샘플을 검색하고 공개할 때 Macie가 사용하는 서비스 주체를 지정합니다.
- `Action` 요소는 서비스 주체가 수행할 수 있는 작업인 AWS Security Token Service(AWS STS) API의 AssumeRole 작업을 지정합니다.
- `Condition` 요소는 aws:SourceAccount 전역 조건 컨텍스트 키를 사용하는 조건을 정의합니다. 이 조건에 따라 지정된 작업을 수행할 수 있는 계정이 결정됩니다. 이를 통해 Macie는 지정된 계정(*`accountID`*)에 대해서만 역할을 수임할 수 있습니다. 이 조건은 Macie가 거래 중에 AWS STS와 혼동된 대리자로 사용되는 것을 방지하는 데 도움이 됩니다.

IAM 역할에 대한 신뢰 정책을 정의한 후 권한 정책을 역할에 연결합니다. 이 권한 정책은 역할 생성을 시작하기 전에 생성한 권한 정책이어야 합니다. 그런 다음 IAM의 나머지 단계를 완료하여 역할 생성 및 구성을 완료합니다. 완료하면 Macie에서 설정을 구성하고 활성화합니다.

영향을 받는 S3 객체 암호 해독

Amazon S3는 S3 객체에 대한 여러 암호화 옵션을 지원합니다. 이러한 옵션의 대부분은 영향을 받는 객체에서 민감한 데이터 샘플을 해독하고 검색하는 데 IAM 사용자나 역할에 추가 리소스나 권한이 필요하지 않습니다. 이는 Amazon S3 관리형 키 또는 AWS 관리형 AWS KMS key를 사용한 서버측 암호화를 사용하여 암호화된 객체의 경우입니다.

하지만 고객 관리형 AWS KMS key를 사용하여 S3 객체를 암호화하는 경우 객체에서 민감한 데이터 샘플의 암호를 해독하고 검색하려면 추가 권한이 필요합니다. 더 구체적으로 말하면 KMS 키에 대한 키 정책은 IAM 사용자 또는 역할이 `kms:Decrypt` 작업을 수행할 수 있도록 허용해야 합니다. 그렇지 않으면 오류가 발생하고 Macie가 객체에서 샘플을 검색하지 않습니다. IAM 사용자에게 해당 액세스 권한을 제공하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서에서 Authentication and access control for AWS KMS를 참조하세요.

IAM 역할에 이 액세스 권한을 제공하는 방법은 AWS KMS key를 소유한 계정이 다음 역할도 소유하는지 여부에 따라 달라집니다.

- 동일한 계정이 KMS 키와 역할을 소유한 경우 해당 계정의 사용자가 키 정책을 업데이트해야 합니다.
- 한 계정이 KMS 키를 소유하고 다른 계정이 역할을 소유한 경우 키를 소유한 계정의 사용자는 키에 대한 크로스 계정 액세스를 허용해야 합니다.

이 주제에서는 S3 객체에서 민감한 데이터 샘플을 검색하기 위해 만든 IAM 역할에 대해 이러한 작업을 수행하는 방법에 대해 설명합니다. 또한 두 시나리오에 대한 예도 제공합니다. 다른 시나리오에서 고객 관리형 AWS KMS keys에 대한 액세스를 허용하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 Authentication and access control for AWS KMS를 참조하세요.

고객 관리형 키에 대한 동일 계정 액세스 허용

동일한 계정이 AWS KMS key와 IAM 역할을 모두 소유하고 있는 경우 해당 계정의 사용자는 키의 정책에 문을 추가해야 합니다. 추가 문은 IAM 역할이 키를 사용하여 데이터를 해독할 수 있도록 허용해야 합니다. 키 정책을 수정하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 변경을 참조하세요.

성명문에서:

- `Principal` 요소는 IAM 역할의 Amazon 리소스 이름(ARN)을 지정해야 합니다.
- `Action` 배열은 `kms:Decrypt` 작업을 지정해야 합니다. 이 작업은 키로 암호화된 객체를 해독하기 위해 IAM 역할이 수행하도록 허용되어야 하는 유일한 AWS KMS 작업입니다.

다음은 KMS 키 정책에 추가할 수 있는 성명문의 예입니다.

```
{
    "Sid": "Allow the Macie reveal role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/IAMRoleName"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

이전 예제에서:

- `Principal` 요소의 `AWS` 필드는 계정에 있는 IAM 역할의 ARN을 지정합니다. 이를 통해 역할이 정책 문에 지정된 작업을 수행할 수 있습니다. *123456789012*는 계정 ID의 예입니다. 이 값을 역할을 소유한 계정의 계정 ID 및 KMS 키로 바꿉니다. *IAMRoleName*은 예시 이름입니다. 이 값을 계정에 있는 IAM 역할의 이름으로 바꿉니다.
- `Action` 배열은 키로 암호화된 KMS 키-암호 해독 사이퍼텍스트를 사용하여 IAM 역할이 수행할 수 있는 작업을 지정합니다.

이 성명문을 키 정책에 추가하는 위치는 정책에 현재 포함되어 있는 구조 및 요소에 따라 달라집니다. 정책에 성명문을 추가할 때 구문이 올바른지 확인합니다. 키 정책은 JSON 형식입니다. 즉, 정책에 성명문을 추가하는 위치에 따라 명령문 앞이나 뒤에 쉼표를 추가해야 합니다.

고객 관리형 키에 대한 크로스 계정 액세스 허용

한 계정이 AWS KMS key를 소유하고(키 소유자) 다른 계정이 IAM 역할을 소유하는(역할 소유자) 경우 키 소유자는 역할 소유자에게 키에 대한 크로스 계정 액세스 권한을 제공해야 합니다. 이를 위한 한 가지 방법은 권한 부여를 사용하는 것입니다. 권한 부여는 AWS보안 주체가 암호화 작업에서 KMS 키를 사용할 수 있도록 하는 정책 도구입니다. 권한 부여에 대해 자세히 알아보려면 AWS Key Management Service개발자 안내서의 AWS KMS 권한 부여를 참조하세요.

이 접근 방식을 사용하면 키 소유자는 먼저 키의 정책에서 역할 소유자가 키에 대한 권한을 만들 수 있도록 허용하는지 확인합니다. 그러면 역할 소유자가 키에 대한 권한 부여를 생성합니다. 권한을 부여하면 계정의 IAM 역할에 관련 권한이 위임됩니다. 이 키를 사용하면 역할이 키로 암호화된 S3 객체를 해독할 수 있습니다.

1단계: 키 정책 업데이트

키 정책에서 키 소유자는 역할 소유자가 자신(역할 소유자) 계정에서 IAM 역할에 대한 권한 부여를 생성할 수 있도록 허용하는 문이 정책에 포함되어 있는지 확인해야 합니다. 이 문에서 `Principal` 요소는 역할 소유자 계정의 ARN을 지정해야 합니다. `Action` 배열은 `kms:CreateGrant` 작업을 지정해야 합니다. `Condition` 블록은 지정된 작업에 대한 액세스를 필터링할 수 있습니다. 다음은 KMS 키를 위한 정책 안의 성명문의 예입니다.

```
{
    "Sid": "Allow a role in an account to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/IAMRoleName"
        },
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": "Decrypt"
```

```
        }
    }
}
```

이전 예제에서:

- `Principal` 요소의 `AWS` 필드는 역할 소유자 계정의 ARN을 지정합니다. 계정에서 정책 정책에 지정된 작업을 수행할 수 있도록 허용합니다. *111122223333*은 계정 ID의 예입니다. 이 값을 역할 소유자 계정의 계정 ID로 바꿉니다.
- `Action` 배열은 역할 소유자가 KMS 키에 대해 수행할 수 있는 작업(키에 대한 권한 부여 생성)을 지정합니다.
- `Condition` 블록은 조건 연산자와 다음 조건 키를 사용하여 역할 소유자가 KMS 키에 대해 수행할 수 있는 작업에 대한 액세스를 필터링합니다.
  - kms:GranteePrincipal - 이 조건을 사용하면 역할 소유자는 자신의 계정에 있는 IAM 역할의 ARN인 지정된 피부여자 보안 주체에 대해서만 권한 부여를 생성할 수 있습니다. 해당 ARN에서 *111122223333#* 예시계정 ID입니다. 이 값을 역할 소유자 계정의 계정 ID로 바꿉니다. *IAMRoleName*은 예시 이름입니다. 이 값을 역할 소유자의 계정에 있는 IAM 역할의 이름으로 바꿉니다.
  - kms:GrantOperations - 이 조건을 사용하면 역할 소유자가 AWS KMS `Decrypt` 작업(키를 사용하여 암호화된 사이퍼텍스트 해독)을 수행할 수 있는 권한만 위임할 수 있는 권한을 만들 수 있습니다. 이는 역할 소유자가 KMS 키에 대해 다른 작업을 수행할 수 있는 권한을 위임하는 권한을 만들지 못하도록 합니다. `Decrypt` 작업은 키로 암호화된 객체를 해독하기 위해 IAM 역할이 수행하도록 허용되어야 하는 유일한 AWS KMS 작업입니다.

키 소유자가 키 정책에 이 문을 추가하는 위치는 현재 정책에 포함된 구조와 요소에 따라 달라집니다. 키 소유자가 성명문을 추가할 때, 구문이 유효한지 확인해야 합니다. 키 정책은 JSON 형식입니다. 이는 키 소유자가 정책에 성명문을 정책에 추가하는 위치에 따라 성명문 앞이나 뒤에 쉼표를 추가해야 합니다. 키 정책을 수정하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 변경을 참조하세요.

2단계: 권한 부여 생성

키 소유자가 필요에 따라 키 정책을 업데이트하면 역할 소유자가 키에 대한 권한 부여를 생성합니다. 이 권한을 부여하면 해당 권한은 (역할 소유자의) 계정에 있는 IAM 역할에 위임됩니다. 역할 소유자는 권한을 생성하기 전에 `kms:CreateGrant` 작업을 수행하도록 허용되었는지 확인해야 합니다. 이 작업을 통해 기존 고객 관리형 AWS KMS key에 권한 부여를 추가할 수 있습니다.

권한 부여를 생성하기 위해 역할 소유자는 AWS Key Management Service API의 CreateGrant 작업을 사용할 수 있습니다. 역할 소유자는 권한 부여를 생성할 때 필수 파라미터에 다음 값을 지정해야 합니다.

- `KeyId` - KMS 키의 ARN KMS 키에 대한 크로스 계정 액세스의 경우 이 값은 ARN이어야 합니다. 키 ID일 수 없습니다.
- `GranteePrincipal` - 계정에 있는 IAM 역할의 ARN 이 값은 `arn:aws:iam::`*`111122223333`*`:role/`*`IAMRoleName`*이어야 합니다. 여기서 *`111122223333`*은 역할 소유자 계정의 계정 ID이고 *`IAMRoleName`*은 역할의 이름입니다.
- `Operations` - AWS KMS 암호 해독 작업(`Decrypt`). 이 작업은 KMS 키로 암호화된 객체를 해독하기 위해 IAM 역할이 수행하도록 허용되어야 하는 유일한 AWS KMS 작업입니다.

역할 소유자가 AWS Command Line Interface(AWS CLI)를 사용하는 경우 create-grant 명령을 실행하여 권한 부여를 생성할 수 있습니다. 다음 예에서는 이 작업을 수행하는 방법을 보여줍니다. 이 예제는 Microsoft Windows용으로 포맷되었으며 가독성을 높이기 위해 캐럿 (^) 줄 연속 문자를 사용합니다.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/IAMRoleName ^
--operations "Decrypt"
```

위치:

- `key-id`권한 부여를 적용할 KMS 키의 ARN을 지정합니다.
- `grantee-principal`은 권한 부여로 지정된 작업을 수행할 수 있는 IAM 역할의 ARN을 지정합니다. 이 값은 키 정책의 `kms:GranteePrincipal` 조건에 지정된 ARN과 일치해야 합니다.
- `operations`는 지정된 주체가 이 권한으로 수행할 수 있는 작업, 즉 키를 사용하여 암호화된 사이퍼 텍스트를 해독하는 작업을 지정합니다.

이 명령이 성공적으로 실행되면 다음과 비슷한 출력이 표시됩니다.

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

여기서 `GrantToken`은 생성된 권한 부여를 나타내는 고유하고 암호화되지 않은 가변 길이 base64 인코딩 문자열이며 `GrantId`은 권한 부여의 고유 식별자입니다.

조사 결과와 함께 민감한 데이터 샘플을 검색하고 공개하도록 Amazon Macie 구성

Macie가 개별적인 민감한 데이터 조사 결과에서 보고하는 민감한 데이터의 샘플을 검색하고 공개하도록 Amazon Macie를 선택적으로 구성하고 사용할 수 있습니다. 샘플을 통해 Macie가 발견한 민감한 데이터의 특성을 확인할 수 있습니다. 또한 영향을 받는 Amazon Simple Storage Service(S3) 객체 및 버킷에 대한 조사를 맞춤 설정하는 데 도움이 될 수 있습니다. 아시아 태평양(오사카)및 이스라엘(텔아비브) 리전을 제외하고 Macie를 현재 이용할 수 있는 모든 AWS 리전에서 민감한 데이터 샘플을 검색하고 공개할 수 있습니다.

조사 결과에 대한 민감한 데이터 샘플을 검색하고 공개하면, Macie는 해당하는 민감한 데이터 검색 결과의 데이터를 사용하여 영향을 받은 S3 객체의 민감한 데이터 발생 항목의 위치를 찾습니다. 그런 다음, Macie는 영향을 받는 객체에서 해당 사건의 샘플을 추출합니다. Macie는 지정한 AWS Key Management Service(AWS KMS)키로 추출된 데이터를 암호화하고 암호화된 데이터를 캐시에 임시로 저장한 다음, 조사 결과에 대한 결과에서 해당 데이터를 반환합니다. Macie는 운영 문제 해결을 위해 일시적으로 추가 보존이 필요한 경우를 제외하고 추출 및 암호화 직후 캐시에서 데이터를 영구적으로 삭제합니다.

조사 결과의 민감한 데이터 샘플을 검색하고 공개하려면 먼저 Macie 계정의 설정을 구성하고 활성화해야 합니다. 또한 계정에 대한 지원 리소스 및 권한을 구성해야 합니다. 이 섹션의 주제에서는 민감한 데이터 샘플을 검색하고 공개하도록 Macie를 구성하고 계정의 구성 상태를 관리하는 프로세스를 안내합니다.

주제

- 시작하기 전 준비 사항
- Amazon Macie 설정 구성 및 활성화
- Amazon Macie 설정 비활성화

> **Tip**
>
> 이 기능에 대한 액세스를 제어하는 데 사용할 수 있는 권장 사항 및 정책의 예는 AWS 보안 블로그의 Amazon Macie를 사용하여 S3 버킷의 민감한 데이터를 미리 보는 방법 블로그 게시물을 참조하세요.

시작하기 전 준비 사항

민감한 데이터 샘플을 검색하여 조사 결과를 공개하도록 Amazon Macie를 구성하기 전에 다음 작업을 완료하여 필요한 리소스와 권한이 있는지 확인하세요.

Tasks

- 1단계: 민감한 데이터 검색 결과의 리포지토리 구성
- 2단계: 영향을 받는 S3 객체에 액세스하는 방법 결정
- 3단계: AWS KMS key 구성
- 4단계: 권한 확인

민감한 데이터 샘플을 검색하고 공개하도록 Macie를 이미 구성한 상태에서 구성 설정만 변경하려는 경우 이 작업은 선택 사항입니다.

1단계: 민감한 데이터 검색 결과의 리포지토리 구성

조사 결과에 대한 민감한 데이터 샘플을 검색하고 공개하면, Macie는 해당하는 민감한 데이터 검색 결과의 데이터를 사용하여 영향을 받은 S3 객체의 민감한 데이터 발생 항목의 위치를 찾습니다. 따라서 민감한 데이터 검색 결과의 리포지토리를 구성했는지 확인하는 것이 중요합니다. 그렇지 않으면 Macie는 검색 및 공개하려는 민감한 데이터 샘플의 위치를 찾을 수 없게 됩니다.

계정에 이 리포지토리를 구성했는지 확인하려면 Amazon Macie 콘솔을 사용하여 탐색 창에서 검색 결과(설정 아래)를 선택하면 됩니다. 프로그래밍 방식으로 이 작업을 수행하려면 Amazon Macie API의 GetClassificationExportConfiguration 작업을 사용합니다. 민감한 데이터 검색 결과와 이 리포지토리를 구성하는 방법에 대한 자세한 내용은 민감한 데이터 검색 결과 저장 및 유지 섹션을 참조하세요.

2단계: 영향을 받는 S3 객체에 액세스하는 방법 결정

영향을 받는 S3 객체에 액세스하고 해당 객체에서 민감한 데이터 샘플을 검색하기 위한 두 가지 옵션이 있습니다. AWS Identity and Access Management(IAM) 사용자 보안 인증을 사용하도록 Macie를 구성할 수 있습니다. 또는 Macie에 액세스를 위임하는 IAM 역할을 수임하도록 Macie를 구성할 수도 있습니다. 조직의 위임된 Macie 관리자 계정, 조직의 Macie 멤버 계정, 독립 실행형 Macie 계정 등 모든 Macie 계정 유형의 각 구성을 사용할 수 있습니다. Macie에서 설정을 구성하기 전에, 사용할 액세스 방법을 결정합니다. 각 방법의 옵션과 요구 사항에 대한 자세한 내용은 조사 결과의 민감한 데이터 샘플을 검색하기 위한 구성 옵션 및 요구 사항 섹션을 참조하세요.

IAM 역할을 사용하려는 경우 Macie에서 설정을 구성하기 전에 역할을 생성하고 구성하세요. 또한 역할에 대한 신뢰 및 권한 정책이 Macie의 역할 수임을 위한 모든 요구 사항을 충족하는지 확인합니다.

여러 Macie 계정을 중앙에서 관리하는 조직에 속해 있는 계정의 경우 먼저 Macie 관리자와 함께 계정에 대한 역할 구성 여부와 구성 방법을 결정합니다.

3단계: AWS KMS key 구성

조사 결과의 민감한 데이터 샘플을 검색하여 공개하는 경우 Macie는 사용자가 지정한 AWS Key Management Service(AWS KMS) 키를 사용하여 샘플을 암호화합니다. 따라서 샘플을 암호화하는 데 어떤 AWS KMS key를 사용할지 결정해야 합니다. 키는 내 계정의 기존 KMS 키 또는 다른 계정이 소유하고 있는 기존 KMS 키일 수 있습니다. 다른 계정이 소유하고 있는 키를 사용하려면 해당 키의 Amazon 리소스 이름(ARN)이 필요합니다. Macie에서 구성 설정을 입력할 때 이 ARN을 지정해야 합니다.

이 KMS 키는 고객 관리형 대칭 암호화 키여야 합니다. 또한 Macie 계정과 동일한 AWS 리전의 활성화된 단일 리전 키여야 합니다. KMS 키는 외부 키 저장소에 있을 수 있습니다. 하지만 이 키는 AWS KMS 내에서 완전히 관리되는 키보다 속도가 느리고 안정성이 떨어질 수 있습니다. 지연 또는 가용성 문제로 인해 Macie가 검색 및 공개하려는 민감한 데이터 샘플을 암호화할 수 없는 경우 오류가 발생하고 Macie는 조사 결과에 대한 샘플을 반환하지 않습니다.

또한 키에 대한 키 정책에서는 적절한 보안 주체(IAM 역할, IAM 사용자 또는 AWS 계정)가 다음 작업을 수행할 수 있도록 허용해야 합니다.

- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

> **Important**
>
> 추가 액세스 제어 레이어로, 검색되는 민감한 데이터 샘플의 암호화 전용 KMS 키를 만들고, 민감한 데이터 샘플을 검색하고 공개할 수 있어야 하는 보안 주체만 키 사용을 제한하는 것이 좋습니다. 사용자가 키를 사용해 앞에 나온 작업을 수행할 수 없는 경우 Macie는 민감한 데이터 샘플을 검색하고 공개하라는 요청을 거부합니다. Macie는 조사 결과에 대해 어떠한 샘플도 반환하지 않습니다.

KMS 키 생성 및 구성에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 Managing keys를 참조하세요. 키 정책을 사용하여 KMS 키에 대한 액세스를 관리하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 Key policies in AWS KMS를 참조하세요.

4단계: 권한 확인

Macie에서 설정을 구성하기 전에 필요한 권한이 있는지도 확인하세요. 권한을 확인하려면 AWS Identity and Access Management(IAM)을 사용하여 IAM ID에 연결된 IAM 정책을 검토하세요. 그런 다음, 해당 정책의 정보와 수행할 수 있어야 하는 다음 작업 목록과 비교합니다.

Amazon Macie

Macie의 경우, 다음 작업을 수행할 수 있는지 확인합니다.

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

첫 번째 작업을 통해 Macie 계정에 액세스할 수 있습니다. 두 번째 작업을 통해 민감한 데이터 샘플을 검색하고 공개하기 위한 구성 설정을 변경할 수 있습니다. 여기에는 계정에 대한 구성 활성화 및 비활성화가 포함됩니다.

필요한 경우 `macie2:GetRevealConfiguration` 작업을 수행할 수도 있는지 확인합니다. 이 작업을 통해 현재 구성 설정과 계정의 현재 구성 상태를 검색할 수 있습니다.

AWS KMS

Amazon Macie 콘솔을 사용하여 구성 설정을 입력하려는 경우 다음 AWS Key Management Service(AWS KMS) 작업을 수행할 수 있는 권한이 있는지도 확인합니다.

- `kms:DescribeKey`
- `kms:ListAliases`

이러한 작업을 통해 계정의 AWS KMS keys에 대한 정보를 검색할 수 있습니다. 그러면 설정을 입력할 때 이러한 키 중 하나를 선택할 수 있습니다.

IAM

민감한 데이터 샘플을 검색하고 공개하는 IAM 역할을 수임하도록 Macie를 구성하려는 경우 IAM 작업 `iam:PassRole`을 수행할 수 있는지도 확인하세요. 이 작업을 수행하면 Macie에 역할을 전달할 수 있으며, 그러면 Macie가 역할을 수임할 수 있습니다. 계정의 구성 설정을 입력하면 Macie는 계정에 역할이 존재하고 올바르게 구성되었는지 확인할 수도 있습니다.

필요한 작업을 수행할 수 없는 경우 다음 단계로 진행하기 전에 AWS 관리자에게 도움을 요청하세요.

Amazon Macie 설정 구성 및 활성화

필요한 리소스와 권한이 있는지 확인한 후에는 Amazon Macie에서 설정을 구성하고 계정의 구성을 활성화할 수 있습니다.

여러 Macie 계정을 중앙에서 관리하는 조직에 속해 있는 계정의 경우 계정 설정을 구성하거나 나중에 변경하기 전에 다음 사항에 유의하세요.

- 멤버 계정인 경우 Macie 관리자와 협업하여 계정의 설정 구성 여부와 구성 방법을 결정합니다. Macie 관리자가 계정의 올바른 구성 설정이 무엇인지 결정하는 데 도움을 줄 수 있습니다.
- Macie 관리자 계정이며, 영향을 받는 S3 객체에 액세스하기 위한 설정을 변경하는 경우 변경 사항이 조직의 다른 계정 및 리소스에 영향을 미칠 수 있습니다. 이는 현재 Macie가 민감한 데이터 샘플을 검색하는 AWS Identity and Access Management(IAM) 역할을 수임하도록 구성되어 있는지 여부에 따라 달라집니다. 이에 해당하며 IAM 사용자 보안 인증을 사용하도록 Macie를 재구성하는 경우 Macie는 IAM 역할에 대한 기존 설정(역할 이름 및 구성에 대한 외부 ID)을 영구적으로 삭제합니다. 나중에 조직에서 IAM 역할을 다시 사용하기로 선택한 경우 해당되는 각 멤버 계정의 역할에 대한 신뢰 정책에서 새 외부 ID를 지정해야 합니다.

각 계정 유형의 구성 옵션에 대한 자세한 내용은 조사 결과의 민감한 데이터 샘플을 검색하기 위한 구성 옵션 및 요구 사항 섹션을 참조하세요.

Macie에서 설정을 구성하고 계정의 구성을 활성화하려면 Amazon Macie 콘솔이나 Amazon Macie API를 사용하면 됩니다.

Console

Amazon Macie 콘솔을 사용하여 설정을 구성하고 활성화하려면 다음 단계를 따르세요.

Macie 설정을 구성하고 활성화하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단 모서리에 있는 AWS 리전 선택기를 사용하여 Macie가 민감한 데이터 샘플을 검색하고 공개하도록 구성하고 활성화하려는 리전을 선택합니다.
3. 탐색 창의 설정아래에서 샘플 표시를 선택합니다.
4. 설정(settings) 섹션에서 편집(Edit)을 선택합니다.
5. 상태(Status)는 활성(Enable)을 선택합니다.
6. 액세스에서 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색하는 경우 사용할 액세스 방법과 설정을 지정합니다.

- Macie에 액세스 권한을 위임하는 IAM 역할을 사용하려면 IAM 역할 수임을 선택합니다. 이 옵션을 선택하면 Macie는 AWS 계정에서 생성하고 구성한 IAM 역할을 수임하여 샘플을 검색합니다. 역할 이름 상자에 역할의 이름을 입력합니다.
- 샘플을 요청하는 IAM 사용자의 보안 인증을 사용하려면 IAM 사용자 자격 증명 사용을 선택합니다. 이 옵션을 선택하면 계정의 각 사용자가 개별 IAM ID를 사용하여 샘플을 검색합니다.

7. 암호화에서, 검색되는 민감한 데이터 샘플을 암호화하는 데 사용하려는 AWS KMS key를 지정합니다.

   - 자신의 계정에 있는 KMS 키를 사용하려면 계정에서 키 선택을 선택합니다. 그런 다음 AWS KMS key목록에서 사용할 키를 선택합니다. 목록에는 계정에 대한 기존의 대칭 암호화 KMS 키가 표시됩니다.
   - 다른 계정이 소유한 KMS 키를 사용하려면 다른 계정에 있는 키의 ARN 입력을 선택합니다. 그런 다음 AWS KMS key ARN 상자에 사용할 키의 Amazon 리소스 이름 (ARN)을 입력합니다(예: **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**).

8. 규칙에 대한 설정 입력을 마치면 저장를 선택합니다.

Macie가 설정을 테스트하고 올바른지 확인합니다. Macie가 IAM 역할을 수임하도록 구성한 경우 Macie는 계정에 해당 역할이 존재하는지, 신뢰 및 권한 정책이 올바르게 구성되어 있는지 확인합니다. 문제가 있는 경우 Macie에서 문제를 설명하는 메시지를 표시합니다.

AWS KMS key 관련 문제를 해결하려면 이전 주제의 요구 사항을 참조하여 요구 사항을 충족하는 KMS 키를 지정하세요. IAM 역할 관련 문제를 해결하려면 먼저 올바른 역할 이름을 입력했는지 확인합니다. 이름이 올바른 경우 역할의 정책이 Macie의 역할 수임을 위한 모든 요구 사항을 충족하는지 확인합니다. 자세한 내용은 영향을 받는 S3 객체에 액세스하도록 IAM 역할 구성 섹션을 참조하세요. 문제를 해결한 후에 설정을 저장하고 활성화할 수 있습니다.

> **Note**
>
> 조직의 Macie 관리자이고 IAM 역할을 수임하도록 Macie를 구성한 경우 계정 설정을 저장하면 Macie가 외부 ID를 생성하여 표시합니다. ID를 적어 두세요. 해당되는 각 멤버 계정의 IAM 역할에 대한 신뢰 정책에 이 ID가 지정되어 있어야 합니다. 그러지 않으면 계정이 소유한 S3 객체에서 민감한 데이터 샘플을 검색할 수 없습니다.

API

설정을 프로그래밍 방식으로 구성하고 활성화하려면 Amazon Macie API의 UpdateRevealConfiguration 작업을 사용하세요. 요청에서 지원되는 파라미터에 적절한 값을 지정합니다.

- `retrievalConfiguration` 파라미터의 경우 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색할 때 사용할 액세스 방법과 설정을 지정합니다.
  - Macie에 액세스 권한을 위임하는 IAM 역할을 수임하려면 `retrievalMode` 파라미터에 `ASSUME_ROLE`을 지정하고 `roleName` 파라미터에 역할 이름을 지정합니다. 이러한 설정을 지정하면 Macie는 AWS 계정에서 생성하고 구성한 IAM 역할을 수임하여 샘플을 검색합니다.
  - 샘플을 요청하는 IAM 사용자의 보안 인증을 사용하려면 `retrievalMode` 파라미터에 `CALLER_CREDENTIALS`를 지정합니다. 이 설정을 지정하면 계정의 각 사용자가 개별 IAM ID를 사용하여 샘플을 검색합니다.

  > **Important**
  >
  > 이러한 파라미터에 대한 값을 지정하지 않으면 Macie는 액세스 방법(`retrievalMode`)을 `CALLER_CREDENTIALS`로 설정합니다. 현재 Macie가 IAM 역할을 사용하여 샘플을 검색하도록 구성되어 있는 경우 Macie는 구성에 대한 현재 역할 이름과 외부 ID도 영구적으로 삭제합니다. 기존 구성에서 이러한 설정을 유지하려면 요청에 `retrievalConfiguration` 파라미터를 포함하고 해당 파라미터에 대한 현재 설정을 지정하세요. 현재 설정을 검색하려면 GetRevealConfiguration 작업을 사용하거나 AWS Command Line Interface(AWS CLI)를 사용하는 경우 get-reveal-configuration 명령을 실행합니다.

- `kmsKeyId` 파라미터의 경우 검색 대상인 민감한 데이터 샘플을 암호화하는 데 사용할 AWS KMS key를 지정합니다.
  - 사용자 계정에서 KMS 키를 사용하려면 키의 Amazon 리소스 이름(ARN), ID 또는 별칭을 지정하세요. 별칭을 지정하는 경우 `alias/` 접두사를 포함하세요(예: `alias/ExampleAlias`).
  - 다른 계정이 소유한 KMS 키를 사용하려면 키의 ARN(예: `arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`)을 지정하세요. 또는 키 별칭의 ARN(예: `arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias`)을 지정합니다.
- `status` 파라미터의 경우, Macie 계정의 구성을 활성화하도록 `ENABLED`을(를) 지정하세요.

또한 요청 시 구성을 활성화하고 사용하려는 AWS 리전을 지정했는지 확인하세요.

AWS CLI를 사용하여 설정을 구성하고 활성화하려면 update-reveal-configuration 명령을 실행하고 지원되는 파라미터에 대해 적절한 값을 지정합니다. 예를 들어 Microsoft Windows에서 AWS CLI를 사용 중인 경우 다음 명령을 실행합니다.

```
C:\> aws macie2 update-reveal-configuration ^
--region us-east-1 ^
--configuration={\"kmsKeyId\":\"arn:aws:kms:us-east-1:111122223333:alias/
ExampleAlias\",\"status\":\"ENABLED\"} ^
--retrievalConfiguration={\"retrievalMode\":\"ASSUME_ROLE\",\"roleName\":
\"MacieRevealRole\"}
```

위치:

- *us-east-1*은 구성을 활성화하고 사용할 리전입니다. 이 예제에서는 미국 동부(버지니아 북부) 리전을 나타냅니다.
- *arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias*는 AWS KMS key에 사용할 별칭의 ARN입니다. 이 예제에서는 다른 계정이 키를 소유하고 있습니다.
- ENABLED은(는) 구성의 상태입니다.
- *ASSUME_ROLE*은 사용할 액세스 방법입니다. 이 예에서는 지정된 IAM 역할을 수임합니다.
- *MacieRevealRole*은 민감한 데이터 샘플을 검색할 때 Macie가 수임하는 IAM 역할의 이름입니다.

앞의 예에서는 가독성을 높이기 위해 캐럿(^) 줄 연속 문자를 사용합니다.

요청을 제출하면 Macie는 설정을 테스트합니다. Macie가 IAM 역할을 수임하도록 구성한 경우 Macie는 계정에 해당 역할이 존재하는지, 신뢰 및 권한 정책이 올바르게 구성되어 있는지 확인합니다. 문제가 있는 경우 요청이 실패하고 Macie가 문제를 설명하는 메시지를 반환합니다. AWS KMS key 관련 문제를 해결하려면 이전 주제의 요구 사항을 참조하여 요구 사항을 충족하는 KMS 키를 지정하세요. IAM 역할 관련 문제를 해결하려면 먼저 올바른 역할 이름을 지정했는지 확인합니다. 이름이 올바른 경우 역할의 정책이 Macie의 역할 수임을 모든 요구 사항을 충족하는지 확인합니다. 자세한 내용은 영향을 받는 S3 객체에 액세스하도록 IAM 역할 구성 섹션을 참조하세요. 문제를 해결한 후 요청을 다시 제출합니다.

요청이 성공하면 Macie는 지정된 리전의 계정 구성을 활성화하고 다음과 비슷한 출력내용을 받게 됩니다.

```
{
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

여기서 `kmsKeyId`는 검색되는 민감한 데이터 샘플을 암호화하는 데 사용할 AWS KMS key를 지정하고 `status`는 Macie 계정의 구성 상태입니다. `retrievalConfiguration` 값은 샘플을 검색할 때 사용할 액세스 방법과 설정을 지정합니다.

> **Note**
>
> 조직의 Macie 관리자이고 IAM 역할을 수임하도록 Macie를 구성한 경우 응답에 외부 ID(`externalId`)가 있는지 확인합니다. 해당되는 각 멤버 계정의 IAM 역할에 대한 신뢰 정책에 이 ID가 지정되어 있어야 합니다. 그러지 않으면 계정이 소유하고 있고 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색할 수 없습니다.

이후, 계정 구성의 설정이나 상태를 확인하려면 GetRevalConfiguration 작업을 사용하거나 AWS CLI의 경우 get-reveal-configuration 명령을 실행하세요.

Amazon Macie 설정 비활성화

언제든지 Amazon Macie 계정의 구성 설정을 비활성화할 수 있습니다. 구성을 비활성화하면 Macie는 검색되는 민감한 데이터 샘플을 암호화하는 데 사용할 AWS KMS key를 지정하는 설정을 유지합니다. Macie는 구성에 대한 Amazon S3 액세스 설정을 영구적으로 삭제합니다.

> **Warning**
>
> Macie 계정의 구성 설정을 비활성화하면 영향을 받는 S3 객체에 대한 액세스 방법을 지정하는 현재 설정도 영구적으로 삭제됩니다. Macie가 현재 AWS Identity and Access Management(IAM) 역할을 수임하여 영향을 받는 객체에 액세스하도록 구성된 경우 여기에는

역할의 이름과 구성에 대해 Macie가 생성한 외부 ID가 포함됩니다. 이러한 설정은 삭제한 후에는 복구할 수 없습니다.

Macie 계정의 구성 설정을 비활성화하려면 Amazon Macie 콘솔이나 Amazon Macie API를 사용하면 됩니다.

Console

Amazon Macie 콘솔을 사용하여 계정의 구성 설정을 비활성화하려면 다음 단계를 따르세요.

Macie 설정을 비활성화하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단 모서리에 있는 AWS 리전 선택기를 사용하여 Macie 계정의 구성 설정을 비활성화하려는 리전을 선택합니다.
3. 탐색 창의 설정아래에서 샘플 표시를 선택합니다.
4. 설정(settings) 섹션에서 편집(Edit)을 선택합니다.
5. 상태에서 비활성화를 선택합니다.
6. 저장을 선택합니다.

API

프로그래밍 방식으로 구성 설정을 비활성화하려면 Amazon Macie API의 UpdateRevealConfiguration 작업을 사용합니다. 요청에서 구성을 비활성화하려는 AWS 리전을 지정해야 합니다. `status` 파라미터에서 `DISABLED`를 지정합니다.

AWS Command Line Interface(AWS CLI)를 사용하여 구성 설정을 비활성화하려면 update-reveal-configuration 명령을 실행합니다. `region` 파라미터를 사용하여 구성을 비활성화하려는 리전을 지정합니다. `status` 파라미터에서 `DISABLED`를 지정합니다. 예를 들어 Microsoft Windows에서 AWS CLI를 사용 중인 경우 다음 명령을 실행합니다.

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --
configuration={\"status\":\"DISABLED\"}
```

위치:

- *us-east-1*은 구성을 비활성화할 리전입니다. 이 예제에서는 미국 동부(버지니아 북부) 리전을 나타냅니다.
- DISABLED는 구성의 새로운 상태입니다.

요청이 성공하면 Macie는 지정된 리전에서 계정의 구성을 비활성화하고 다음과 유사한 출력을 얻게 됩니다.

```
{
    "configuration": {
        "status": "DISABLED"
    }
}
```

여기서 status는 Macie 계정의 새로운 구성 상태입니다.

Macie가 IAM 역할을 수임하여 민감한 데이터 샘플을 검색하도록 구성된 경우 역할과 역할의 권한 정책을 삭제할 수 있습니다(선택 사항). 계정의 구성 설정을 비활성화하더라도 Macie는 이러한 리소스를 삭제하지 않습니다. 또한 Macie는 이러한 리소스를 사용하여 계정에 대한 다른 작업을 수행하지 않습니다. 역할과 해당 권한 정책을 삭제하려면 IAM 콘솔 또는 IAM API를 사용하면 됩니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 역할 삭제를 참조하세요.

조사 결과를 사용하여 민감한 데이터 샘플 검색 및 공개

Amazon Macie를 사용하면 Macie가 각 민감한 데이터 조사 결과에서 보고하는 민감한 데이터의 샘플을 검색하고 공개할 수 있습니다. 여기에는 Macie가 관리형 데이터 식별자를 사용하여 탐지한 민감한 데이터와 사용자 지정 데이터 식별자의 기준과 일치하는 데이터가 포함됩니다. 샘플을 통해 Macie가 발견한 민감한 데이터의 특성을 확인할 수 있습니다. 또한 영향을 받는 Amazon Simple Storage Service(S3) 객체 및 버킷에 대한 조사를 맞춤 설정하는 데 도움이 될 수 있습니다. 아시아 태평양 (오사카) 및 이스라엘 (텔아비브) 지역을 제외하고 현재 Macie를 이용할 수 AWS 리전 있는 모든 지역에서 민감한 데이터 샘플을 검색하고 공개할 수 있습니다.

검색 결과에 대한 민감한 데이터 샘플을 검색하여 공개하는 경우, Macie는 해당하는 민감한 데이터 검색 결과의 데이터를 사용하여 해당 검색 결과에서 보고된 민감한 데이터 중 처음 1~10개의 항목을 찾습니다. 그런 다음 Macie는 영향을 받는 S3 객체에서 각 발생 항목의 처음 1~128자를 추출합니다. 조사 결과에서 여러 유형의 민감한 데이터가 보고되는 경우 Macie는 해당 조사 결과에서 보고한 최대 100가지 유형의 민감한 데이터에 대해 이 작업을 수행합니다.

Macie는 영향을 받는 S3 객체에서 민감한 데이터를 추출할 때 지정한 AWS Key Management Service (AWS KMS) 키로 데이터를 암호화하고 암호화된 데이터를 캐시에 임시로 저장한 다음 검색 결과에 데이터를 반환합니다. Macie는 운영 문제 해결을 위해 일시적으로 추가 보존이 필요한 경우를 제외하고 추출 및 암호화 직후 캐시에서 데이터를 영구적으로 삭제합니다.

조사 결과에 대한 민감한 데이터 샘플을 검색하여 다시 찾도록 선택하면 Macie는 샘플을 찾고, 추출하고, 암호화하고, 저장하고, 최종적으로 삭제하는 프로세스를 반복합니다.

Amazon Macie 콘솔을 사용하여 민감한 데이터 샘플을 검색하고 공개하는 방법에 대한 데모를 보려면 Amazon Macie를 사용한 민감한 데이터 샘플 검색 및 공개 동영상을 시청하십시오.

주제

시작하기 전에

검색 결과에 대한 민감한 데이터 샘플을 검색하고 공개하려면 먼저 Amazon Macie 계정의 설정을 구성하고 활성화해야 합니다. 또한 AWS 관리자와 협력하여 필요한 권한과 리소스가 있는지 확인해야 합니다.

사용자가 조사 결과의 민감한 데이터 샘플을 검색하여 공개할 때 Macie는 샘플을 찾고, 검색하고, 암호화하고, 공개하기 위한 일련의 작업을 수행합니다. Macie는 사용자 계정의 Macie 서비스 연결 역할을 사용하여 이러한 작업을 수행하지 않습니다. 대신 AWS Identity and Access Management (IAM) ID를 사용하거나 Macie가 계정에서 IAM 역할을 맡도록 허용하십시오.

검색 결과에 대한 민감한 데이터 샘플을 검색하여 공개하려면 검색 결과, 해당하는 민감한 데이터 검색 결과 및 Macie가 민감한 데이터 샘플을 암호화하는 데 사용하도록 구성한 결과에 액세스할 수 있어야 합니다. AWS KMS key 또한 사용자 또는 IAM 역할이 영향을 받는 S3 버킷 및 S3 객체에 액세스할 수 있어야 합니다. 해당하는 경우 사용자 또는 역할이 영향 받는 객체를 암호화하는 데 사용된 데이터를 사용할 수도 있어야 합니다. AWS KMS key IAM 정책, 리소스 정책 또는 기타 권한 설정이 필요한 액세스를 거부하는 경우 오류가 발생하고 Macie가 조사 결과에 대한 샘플을 반환하지 않습니다.

다음과 같은 Macie 작업을 수행할 수도 있어야 합니다.

- `macie2:GetMacieSession`

- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

처음 세 가지 작업을 통해 Macie 계정에 액세스하여 조사 결과의 세부 정보를 검색할 수 있습니다. 마지막 작업을 통해 민감한 데이터 샘플을 검색하여 조사 결과를 공개할 수 있습니다.

Amazon Macie 콘솔을 사용하여 민감한 데이터 샘플을 검색하고 공개하려면 `macie2:GetSensitiveDataOccurrencesAvailability` 작업도 수행할 수 있어야 합니다. 이 작업을 통해 개별 조사 결과에 샘플을 사용할 수 있는지 여부를 결정할 수 있습니다. 프로그래밍 방식으로 샘플을 검색하고 공개하는 데에는 이 작업을 수행할 수 있는 권한이 필요하지 않습니다. 하지만 이 권한이 있으면 샘플 검색을 간소화할 수 있습니다.

조직의 Macie 위임 관리자이고 민감한 데이터 샘플을 검색하는 IAM 역할을 수임하도록 Macie를 구성한 경우 `macie2:GetMember` 작업도 수행할 수 있어야 합니다. 이 작업을 수행하면 내 계정과 영향을 받은 계정 간의 연결에 대한 정보를 검색할 수 있습니다. 이를 통해 Macie는 사용자가 현재 해당 계정의 Macie 관리자인지 확인할 수 있습니다.

필요한 작업을 수행하거나 필수 데이터 및 리소스에 액세스할 수 없는 경우 AWS 관리자에게 도움을 요청하십시오.

민감한 데이터 샘플을 조사 결과에 사용할 수 있는지 여부 결정

조사 결과에 대한 민감한 데이터 샘플을 검색하고 공개하려면 조사 결과가 특정 기준을 충족해야 합니다. 여기에는 특정 상황의 민감한 데이터에 대한 위치 데이터가 포함되어야 합니다. 또한 유효한 해당 민감한 데이터 검색 결과의 위치도 지정해야 합니다. 민감한 데이터 검색 결과는 검색 결과와 AWS 리전 동일하게 저장해야 합니다. Amazon Macie가 AWS Identity and Access Management (IAM) 역할을 맡아 영향을 받는 S3 객체에 액세스하도록 구성한 경우, Macie가 해시 기반 메시지 인증 코드 (HMAC)로 서명한 S3 객체에도 민감한 데이터 검색 결과를 저장해야 합니다. AWS KMS key

영향을 받는 S3 객체도 특정 기준을 충족해야 합니다. 객체의 MIME 유형이며 다음 중 하나여야 합니다.

- application/avro, Apache Avro 객체 컨테이너(.avro) 파일의 경우
- application/gzip, GNU Zip 압축 아카이브(.gz 또는 .gzip) 파일의 경우
- application/json, JSON 또는 JSON 라인(.json 또는 .jsonl) 파일의 경우
- application/parquet, Apache Parquet(.parquet) 파일의 경우

- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, Microsoft Excel 통합문서(.xlsx) 파일의 경우
- application/zip, ZIP 압축 아카이브(.zip) 파일의 경우
- text/csv, CSV(.csv) 파일의 경우
- text/plain, CSV, JSON, JSON 라인 또는 TSV 파일이 아닌 바이너리가 아닌 텍스트 파일의 경우
- text/tab-separated-values, TSV(.tsv) 파일의 경우

또한 S3 객체의 내용은 조사 결과를 생성할 때와 같아야 합니다. Macie는 객체의 엔터티 태그(ETag)를 검사하여 조사 결과에서 지정한 ETag와 일치하는지 확인합니다. 또한 객체의 스토리지 크기는 민감한 데이터 샘플을 검색하고 공개하기 위한 해당 크기 할당량을 초과할 수 없습니다. 적용 가능한 할당량 목록은 Amazon Macie 할당량 섹션을 참조하세요.

조사 결과와 영향을 받는 S3 객체가 위 기준을 충족하는 경우, 민감한 데이터 샘플을 검조사 결과에 사용할 수 있습니다. 원하는 경우 조사 결과에 대한 샘플을 검색하여 공개하기 전에 이러한 결과가 특정 검색 조사 결과에 해당되는지 여부를 선택적으로 판단할 수 있습니다.

민감한 데이터 샘플을 조사 결과에 사용할 수 있는지 여부를 확인하려면

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 민감한 데이터 샘플을 조사 결과에 사용할 수 있는지 여부를 결정할 수 있습니다.

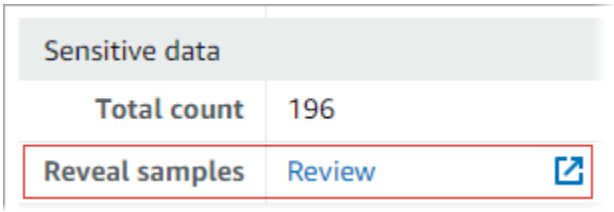
Console

Amazon Macie 콘솔에서 다음 단계에 따라 민감한 데이터 샘플을 검색 결과에 사용할 수 있는지 확인하세요.

조사 결과에 샘플을 사용할 수 있는지 여부를 확인하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. 조사 결과 페이지에서 조사 결과를 선택합니다. 세부 정보 패널에 조사 결과의 정보가 표시됩니다.
4. 세부 정보 패널에서 민감한 데이터 섹션으로 스크롤합니다. 그런 다음 샘플 공개 필드를 참조하세요.

   조사 결과에 민감한 데이터 샘플을 사용할 수 있는 경우, 다음 이미지와 같이 필드에 검토 링크가 나타납니다.



민감한 데이터 샘플을 조사 결과에 사용할 수 없는 경우, 샘플 공개 필드에 다음과 같은 이유를 나타내는 텍스트가 표시됩니다.

- 조직에 속하지 않은 계정 - Macie를 사용하여 영향을 받는 S3 객체에 액세스할 수 없습니다. 영향을 받은 계정은 현재 조직에 속해 있지 않습니다. 또는 계정이 조직에 속해 있지만 현재 AWS 리전에서 계정에 Macie를 사용하도록 설정되어 있지 않은 경우입니다.
- 잘못된 분류 결과 - 해당 조사 결과에 해당하는 민감한 데이터 검색 결과가 없습니다. 또는 해당하는 민감한 데이터 검색 결과가 현재 AWS 리전에서 제공되지 않거나, 형식이 잘못되었거나 손상되었거나, 지원되지 않는 저장 형식을 사용하는 경우도 있습니다. Macie가 검색할 민감한 데이터의 위치를 확인할 수 없습니다.
- 잘못된 결과 서명 - 해당하는 민감한 데이터 검색 결과는 Macie가 서명하지 않은 S3 객체에 저장됩니다. Macie는 민감한 데이터 검색 결과의 무결성과 신뢰성을 확인할 수 없습니다. 따라서 Macie가 검색할 민감한 데이터의 위치를 확인할 수 없습니다.
- 과도하게 허용적인 멤버 역할 - 영향을 받는 멤버 계정의 IAM 역할에 대한 신뢰 또는 권한 정책이 역할에 대한 액세스를 제한하기 위한 Macie 요구 사항을 충족하지 않습니다. 또는 역할의 신뢰 정책에 조직에 대한 올바른 외부 ID가 지정되어 있지 않습니다. Macie는 민감한 데이터를 검색하는 역할을 수임할 수 없습니다.
- GetMember 권한 누락 — 계정과 영향을 받는 계정 간의 연결에 대한 정보를 검색할 수 없습니다. Macie는 사용자가 영향을 받는 계정의 위임된 Macie 관리자로서 영향을 받는 S3 객체에 액세스할 수 있는지 여부를 확인할 수 없습니다.
- 객체 크기 할당량 초과 - 영향을 받는 S3 객체의 스토리지 크기가 해당 유형의 파일에서 민감한 데이터의 샘플을 검색하고 공개하는 데 필요한 크기 할당량을 초과합니다.
- 객체 사용 불가 - 영향을 받은 S3 객체를 사용할 수 없습니다. Macie가 조사 결과를 생성한 후 객체 이름이 변경되거나, 이동 또는 삭제되었거나, 내용이 변경되었습니다. 또는 객체가 현재 비활성화된 AWS KMS key 로 암호화되어 있을 수도 있습니다.
- 서명되지 않은 결과 - 해당하는 민감한 데이터 검색 결과가 서명되지 않은 S3 객체에 저장됩니다. Macie는 민감한 데이터 검색 결과의 무결성과 신뢰성을 확인할 수 없습니다. 따라서 Macie가 검색할 민감한 데이터의 위치를 확인할 수 없습니다.

- 과도하게 허용적인 역할 - 계정이 신뢰 또는 권한 정책이 역할에 대한 액세스를 제한하는 Macie 요구 사항을 충족하지 않는 IAM 역할을 사용하여 민감한 데이터의 발생을 검색하도록 구성되어 있습니다. Macie는 민감한 데이터를 검색하는 역할을 수임할 수 없습니다.
- 지원되지 않는 객체 유형 - 영향을 받는 S3 객체는 Macie가 지원하지 않는 파일 또는 스토리지 형식을 사용하여 민감한 데이터의 샘플을 검색하고 공개합니다. 영향을 받는 S3 개체의 MIME 유형이 이전 목록에 있는 값 중 하나가 아닙니다.

조사 결과에 대한 민감한 데이터 검색 결과에 문제가 있는 경우 조사 결과의 상세 결과 위치 필드에 있는 정보가 문제를 조사하는 데 도움이 될 수 있습니다. 이 필드는 Amazon S3의 결과에 대한 원래 경로를 지정합니다. IAM 역할의 문제를 조사하려면 해당 역할의 정책이 Macie의 역할 수임을 위한 모든 요구 사항을 충족하는지 확인합니다. 자세한 내용은 영향을 받는 S3 객체에 액세스하도록 IAM 역할 구성 섹션을 참조하세요.

API

민감한 데이터 샘플을 검색 결과에 사용할 수 있는지 여부를 프로그래밍 방식으로 결정하려면 Amazon GetSensitiveDataOccurrencesAvailabilityMacie API의 작업을 사용하십시오. 요청을 제출할 때 `findingId` 파라미터를 사용하여 조사 결과의 고유 식별자를 지정합니다. 작업을 사용하여 이 식별자를 얻을 수 있습니다. ListFindings

AWS Command Line Interface (AWS CLI) 를 사용하는 경우 get-sensitive-data-occurrences-availability 명령을 실행하고 `finding-id` 매개 변수를 사용하여 검색 결과의 고유 식별자를 지정하십시오. 이 식별자를 얻기위해 list-findings 명령을 실행할 수 있습니다.

요청이 성공하고 조사 결과에 샘플을 사용할 수 있는 경우, 다음과 비슷한 출력이 나타납니다.

```
{
    "code": "AVAILABLE",
    "reasons": []
}
```

요청이 성공하고 조사 결과에 샘플을 사용할 수 없는 경우 `code` 필드의 값은 `UNAVAILABLE`이며 `reasons` 배열은 이유를 지정합니다. 예:

```
{
    "code": "UNAVAILABLE",
    "reasons": [
        "UNSUPPORTED_OBJECT_TYPE"
```

```
    ]
}
```

조사 결과에 대한 민감한 데이터 검색 결과에 문제가 있는 경우 결과의 `classificationDetails.detailedResultsLocation` 필드에 있는 정보가 문제를 조사하는 데 도움이 될 수 있습니다. 이 필드는 Amazon S3의 결과에 대한 원래 경로를 지정합니다. IAM 역할의 문제를 조사하려면 해당 역할의 정책이 Macie의 역할 수임을 위한 모든 요구 사항을 충족하는지 확인합니다. 자세한 내용은 영향을 받는 S3 객체에 액세스하도록 IAM 역할 구성 섹션을 참조하세요.

조사 결과의 민감한 데이터 샘플 검색 및 공개

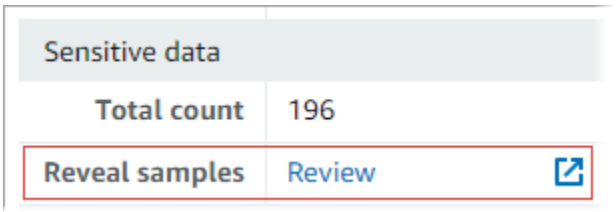
Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 조사 결과에 대한 민감한 데이터 샘플을 검색하고 확인할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 조사 결과에 대한 민감한 데이터 샘플을 검색하고 공개하려면 다음 단계를 따르세요.

조사 결과에 사용할 민감한 데이터 샘플을 검색하고 공개하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. 조사 결과 페이지에서 조사 결과를 선택합니다. 세부 정보 패널에 조사 결과의 정보가 표시됩니다.
4. 세부 정보 패널에서 민감한 데이터 섹션으로 스크롤합니다. 그런 다음 샘플 공개 필드에서 검토를 선택합니다.

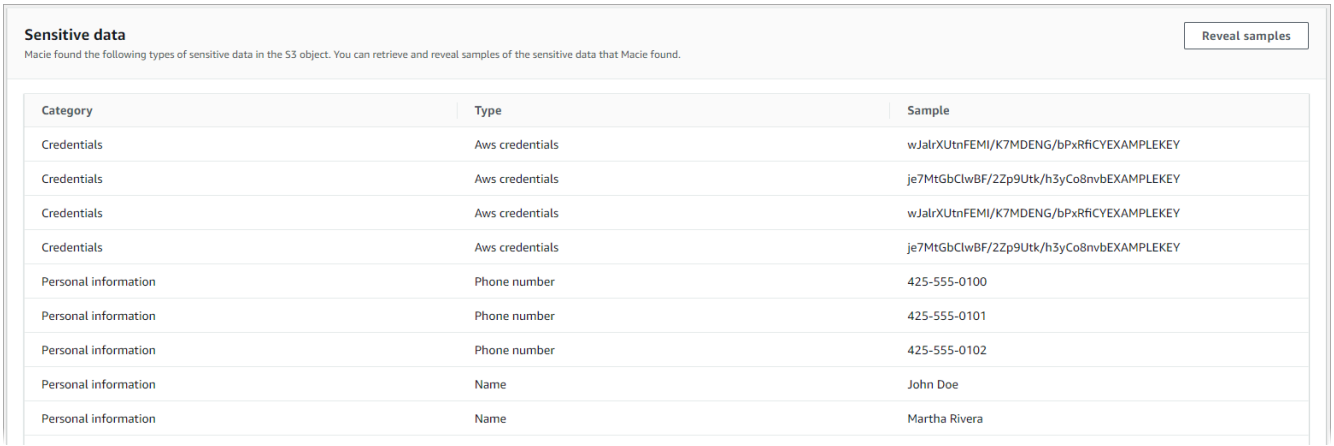


> **Note**
>
> 검토 링크가 샘플 공개 필드에 나타나지 않으면 민감한 데이터 샘플을 조사 결과에 사용할 수 없습니다. 이 문제가 발생하는 이유에 대한 자세한 내용은 이전 주제를 참조하세요.

검토를 선택하면 Macie는 조사 결과의 주요 세부 정보를 요약하는 페이지를 표시합니다. 세부 정보에는 Macie가 영향을 받는 S3 객체에서 발견한 민감한 데이터의 범주, 유형 및 발생 횟수가 포함되어 있습니다.

5. 페이지의 민감한 데이터 섹션에서 샘플 공개를 선택합니다. 그러면 Macie는 조사 결과에서 보고된 민감한 데이터 중 처음 1~10건의 샘플을 검색하여 공개합니다. 각 샘플에는 민감한 데이터 발생 항목의 첫 1~128자가 포함되어 있습니다. 샘플을 검색하고 공개하는 데 몇 분 정도 걸릴 수 있습니다.

   조사 결과에 여러 유형의 민감한 데이터가 보고되는 경우 Macie는 최대 100가지 유형의 샘플을 검색하고 공개합니다. 예를 들어, 다음 이미지는AWS 자격 증명, 미국 전화번호, 사람 이름 등 여러 범주와 유형의 민감한 데이터에 걸친 샘플을 보여줍니다.



   샘플은 먼저 민감한 데이터 범주별로 구성되어 있고, 그 다음에는 민감한 데이터 유형별로 구성되어 있습니다.

API

민감한 데이터 샘플을 가져와 프로그래밍 방식으로 검색 결과를 찾아내려면 Amazon Macie API의 GetSensitiveDataOccurrences 작업을 사용하십시오. 요청을 제출할 때 `findingId`

파라미터를 사용하여 조사 결과의 고유 식별자를 지정합니다. 작업을 사용하여 이 식별자를 얻을 수 있습니다. ListFindings

AWS Command Line Interface (AWS CLI) 를 사용하여 민감한 데이터 샘플을 검색하고 표시하려면 get-sensitive-data-occurrences명령을 실행하고 `finding-id` 매개 변수를 사용하여 검색 결과의 고유 식별자를 지정하십시오. 예:

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
 "1f1c2d74db5d8caa76859ec52example"
```

여기서 *1f1c2d74db5d8caa76859ec52example*은 조사 결과의 고유 식별자입니다. 를 사용하여 이 식별자를 가져오려면 list-find 명령을 실행하면 됩니다. AWS CLI

요청이 성공하면 Macie가 요청 처리를 시작하고 다음과 비슷한 출력이 표시됩니다.

```
{
    "status": "PROCESSING"
}
```

요청을 처리하는 데 몇 분 정도 걸릴 수 있습니다. 몇 분 정도 기다린 후, 다시 요청을 제출합니다.

Macie가 민감한 데이터 샘플을 찾고 검색하고 암호화할 수 있는 경우, Macie는 해당 샘플을 `sensitiveDataOccurrences` 맵에 반환합니다. 이 맵에는 조사 결과를 통해 보고된 1~100가지 유형의 민감한 데이터가 지정되어 있으며, 이 각 유형에는 1~10개의 샘플이 지정되어 있습니다. 각 샘플에는 조사 결과에서 보고된 민감한 데이터 발생 항목의 처음 1~128자가 들어 있습니다.

맵에서 각 키는 민감한 데이터를 감지한 관리형 데이터 식별자의 ID 또는 민감한 데이터를 감지한 사용자 지정 데이터 식별자의 이름 및 고유 식별자입니다. 값은 지정된 관리형 데이터 식별자 또는 사용자 지정 데이터 식별자의 샘플입니다. 예를 들어, 다음 응답은 관리형 데이터 식별자(`NAME`및`AWS_CREDENTIALS`) 로 탐지된 사용자 이름 샘플 3개와 AWS 보안 액세스 키 샘플 2개를 제공합니다.

```
{
    "sensitiveDataOccurrences": {
        "NAME": [
            {
                "value": "Akua Mansa"
            },
            {
```

```
                "value": "John Doe"
            },
            {
                "value": "Martha Rivera"
            }
        ],
        "AWS_CREDENTIALS": [
            {
                "value": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
            },
            {
                "value": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
            }
        ]
    },
    "status": "SUCCESS"
}
```

요청이 성공했지만 민감한 데이터 샘플을 찾을 수 없는 경우, 샘플을 사용할 수 없는 이유를 설명하는 `UnprocessableEntityException` 메시지를 받게 됩니다. 예:

```
{
    "message": "An error occurred (UnprocessableEntityException) when calling the
 GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```

앞의 예에서 Macie는 영향을 받은 S3 객체에서 샘플을 검색하려고 시도했지만 해당 객체는 더 이상 사용할 수 없습니다. Macie가 조사 결과를 생성한 후 객체의 내용이 변경되었습니다.

요청이 성공했지만 다른 유형의 오류로 인해 Macie가 조사 결과에 대한 민감한 데이터 샘플을 검색하고 공개하지 못한 경우, 다음과 비슷한 출력이 표시됩니다.

```
{
    "error": "Macie can't retrieve the samples. You're not allowed to access the
 affected S3 object or the object is encrypted with a key that you're not allowed to
 use.",
    "status": "ERROR"
}
```

`status`필드 값은 `ERROR`이고 `error` 필드는 발생한 오류를 설명합니다. 이전 주제의 정보는 오류를 조사하는 데 도움이 될 수 있습니다.

민감한 데이터 위치에 대한 JSON 스키마

Amazon Macie는 Amazon Simple Storage Service(S3) 객체에서 민감한 데이터를 찾은 위치에 대한 정보를 저장하는 데 표준화된 JSON 구조를 사용합니다. 구조는 민감한 데이터 조사 결과와 민감한 데이터 검색 결과에 사용됩니다. 민감한 데이터 조사 결과의 경우 구조는 조사 결과에 대한 JSON 스키마의 일부입니다. 전체 JSON 스키마에서 발견된 내용을 검토하려면 Amazon Macie API 참조의 조사 결과를 참조하세요. 민감한 데이터 조사 결과에 대한 자세한 내용은 민감한 데이터 검색 결과 저장 및 유지을(를) 참조하세요.

주제

- 민감한 데이터 위치에 대한 JSON 스키마 개요
- 민감한 데이터 위치에 대한 JSON 스키마 세부 정보 및 예제

민감한 데이터 위치에 대한 JSON 스키마 개요

Amazon Macie가 영향을 받는 S3 객체에서 발견한 민감한 데이터의 위치를 보고하기 위해 민감한 데이터 조사 결과 및 민감한 데이터 검색 결과에 대한 JSON 스키마에는 `customDataIdentifiers` 객체 1개와 `sensitiveData` 객체 1개가 포함됩니다. `customDataIdentifiers` 객체는 Macie가 사용자 지정 데이터 식별자를 사용하여 탐지한 데이터에 대한 세부 정보를 제공합니다. `sensitiveData` 객체는 Macie가 관리형 데이터 식별자를 사용하여 탐지한 데이터에 대한 세부 정보를 제공합니다.

각 `customDataIdentifiers` 및 `sensitiveData` 객체에는 하나 이상의 `detections` 배열이 포함되어 있습니다.

- `customDataIdentifiers` 객체에서 `detections` 배열은 데이터를 탐지하고 조사 결과를 생성한 사용자 지정 데이터 식별자를 나타냅니다. 각 사용자 지정 데이터 식별자에 대해 배열은 식별자가 탐지한 데이터의 발생 횟수도 나타냅니다. 식별자가 탐지한 데이터의 위치를 나타낼 수도 있습니다.
- `sensitiveData` 객체에서 `detections` 배열은 Macie가 관리 데이터 식별자를 사용하여 탐지한 민감한 데이터의 유형을 나타냅니다. 각 유형의 민감한 데이터에 대해 배열은 데이터 발생 횟수를 나타내며 데이터의 위치를 나타낼 수도 있습니다.

민감한 데이터 조사 결과의 경우 `detections` 배열에 1~15개의 `occurrences` 객체가 포함될 수 있습니다. 각 `occurrences` 객체는 Macie가 특정 유형의 민감한 데이터를 개별적으로 감지한 위치를 지정합니다.

예를 들어, 다음 `detections` 배열은 Macie가 CSV 파일에서 찾은 민감한 데이터 (미국 사회보장번호)가 세 번 나오는 위치를 나타냅니다.

```
"sensitiveData": [
     {
       "category": "PERSONAL_INFORMATION",
       "detections": [
          {
             "count": 30,
             "occurrences": {
                "cells": [
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 2
                   },
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 3
                   },
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 4
                   }
                ]
             },
             "type": "USA_SOCIAL_SECURITY_NUMBER"
          }
```

detections 배열에 있는 occurrences 객체의 위치와 개수는 Macie가 자동화된 중요 데이터 검색 분석 주기 또는 중요한 데이터 검색 작업 실행 중에 탐지한 중요한 데이터의 범주, 유형 및 발생 횟수에 따라 달라집니다. Macie는 각 분석 주기 또는 작업 실행에 대해 깊이 우선 검색 알고리즘을 사용하여 Macie가 S3 객체에서 감지한 1~15개의 민감한 데이터에 대한 위치 데이터로 결과적인 조사 결과를 채웁니다. 이러한 상황은 영향을 받는 S3 버킷과 객체에 포함될 수 있는 민감한 데이터의 범주 및 유형을 나타냅니다.

occurrences 객체에는 영향을 받는 S3 객체의 파일 유형 또는 스토리지 형식에 따라 다음과 같은 구조가 포함될 수 있습니다.

- `cells` 배열 – 이 배열은 Microsoft Excel 통합 문서, CSV 파일 및 TSV 파일에 적용됩니다. 이 배열의 객체는 Macie가 민감한 데이터의 발생을 감지한 셀 또는 필드를 지정합니다.
- `lineRanges` 배열 – 이 배열은 이메일 메시지 (EML) 파일과 CSV, JSON, JSON Lines 및 TSV 파일을 제외한 바이너리가 아닌 텍스트 파일 (예: HTML, TXT, XML 파일) 에 적용됩니다. 이 배열의 객체는 Macie가 민감한 데이터의 발생을 감지한 줄 또는 여러 줄의 범위를 지정하고 지정된 줄 또는 한 줄에서의 데이터 위치를 지정합니다.

  배열의 객체가 다른 유형의 `lineRanges` 배열에서 지원하는 파일 유형이나 스토리지 형식으로 민감한 데이터 탐지 위치를 지정하는 경우도 있습니다. 이러한 경우는 파일 내 주석과 같이 비정형 파일의 비정형 섹션에서의 탐지, Macie가 일반 텍스트로 분석하는 잘못된 형식의 파일에서의 탐지, Macie가 민감한 데이터를 감지한 하나 이상의 열 이름이 있는 CSV 또는 TSV 파일 등입니다.
- `offsetRanges` 배열 – 이 배열은 나중에 사용하기 위해 예약되어 있습니다. 이 배열이 있는 경우 해당 배열의 값은 null입니다.
- `pages` 배열 – 이 배열은 Adobe Portable Document Format (PDF) 파일에 적용됩니다. 이 배열의 객체는 Macie가 민감한 데이터의 발생을 감지한 페이지를 지정합니다.
- `records` 배열 – 이 배열은 Apache Avro 객체 컨테이너, Apache Parquet 파일, JSON 파일 및 JSON Lines 파일에 적용됩니다. Avro 객체 컨테이너 및 Parquet 파일의 경우 이 배열의 객체는 Macie가 민감한 데이터의 발생을 감지한 레코드의 필드 경로와 레코드 색인을 지정합니다. JSON 및 JSON Lines 파일의 경우 이 배열의 객체는 Macie가 민감한 데이터의 발생을 감지한 필드 또는 배열의 경로를 지정합니다. JSON Lines 파일의 경우 데이터가 포함된 라인의 인덱스도 지정합니다.

이러한 배열의 콘텐츠는 영향을 받는 S3 객체의 파일 유형이나 스토리지 형식 및 콘텐츠에 따라 달라집니다.

민감한 데이터 위치에 대한 JSON 스키마 세부 정보 및 예제

Amazon Macie는 특정 유형의 파일 및 콘텐츠에서 민감한 데이터를 탐지한 위치를 나타내는 데 사용하는 JSON 구조의 콘텐츠를 조정합니다. 다음 주제에서는 이러한 구조를 설명하고 이에 대한 예제를 제공합니다.

주제

민감한 데이터 조사 결과에 포함될 수 있는 JSON 구조의 전체 목록은 Amazon Macie API 참조의 조사 결과를 참조하세요.

셀 배열

적용 대상: Microsoft Excel 통합 문서, CSV 파일 및 TSV 파일

`cells` 배열에서 `Cell` 객체는 Macie가 민감한 데이터의 발생을 감지한 셀 또는 필드를 지정합니다. 다음 표에는 `Cell` 객체에 있는 각 필드의 용도가 설명되어 있습니다.

필드	유형	설명
`cellReference`	문자열	발생을 포함하는 셀의 위치 (절대 셀 참조). 이 필드는 Excel 통합 문서에만 적용됩니다. CSV 및 TSV 파일의 경우 이 값은 null입니다.
`column`	Integer	발생을 포함하는 열의 열 번호입니다. Excel 통합 문서의 경우 이 값은 열 식별자의 영문자 (예: 열 A의 1, 열 B의 2 등) 와 상호 연관됩니다.
`columnName`	문자열	발생을 포함하는 열의 이름입니다 (사용 가능한 경우).
`row`	Integer	발생을 포함하는 행의 행 번호입니다.

다음 예제는 Macie가 CSV 파일에서 감지한 민감한 데이터의 발생 위치를 지정하는 `Cell` 객체의 구조를 보여줍니다.

```
"cells": [
   {
      "cellReference": null,
      "column": 3,
      "columnName": "SSN",
      "row": 5
```

```
   }
]
```

위 예제에서 조사 결과는 Macie가 파일의 세 번째 열(이름: SSN)의 다섯 번째 행에 있는 필드에서 민감한 데이터를 탐지했음을 나타냅니다.

다음 예제는 Macie가 Excel 통합 문서에서 감지한 민감한 데이터의 발생 위치를 지정하는 `Cell` 객체의 구조를 보여줍니다.

```
"cells": [
   {
      "cellReference": "Sheet2!C5",
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

위 예제에서 조사 결과는 Macie가 통합 문서의 Sheet2라는 워크시트에서 민감한 데이터를 발견했음을 나타냅니다. 이 워크시트에서 Macie는 세 번째 열의 다섯 번째 행에 있는 셀(C열, 이름: SSN)에서 민감한 데이터를 발견했습니다.

LineRanges 배열

적용 대상: 이메일 메시지(EML) 파일 및 CSV, JSON, JSON Lines 및 TSV 파일을 제외한 바이너리가 아닌 텍스트 파일(예: HTML, TXT 및 XML 파일)

`lineRanges` 배열에서 `Range` 객체는 Macie가 민감한 데이터의 발생을 감지한 줄 또는 여러 줄의 범위를 지정하고 지정된 줄 또는 줄에서의 데이터 위치를 지정합니다.

`occurrences` 객체의 다른 유형의 배열에서 지원하는 파일 유형의 경우 이 객체는 비어 있는 경우가 많습니다. 예외는 다음과 같습니다.

- 기타 정형 파일의 비정형 섹션에 있는 데이터(예: 파일 내 댓글).
- Macie가 일반 텍스트로 분석하는 잘못된 형식의 파일에 있는 데이터.
- Macie가 민감한 데이터를 탐지한 열 이름이 하나 이상 있는 CSV 또는 TSV 파일.

다음 표에서는 `lineRanges` 배열의 `Range` 객체에 있는 각 필드의 용도를 설명합니다.

필드	유형	설명
end	Integer	파일의 시작 부분부터 발생 끝 부분까지의 행 수입니다.
start	Integer	파일의 시작 부분부터 발생 시작 부분까지의 행 수입니다.
startColumn	Integer	스페이스를 포함하며 1부터 시작하여 해당 항목(start)이 포함된 첫 번째 행의 시작 부분부터 발생 시작 부분까지의 문자 수입니다.

다음 예제는 Macie가 TXT 파일의 한 행에서 감지한 중요한 데이터의 발생 위치를 지정하는 Range 객체의 구조를 보여줍니다.

```
"lineRanges": [
   {
      "end": 1,
      "start": 1,
      "startColumn": 119
   }
]
```

위 예제의 조사 결과는 Macie가 파일의 첫 번째 행에서 민감한 데이터(우편 주소)가 완전히 발생한 것을 탐지했음을 나타냅니다. 첫 번째 문자는 해당 행의 시작 부분부터 119자(스페이스 포함)입니다.

다음 예제는 TXT 파일에서 여러 행에 걸쳐 나타나는 민감한 데이터의 위치를 지정하는 Range 객체의 구조를 보여줍니다.

```
"lineRanges": [
   {
      "end": 54,
      "start": 51,
      "startColumn": 1
   }
]
```

위 예제의 조사 결과는 Macie가 파일의 51~54행에 걸쳐 민감한 데이터(우편 주소)의 발생을 탐지했음을 나타냅니다. 해당 항목의 첫 번째 문자는 파일 51행의 첫 번째 문자입니다.

페이지 배열

적용 대상: Adobe Portable Document Format (PDF) 파일

pages 배열에서 Page 객체는 Macie가 민감한 데이터의 발생을 감지한 페이지를 지정합니다. 객체는 pageNumber 필드를 포함하고 있습니다. pageNumber 필드에는 해당 항목이 포함된 페이지의 페이지 번호를 지정하는 정수가 저장됩니다.

다음 예제는 Macie가 PDF 파일에서 탐지한 민감한 데이터의 발생 위치를 지정하는 Page 개체의 구조를 보여줍니다.

```
"pages": [
   {
      "pageNumber": 10
   }
]
```

위 예제의 조사 결과는 파일 10페이지에 해당 발생이 포함되어 있음을 나타냅니다.

레코드 배열

적용 대상: Apache Avro 객체 컨테이너, Apache Parquet 파일, JSON 파일 및 JSON Lines 파일

Avro 객체 컨테이너 또는 Parquet 파일의 경우 records 배열의 Record 객체는 Macie가 민감한 데이터의 발생을 감지한 레코드의 필드 경로와 레코드 색인을 지정합니다. JSON 및 JSON Lines 파일의 경우 Record 객체는 Macie가 민감한 데이터의 발생을 감지한 필드 또는 배열의 경로를 지정합니다. JSON Lines 파일의 경우 발생이 포함된 행의 인덱스도 지정합니다.

다음 표에는 Record 객체에 있는 각 필드의 용도가 설명되어 있습니다.

필드	유형	설명
jsonPath	문자열	해당 발생까지의 경로(JSONPath 표현식) Avro 객체 컨테이너 또는 Parquet 파일의 경우 이 경로

필드	유형	설명
		는 해당 발생이 포함된 레코드(`recordIndex`)의 필드 경로입니다. JSON 또는 JSON Lines 파일의 경우 이 경로는 해당 발생이 포함된 필드 또는 배열의 경로입니다. 데이터가 배열의 값인 경우 경로에는 해당 발생이 포함된 값도 표시됩니다. Macie가 경로에 있는 요소 이름에서 민감한 데이터를 감지하면 Macie는 해당 `jsonPath` 필드를 `Record` 객체에서 생략합니다. 경로 요소 이름이 240자를 초과하는 경우 Macie는 이름의 시작 부분에서 문자를 제거하여 이름을 잘라냅니다. 결과적인 전체 경로가 250자를 초과하는 경우 Macie는 경로의 첫 번째 요소부터 시작하여 경로에 250자 이하가 될 때까지 경로를 잘라냅니다.
`recordIndex`	Integer	Avro 객체 컨테이너 또는 Parquet 파일의 경우 발생이 포함된 레코드의 레코드 인덱스(0부터 시작). JSON Lines 파일의 경우, 발생이 포함된 행의 행 인덱스 (0부터 시작) JSON 파일의 경우 이 값은 항상 `0`입니다.

다음 예제는 Macie가 Parquet 파일에서 탐지한 민감한 데이터의 발생 위치를 지정하는 `Record` 객체의 구조를 보여줍니다.

```
"records": [
   {
      "jsonPath": "$['abcdefghijklmnopqrstuvwxyz']",
      "recordIndex": 7663
   }
]
```

위의 예에서 조사 결과는 Macie가 인덱스 7663의 레코드 (레코드 번호 7664) 에서 민감한 데이터를 탐지했음을 나타냅니다. 이 레코드에서 Macie는 이름이 abcdefghijklmnopqrstuvwxyz인 필드에서 민감한 데이터를 발견했습니다. 레코드에 있는 필드의 전체 JSON 경로는 $.abcdefghijklmnopqrstuvwxyz입니다. 필드는 루트 (외부 수준) 객체의 직계 하위 항목입니다.

다음 예제는 Macie가 Parquet 파일에서 감지한 민감한 데이터 발생에 대한 Record 객체 구조도 보여줍니다. 하지만 이 예제에서는 이름이 문자 제한을 초과했기 때문에 Macie가 해당 발생이 포함된 필드 이름을 잘라냈습니다.

```
"records": [
   {
      "jsonPath":
 "$['...uvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabc
      "recordIndex": 7663
   }
]
```

위 예제에서 필드는 루트 (외부 수준) 객체의 직계 하위 항목입니다.

다음 예제에서도 Macie가 Parquet 파일에서 감지한 민감한 데이터의 경우 해당 항목이 포함된 필드의 전체 경로를 잘라냈습니다. 전체 경로가 문자 제한을 초과했습니다.

```
"records": [
   {
      "jsonPath":
 "$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
      "recordIndex": 2335
   }
]
```

위의 예에서 조사 결과는 Macie가 인덱스 2335의 레코드 (레코드 번호 2336) 에서 민감한 데이터를 탐지했음을 나타냅니다. 이 레코드에서 Macie는 이름이 abcdefghijklmnopqrstuvwxyz인 필드에서 민감한 데이터를 발견했습니다. 레코드에 있는 필드의 전체 JSON 경로는 다음과 같습니다.

```
$['1234567890']usssn1.usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

다음 예제는 Macie가 JSON 파일에서 탐지한 민감한 데이터의 발생 위치를 지정하는 Record 개체의 구조를 보여줍니다. 이 예제에서 이 발생은 배열의 특정 값입니다.

```
"records": [
   {
      "jsonPath": "$.access.key[2]",
      "recordIndex": 0
   }
]
```

위 예제에서 조사 결과는 Macie가 이름이 key인 배열의 두 번째 값에서 민감한 데이터를 탐지했음을 나타냅니다. 배열은 이름이 access인 객체의 하위 배열입니다.

다음 예제는 Macie가 JSON Lines 파일에서 탐지한 민감한 데이터의 발생 위치를 지정하는 Record 개체의 구조를 보여줍니다.

```
"records": [
   {
      "jsonPath": "$.access.key",
      "recordIndex": 3
   }
]
```

위 예제의 결과는 Macie가 파일의 세 번째 값(행)에서 민감한 데이터를 탐지했음을 나타냅니다. 이 줄에서는 이름이 key인 필드에서 발생하는데, 이 필드는 이름이 access인 객체의 하위 필드입니다.

Amazon Macie 조사 결과 안 보이게 하기

검색 결과 분석을 간소화하기 위해 억제 규칙을 만들어 사용할 수 있습니다. 억제 규칙은 Amazon Macie에서 검색 결과를 자동으로 아카이브할 경우를 정의하는 속성 기반 필터 기준의 집합입니다. 억제 규칙은 일련의 결과를 검토한 후 다시 알림을 받고 싶지 않은 경우에 유용합니다.

예를 들어, S3 버킷이 공개 액세스를 허용하지 않고 특정 객체를 사용하여 새 객체를 특정 AWS KMS key과 함께 자동으로 암호화하는 경우 S3 버킷에 우편 주소를 포함하도록 허용할 수 있습니다. 이 경우 다음 필드에 대한 필터 기준을 지정하는 억제 규칙을 만들 수 있습니다. 민감한 데이터 탐지 유형, S3 버킷 공개 액세스 권한, S3 버킷 암호화 KMS 키 ID. 이 규칙은 필터 기준과 일치하는 향후 검색 결과를 억제합니다.

억제 규칙으로 검색 결과를 억제하는 경우, Macie는 규칙의 기준과 일치하는 민감한 데이터 및 잠재적 정책 위반의 후속 발생에 대한 검색 결과를 계속 생성합니다. 하지만 Macie는 자동으로 조사 결과 상태를 보관됨으로 변경합니다. 즉, 조사 결과는 Amazon Macie 콘솔에 기본적으로 표시되지 않지만 만료될 때까지 Macie에서 유지됩니다. Macie는 조사 결과를 90일 동안 저장합니다.

또한 Macie는 안 보이게 한 결과를 Amazon EventBridge에 이벤트로서 혹은 AWS Security Hub에 게시하지 않습니다. 하지만 Macie는 사용자가 숨기는 민감한 데이터 결과와 상관 관계가 있는 민감한 데이터 검색 결과를 계속 생성하고 저장합니다. 이렇게 하면 수행하는 데이터 개인 정보 보호 및 보호 감사 또는 조사에 대한 민감한 데이터 결과 기록이 있는지 확인할 수 있습니다.

> **Note**
>
> 계정이 여러 개의 Macie 계정을 중앙에서 관리하는 조직에 속해 있는 경우 해당 계정에 대한 억제 규칙이 다르게 적용될 수 있습니다. 이는 숨기려는 조사 결과의 범주와 Macie 관리자 계정이 있는지 아니면 회원 계정이 있는지에 따라 달라집니다.
>
> - 정책 조사 결과 — Macie 관리자만이 조직 계정에 대한 정책 조사 결과를 숨길 수 있습니다.
>
> Macie 관리자 계정이 있고 억제 규칙을 생성하는 경우 특정 계정을 제외하도록 규칙을 구성하지 않는 한 조직의 모든 계정에 대한 정책 결과에 해당 규칙이 적용됩니다. Macie 회원 계정이 있는데 계정에 대한 정책 결과를 숨기고 싶다면 Macie 관리자에게 문의하세요.
> - 민감한 데이터 검색 결과 - Macie 관리자와 개별 구성원은 민감한 데이터 검색 작업에서 발생하는 민감한 데이터 검색 결과를 숨길 수 있습니다. 또한 Macie 관리자는 조직의 민감한 데이터 자동 검색을 수행하는 동안 Macie가 생성하는 결과를 숨길 수 있습니다.
>
> 민감한 데이터 검색 작업을 만든 계정만 해당 작업에서 생성되는 민감한 데이터 검색 결과를 숨기거나 액세스할 수 있습니다. 조직의 Macie 관리자 계정만 조직의 계정에 대해 민감한 데이터 자동 검색이 생성하는 결과를 표시하지 않거나 다른 방법으로 액세스할 수 있습니다.
>
> 관리자와 구성원이 수행할 수 있는 작업에 대한 자세한 내용은 Amazon Macie 관리자 및 멤버 계정 간의 관계 이해을 참조하세요.

억제 규칙을 생성하고 관리하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 다음 주제에서는 방법을 설명합니다. API의 경우 항목에는 AWS Command Line Interface(AWS CLI) 를 사용하여 이러한 작업을 수행하는 방법에 대한 예가 포함되어 있습니다. 또한 최신 버전의 또 다른 AWS 명령줄 도구 또는 AWS SDK를 사용하거나 Macie에 직접 HTTPS 요청을 보냄으로써 이 작업을 수행할 수도 있습니다. AWS도구와 SDK에 대한 자세한 내용은, AWS 기반의 도구를 참조하세요.

주제

억제 규칙 생성

억제 규칙을 생성하기 전에 억제 규칙을 사용하여 억제하는 검색 결과는 복원(보관 취소)할 수 없다는 점에 유의해야 합니다. 하지만 Amazon Macie 콘솔에서 안 보이게 한 조사 결과를 검토하고 Amazon Macie API를 사용하여 숨겨진 결과에 액세스할 수 있습니다.

억제 규칙을 생성할 때 필터 기준, 이름, 선택 사항으로 규칙에 대한 설명을 지정합니다. Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 억제 규칙을 생성할 수 있습니다.

Console

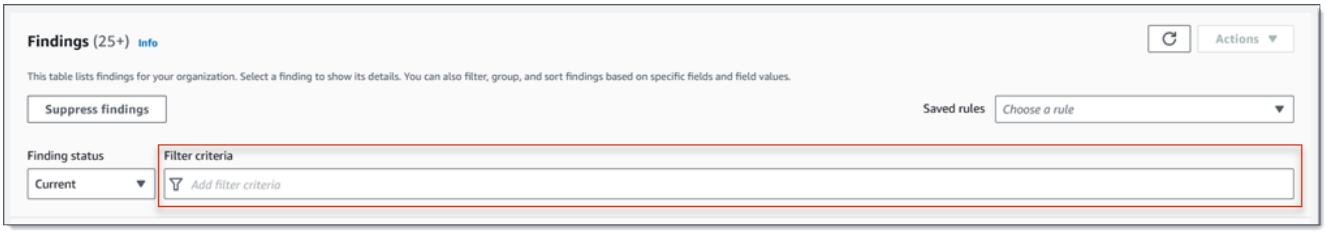
Amazon Macie 콘솔을 사용하여 억제 규칙을 만들려면 다음 단계를 따르세요.

억제 규칙을 생성하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.

> **Tip**
>
> 기존 억제 또는 필터 규칙을 시작점으로 사용하려면 저장된 규칙 목록에서 규칙을 선택합니다.
> 사전 정의된 논리 그룹별로 조사 결과를 피벗하고 드릴다운하여 규칙을 간편하게 생성할 수 있습니다. 이렇게 하면 Macie가 적절한 필터 조건을 자동으로 만들어 적용하므로 규칙을 만들 때 유용한 출발점이 될 수 있습니다. 이렇게 하려면 탐색 창(조사 결과 아래)에서 버킷별, 유형별 또는 작업별을 선택한 다음 테이블에서 항목을 선택합니다. 디테일 패널에서 피벗할 필드의 링크를 선택합니다.

3. 필터 기준 상자에 규칙에서 제외하려는 조사 결과의 속성을 지정하는 필터 조건을 추가합니다.



필터 조건을 추가하는 방법을 알아보려면 조사 결과에 필터 생성 및 적용을 참조하십시오.

4. 규칙에 필터 조건을 모두 추가했으면 조사 결과 숨기기를 선택합니다.
5. 억제 규칙에서 규칙의 이름과 선택 사항으로 규칙에 대한 설명을 입력합니다.
6. 저장을 선택합니다.

API

프로그래밍 방식으로 억제 규칙을 생성하려면 Amazon Macie API의 CreateFindingsFilter 작업을 사용하고 필수 파라미터에 적절한 값을 지정하세요:.

- `action` 파라미터의 경우, Macie가 규칙 기준과 일치하는 결과를 숨기도록 `ARCHIVE`를 지정하세요.
- `criterion` 파라미터의 경우, 규칙의 필터 기준을 정의하는 조건 맵을 지정하세요.

  맵에서 각 조건은 필드, 연산자 및 필드에 대한 하나 이상의 값을 지정해야 합니다. 값의 유형과 개수는 선택한 필드와 연산자에 따라 달라집니다. 조건에 사용할 수 있는 필드, 연산자 및 값 유형에 대한 자세한 내용은 조사 결과 필터링 필드, 조건에서·연산자 사용 및 필드 값 지정 을 참조하십시오.

AWS CLI을(를) 사용하여 억제 규칙을 만들려면 create-findings-filter 명령을 실행하고 필요한 파라미터에 적절한 값을 지정합니다. 다음 예제에서는 S3 객체의 현재 AWS 리전 및 보고서에서 발견된 모든 민감한 데이터 결과(다른 유형의 민감한 데이터는 제외)를 반환하는 억제 규칙을 생성합니다.

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

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
```

```
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS"]}}}'
```

이 예제는 Microsoft Windows용으로 포맷되었으며 가독성을 높이기 위해 캐럿(^) 줄 연속 문자를 사용합니다.

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.detections.type\":{\"eqExactMatch\":
[\"ADDRESS\"]}}}
```

위치:

- *my_suppression_rule*은 규칙의 사용자 지정 이름입니다.
- `criterion` 규칙의 필터 조건 맵입니다.
  - *classificationDetails.result.sensitiveData.detections.type*은Sensitive data detection type필드의 JSON 이름입니다.
  - *eqExactMatch*는 동일 완전 일치 연산자를 지정합니다.
  - *ADDRESS*는 민감한 데이터 탐지 유형 필드의 열거 값입니다.

이 명령이 성공적으로 실행되면 다음과 비슷한 출력이 표시됩니다.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

여기서 `arn`은 생성된 억제 규칙의 Amazon 리소스 이름(ARN)이며 `id`는 규칙의 고유 식별자입니다.

필터 기준의 추가 예는 Amazon Macie API를 사용하여 프로그래밍 방식으로 조사 결과 필터링을 참조하세요.

안 보이게 한 조사 결과 검토

기본적으로 Macie는 Amazon Macie 콘솔에 안 보이게 한 결과를 표시하지 않습니다. 하지만 필터 설정을 변경하여 콘솔에서 이러한 조사 결과를 검토할 수 있습니다.

콘솔에서 숨겨진 조사 결과를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다. 조사 결과 페이지는 Macie가 지난 90일 간 현재의 AWS 리전에서 사용자의 계정을 위해 생성하거나 업데이트한 조사 결과를 보여 줍니다. 기본적으로 억제 규칙에 의해 안 보이게 된 조사 결과는 여기 포함되지 않습니다.
3. 상태 찾기의 경우, 다음 중 하나를 수행하세요.
   - 숨겨진 조사 결과만 표시하려면 [보관됨]을 선택합니다.
   - 안 보이는 결과와 보이는 결과를 모두 표시하려면 모두를 선택합니다.
   - 안 보이게 한 결과를 다시 숨기려면 현재를 선택합니다.

Amazon Macie API를 사용하여 안 보이게 한 결과에 액세스할 수도 있습니다. 안 보이게 한 조사 결과 목록을 검색하려면 ListFinding 작업을 사용하고 `archived`필드에 대해 `true`를 지정하는 필터 조건을 포함하세요. AWS CLI를 사용하여 이 작업을 수행하는 방법의 예는 프로그래밍 방식으로 조사 결과 필터링을(를) 참조하세요. 그런 다음 하나 이상의 안 보이게 한 조사 결과에 대한 세부 정보를 검색하려면, GetVinding 작업을 사용하고 검색할 각 조사 결과에 대해 고유한 식별자를 지정합니다.

억제 규칙 변경

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 언제든지 억제 규칙의 설정을 변경할 수 있습니다. 규칙에 태그를 지정하고 관리할 수도 있습니다.

태그는 사용자가 정의하여 특정 유형의 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별, 분류, 관리하는 데 도움이 됩니다. 자세한 내용은 Amazon Macie에 리소스 태그 지정(을)를 참조하세요.

Console

Amazon Macie 콘솔을 사용하여 기존 억제 규칙의 설정을 변경하려면 다음 단계를 따르세요.

억제 규칙 변경

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. 저장된 규칙 목록에서 변경하려는 억제 규칙 옆의 아이콘 편집 (✎) 을 선택합니다.
4. 다음을 수행하세요.
   - 규칙의 기준을 변경하려면 필터 기준 상자를 사용하여 규칙에서 제외하려는 조사 결과의 속성을 지정하는 조건을 입력합니다. 자세한 방법은 조사 결과에 필터 생성 및 적용 섹션을 참조하세요.
   - 규칙의 이름을 변경하려면 억제 규칙 아래의 이름 상자에 새 이름을 입력합니다.
   - 규칙의 설명을 변경하려면 억제 규칙 아래의 설명 상자에 새 설명을 입력합니다.
   - 규칙에 대한 태그를 할당, 검토 또는 편집하려면 억제 규칙에서 태그 관리를 선택합니다. 그런 다음 필요에 따라 태그를 검토하고 변경합니다. 규칙은 최대 50개의 태그를 가질 수 있습니다.
5. 변경 작업을 마치면, 저장을 선택합니다.

API

프로그래밍 방식으로 억제 규칙을 변경하려면 Amazon Macie API의 UpdateFindingsFilter 작업을 사용하세요. 요청을 제출할 때 지원되는 파라미터를 사용하여 변경하려는 각 설정에 대해 새 값을 지정하세요.

`id`매개 변수의 경우, 변경할 규칙의 고유 식별자를 지정하십시오. ListFindingsFilter 작업을 사용하여 계정에 대한 금지 및 필터 규칙 목록을 검색하면 이 식별자를 얻을 수 있습니다. AWS CLI를 사용하는 경우, list-findings-filters 명령을 실행하여 이 목록을 검색하십시오.

AWS CLI을(를) 사용하여 억제 규칙을 변경하려면 update-findings-filter 명령을 실행하고 지원되는 파라미터를 사용하여 변경하려는 각 설정에 대해 새 값을 지정합니다. 예를 들어 다음 명령은 기존 억제 규칙의 이름을 변경합니다.

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --
name mailing_addresses_only
```

위치:

- *8a3c5608-aa2f-4940-b347-d1451example*는 규칙에 대한 고유 식별자입니다.
- *mailing_addresses_only*는 규칙의 새 이름입니다.

이 명령이 성공적으로 실행되면 다음과 비슷한 출력이 표시됩니다.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

여기서 arn은 변경된 규칙의 Amazon 리소스 이름(ARN)이며, id는 규칙의 고유 식별자입니다.

마찬가지로 다음 예제에서는 action 파라미터 값을 NOOP에서 ARCHIVE로 변경하여 필터 규칙을 억제 규칙으로 변환합니다.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action ARCHIVE
```

위치:

- *8a1c3508-aa2f-4940-b347-d1451example*는 규칙에 대한 고유 식별자입니다.
- *####*는 Macie가 규칙의 기준과 일치하는 조사 결과에 대해 수행하는 새로운 작업(조사 결과를 억제)입니다.

이 명령이 성공적으로 실행되면, 다음과 비슷한 출력이 표시됩니다.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

여기서 arn은 변경된 규칙의 Amazon 리소스 이름(ARN)이며, id는 규칙의 고유 식별자입니다.

억제 규칙 삭제

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 언제든지 억제 규칙을 삭제할 수 있습니다. 억제 규칙을 삭제하면 Macie는 규칙의 기준과 일치하고 다른 규칙에 의해 억제되지 않는 새로운 검색 결과 및 후속 검색 결과의 발생을 억제하지 않습니다. 하지만 Macie는 현재 처리 중이고 규칙 기준과 일치하는 결과를 계속 안 보이게 할 수도 있다는 점을 주의하세요.

억제 규칙을 삭제한 후에는 규칙의 기준과 일치하는 새로운 검색 결과와 이후에 발생하는 검색 결과의 상태가 현재(아카이브되지 않음)가 됩니다. 즉, Amazon Macie 콘솔에 기본적으로 표시됩니다. 또한 Macie는 이러한 결과를 Amazon EventBridge에 이벤트로서 게시합니다. 사용자 계정의 게시 설정에 따라 Macie는 조사 결과를 AWS Security Hub에 게시할 수도 있습니다.

Console

Amazon Macie 콘솔을 사용하여 억제 규칙을 삭제하려면 다음 단계를 따르세요.

억제 규칙 삭제

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 조사 결과를 선택합니다.
3. 저장된 규칙 목록에서 삭제하려는 억제 규칙 옆의 아이콘 편집 ( ) 을 선택합니다.
4. 억제 규칙에서 삭제를 선택합니다.

API

프로그래밍 방식으로 억제 규칙을 삭제하려면 Amazon Macie API의 DeleteFindingsFilter 작업을 사용하세요. `id` 파라미터의 경우 삭제할 억제 규칙의 고유 식별자를 지정합니다. ListFindingsFilter 작업을 사용하여 계정에 대한 금지 및 필터 규칙 목록을 검색하면 이 식별자를 얻을 수 있습니다. AWS CLI를 사용하는 경우, list-findings-filters 명령을 실행하여 이 목록을 검색하십시오.

AWS CLI을(를) 사용하여 억제 규칙을 삭제하려면 delete-findings-filter 명령을 실행합니다. 예:

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

여기서 *8a3c5608-aa2f-4940-b347-d1451example*은 삭제할 억제 규칙의 고유 식별자입니다.

명령이 성공적으로 실행되면, Macie는 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Macie는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

Amazon Macie 조사 결과에 대한 심각도 점수

Amazon Macie는 정책 또는 민감한 데이터 조사 결과를 생성할 때 조사 결과에 심각도를 자동으로 할당합니다. 조사 결과의 심각도는 조사 결과의 주요 특징을 반영하므로 결과를 평가하고 우선 순위를 정하는 데 도움이 될 수 있습니다. 조사 결과의 심각도는 영향을 받는 리소스가 조직에 미칠 수 있는 중요도나 중요성을 암시하거나 나타내지 않습니다.

정책 조사 결과의 심각도는 Amazon Simple Storage Service (Amazon S3) 범용 버킷의 보안 또는 개인 정보 보호와 관련된 잠재적 문제의 특성을 기반으로 합니다. 민감한 데이터 발견의 경우 심각도는 Macie가 S3 객체에서 발견한 민감한 데이터의 특성과 발생 횟수를 기반으로 합니다.

Macie에서는 조사 결과의 심각도가 두 가지 방식으로 표현됩니다.

심각도 수준

이는 심각도를 정성적으로 나타낸 것입니다. 심각도 수준은 심각도가 가장 낮은 Low부터 가장 심각한 High것까지 다양합니다.

심각도 수준은 Amazon Macie 콘솔에 바로 표시됩니다. 또한 Macie 콘솔, Amazon Macie API의 결과를 JSON으로 표현한 형태로도 사용할 수 있으며 민감한 데이터 검색 결과와 상관관계가 있는 민감한 데이터 검색 결과에서도 사용할 수 있습니다. 심각도 수준은 Macie가 EventBridge Amazon에 게시하는 이벤트와 Macie가 게시하는 조사 결과를 찾는 데도 포함됩니다. AWS Security Hub

심각도 점수

이는 심각도를 숫자로 나타낸 것입니다. 심각도 점수의 범위는 1~3이며 심각도 수준에 직접 반영됩니다.

심각도 점수	심각도 수준
1	낮음
2	중간
3	높음

심각도 점수는 Amazon Macie 콘솔에 직접 표시됩니다. 하지만 Macie 콘솔, Amazon Macie API의 결과를 JSON으로 표현한 형태로, 민감한 데이터 검색 결과와 상관관계가 있는 민감한 데이터 검색 결과에서도 사용할 수 있습니다. 심각도 점수는 Macie가 Amazon에 게시하는 이벤트를 찾는 데도 포함됩니다. EventBridge Macie가 발표하는 연구 결과에는 이러한 내용이 포함되지 않습니다. AWS Security Hub

이 섹션의 주제에서는 Macie가 정책 조사 결과 및 민감한 데이터 조사 결과의 심각도를 결정하는 방법을 설명합니다.

주제

정책 조사 결과에 대한 심각도 점수

정책 결과의 심각도는 S3 범용 버킷의 보안 또는 개인 정보 보호와 관련된 잠재적 문제의 특성을 기반으로 합니다. 다음 표에는 Macie가 각 유형의 정책 결과에 할당하는 심각도 수준이 나와 있습니다. 유형에 대한 자세한 내용은 조사 결과의 유형 섹션을 참조하세요.

찾기 유형	심각도 수준
Policy:IAMUser/S3BlockPublicAccessDisabled	높음
Policy:IAMUser/S3BucketEncryptionDisabled	낮음
Policy:IAMUser/S3BucketPublic	높음
Policy:IAMUser/S3BucketReplicatedExternally	높음
Policy:IAMUser/S3BucketSharedExternally	높음
Policy:IAMUser/S3BucketSharedWithCloudFront	중간

정책 조사 결과의 심각도는 조사 결과의 발생 횟수에 따라 달라지지 않습니다.

민감한 데이터 조사 결과에 대한 심각도 점수

민감한 데이터 조사 결과의 심각도는 Macie가 S3 객체에서 발견한 민감한 데이터의 특성과 발생 횟수를 기반으로 합니다. 다음 항목은 Macie가 각 유형의 민감한 데이터 조사 결과의 심각도를 결정하는 방법을 보여줍니다.

- SensitiveData:S3Object/Credentials
- SensitiveData:S3Object/CustomIdentifier
- SensitiveData:S3Object/Financial
- SensitiveData:S3Object/Personal
- SensitiveData:S3Object/Multiple

Macie가 민감한 데이터 조사 결과에서 탐지하고 보고할 수 있는 민감한 데이터 유형에 대한 자세한 내용은 관리형 데이터 식별자 사용 및 사용자 지정 데이터 식별자 빌드 을 참조하세요.

SensitiveData:S3Object/Credentials

A:S3객체/자격 증명 SensitiveData검색 결과는 S3 객체에 민감한 자격 증명 데이터가 포함되어 있음을 나타냅니다. 이러한 유형의 조사 결과에서 Macie는 Macie가 객체에서 찾은 자격 증명 데이터의 유형 및 발생 횟수를 기반으로 심각도를 결정합니다.

다음 표는 Macie가 S3 객체에서 자격 증명 데이터 발생을 보고하는 조사 결과에 할당하는 심각도 수준을 나타냅니다.

민감한 데이터 유형	1회 발생	2~99회 발생	100회 이상 발생
AWS 보안 액세스 키	높음	높음	높음
Google Cloud API 키	높음	높음	높음
HTTP Basic Authorization 헤더	높음	높음	높음
JSON Web Token(JWT)	높음	높음	높음
OpenSSH 프라이빗 키	높음	높음	높음

민감한 데이터 유형	1회 발생	2~99회 발생	100회 이상 발생
PGP 프라이빗 키	높음	높음	높음
퍼블릭 키 암호화 표준 (PKCS) 프라이빗 키	높음	높음	높음
PuTTY 프라이빗 키	높음	높음	높음
Stripe API 키	높음	높음	높음

SensitiveData:S3Object/CustomIdentifier

A:S3Object/ SensitiveDataCustomIdentifier파인딩은 S3 객체에 하나 이상의 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 텍스트가 포함되어 있음을 나타냅니다. 객체에는 두 가지 이상의 민감한 데이터 유형이 포함될 수 있습니다.

기본적으로 Macie는 이 유형의 검색에 중간 심각도를 할당합니다. 즉, S3 객체에 하나 이상의 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 텍스트가 하나 이상 포함되어 있는 경우 Macie는 자동으로 중간 심각도 수준을 조사 결과에 할당합니다. 조사 결과의 심각도는 사용자 지정 데이터 식별자의 기준과 일치하는 텍스트의 발생 횟수에 따라 달라지지 않습니다.

그러나 이러한 검색 유형의 심각도는 조사 결과를 생성한 사용자 지정 데이터 식별자에 대해 사용자 지정 심각도 설정을 정의한 경우 달라질 수 있습니다. 이 경우 Macie는 다음과 같이 심각도를 결정합니다.

- S3 객체에 단 하나의 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 텍스트가 포함된 경우 Macie는 해당 식별자의 심각도 설정을 기반으로 조사 결과의 심각도를 결정합니다.
- S3 객체에 둘 이상의 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 텍스트가 포함되어 있는 경우, Macie는 각 사용자 지정 데이터 식별자의 심각도 설정을 평가하여 심각도가 가장 높은 설정을 결정한 다음 조사 결과에 가장 높은 심각도를 할당하여 조사 결과의 심각도를 결정합니다.

사용자 지정 데이터 식별자의 심각도 설정을 검토하려면 Amazon Macie 콘솔의 탐색 창에서 사용자 지정 데이터 식별자를 선택합니다. 그런 다음 사용자 지정 데이터 식별자에 대한 이름을 선택합니다. 심각도 섹션에는 설정이 표시됩니다. 자세한 정보는 사용자 지정 데이터 식별자의 조사 결과 심각도 설정 정의을 참조하세요.

SensitiveData:S3Object/Financial

A:S3객체/재무 조사 결과는 S3 객체에 SensitiveData 민감한 금융 정보가 포함되어 있음을 나타냅니다. 이러한 유형의 조사 결과에 대해 Macie는 Macie가 객체에서 발견한 재무 정보의 유형 및 발생 횟수를 기반으로 심각도를 결정합니다.

다음 표는 Macie가 S3 객체에서 재무 정보의 발생을 보고하는 조사결과에 할당하는 심각도 수준을 표시합니다.

민감한 데이터 유형	1회 발생	2~99회 발생	100회 이상 발생
은행 계좌 번호 [1]	높음	높음	높음
신용 카드 유효 기간	낮음	중간	높음
신용 카드 마그네틱 스트립 데이터	높음	높음	높음
신용 카드 번호[2]	높음	높음	높음
신용 카드 인증 코드	중간	높음	높음

1. 기본 은행 계좌 번호(BBAN), 국제 은행 계좌 번호(IBAN), 캐나다 또는 미국 은행 계좌 번호 등 모든 유형의 은행 계좌 번호에 대한 심각도 수준은 동일합니다.
2. 키워드 근처에 있거나 키워드와 인접하지 않은 신용 카드 번호의 심각도 수준은 동일합니다.

조사 결과 객체에 있는 여러 유형의 금융 정보가 보고되는 경우 Macie는 Macie가 찾은 각 유형의 재무 정보에 대한 심각도를 계산하여 심각도가 가장 높은 유형을 결정한 다음 조사 결과에 가장 높은 심각도를 할당하여 조사 결과의 심각도를 결정합니다. 예를 들어 Macie가 객체에서 10개 신용 카드 만료 날짜(중간 심각도 수준)와 10개 신용 카드 번호(높은 심각도 수준)가 있는 것을 감지하면, Macie는 조사 결과에 높은 심각도 수준을 할당합니다.

SensitiveData:S3Object/Personal

A:S3객체/개인 SensitiveData조사 결과에 따르면 S3 객체에는 개인 건강 정보 (PHI), 개인 식별 정보 (PII) 또는 이 둘의 조합 등 민감한 개인 정보가 포함되어 있습니다. 이러한 유형의 조사 결과에 대해 Macie는 Macie가 객체에서 발견한 개인 정보의 유형 및 발생 횟수를 기준으로 심각도를 결정합니다.

다음 표는 Macie가 S3 객체의 PHI 발생을 보고하는 민감한 데이터 발견에 할당하는 심각도 수준을 나타냅니다.

민감한 데이터 유형	1회 발생	2~99회 발생	100회 이상 발생
마약단속국(DEA) 등록 번호	높음	높음	높음
건강 보험 청구 번호 (HICN)	높음	높음	높음
건강 보험 또는 의료 식별 번호	높음	높음	높음
Healthcare Common Procedure Coding System(HCPCS) 코드	높음	높음	높음
국가 의약품 코드 (NDC)	높음	높음	높음
국가 공급자 식별자 (NPI)	높음	높음	높음
고유 디바이스 식별자 (UDI)	낮음	중간	높음

다음 표는 Macie가 S3 객체의 PII 발생을 보고하는 민감한 데이터 발견에 할당하는 심각도 수준을 나타냅니다.

민감한 데이터 유형	1회 발생	2~99회 발생	100회 이상 발생
생년월일	낮음	중간	높음
운전면허증 식별 번호	낮음	중간	높음
선거인단 번호	높음	높음	높음
전체 이름	낮음	중간	높음
위성 항법 시스템 (GPS) 좌표	낮음	중간	중간
HTTP 쿠키	낮음	중간	높음
우편 주소	낮음	중간	높음
국적 식별 번호	높음	높음	높음
National Insurance Number(NINO)	높음	높음	높음
여권 번호	중간	높음	높음
영주권 번호	높음	높음	높음
전화번호	낮음	중간	높음
Social Insurance Number(SIN)	높음	높음	높음
사회 보장 번호(SSN)	높음	높음	높음
납세자 식별 번호 또는 참조 번호	높음	높음	높음
차량 식별 번호(VIN)	낮음	낮음	중간

조사 결과가 객체의 여러 유형의 PHI, PII 또는 PHI와 PII 모두를 보고하는 경우 Macie는 각 유형의 심각도를 계산하여 심각도가 가장 높은 유형을 결정한 다음 가장 높은 심각도를 조사 결과에 할당하여 조사 결과의 심각도를 결정합니다.

예를 들어 Macie가 객체에서 전체 이름 10개(중간 심각도 수준)와 여권 번호 5개(높은 심각도 수준)를 탐지하면 Macie는 조사 결과에 심각도 높음 수준을 할당합니다. 마찬가지로 Macie가 객체에서 10개의 전체 이름(중간 심각도 수준)과 10개의 건강 보험 식별 번호(높은 심각도 수준)를 탐지하면 Macie는 조사 결과에 높은 심각도 수준을 할당합니다.

SensitiveData:S3Object/Multiple

A:S3객체/다중 SensitiveData검색 결과는 S3 객체에 하나 이상의 사용자 지정 데이터 식별자의 탐지 기준과 일치하는 자격 증명 데이터, 재무 정보, 개인 정보 또는 텍스트의 모든 조합 등 여러 민감한 데이터 범주에 걸친 데이터가 포함되어 있음을 나타냅니다.

이러한 유형의 검색에서 Macie는 Macie가 발견한 각 유형의 민감한 데이터에 대한 심각도를 계산하고 (이전 항목에서 설명함), 심각도가 가장 높은 유형을 결정한 다음 조사 결과에 가장 높은 심각도를 할당하여 심각도를 결정합니다.

예를 들어 Macie가 객체에서 10개의 전체 이름 (중간 심각도 수준) 과 10개의 AWS 비밀 액세스 키 (높은 심각도 수준) 를 탐지하면 Macie는 검색 결과에 높은 심각도 수준을 할당합니다.

Amazon Macie 조사 결과 모니터링 및 처리

Amazon Macie는 모니터링 또는 이벤트 관리 시스템과 같은 다른 애플리케이션, 서비스 및 시스템과의 통합을 지원하기 위해 Amazon EventBridge에 정책 및 민감한 데이터 조사 결과를 이벤트로 자동 게시합니다. 조직의 보안 태세에 대한 추가 지원 및 광범위한 분석을 위해 정책 및 민감한 데이터 조사 결과를 AWS Security Hub에 게시하도록 Macie를 구성할 수도 있습니다.

Amazon EventBridge

Amazon EventBridge(전 Amazon CloudWatch Events)는 애플리케이션 및 서비스에서 실시간 데이터 스트림을 전달하고 해당 데이터를 AWS Lambda 함수, Amazon Simple Notification Service 주제 및 Amazon Kinesis 스트림과 같은 대상으로 라우팅하는 서버리스 이벤트 버스 서비스입니다. EventBridge를 사용하면 Macie가 조사 결과를 위해 게시하는 이벤트를 포함하여 특정 유형의 이벤트에 대한 모니터링 및 처리를 자동화할 수 있습니다. EventBridge에 대해 자세히 알아보려면 Amazon EventBridge 사용 설명서를 참조하세요.

AWS 사용자 알림을 Macie와 통합하면 EventBridge 이벤트를 사용하여 Macie가 조사 결과를 위해 게시하는 이벤트에 대한 알림을 자동으로 생성할 수도 있습니다. 사용자 알림을 사용하면 사용자 지정 규칙을 만들고 관심 있는 EventBridge 이벤트에 대한 알림을 수신하기 위한 전송 채널을 구성할 수 있습니다. 전송 채널에는 이메일, AWS Chatbot 채팅 알림 및 AWS Console Mobile Application 푸시 알림이 포함됩니다. AWS Management Console의 중앙 위치에서 알림을 검토할 수도 있습니다. 사용자 알림에 대해 자세히 알아보려면 AWS 사용자 알림 사용 설명서를 참조하세요.

AWS Security Hub

AWS Security Hub은(는) AWS 환경 전반의 보안 상태에 대한 포괄적인 뷰를 제공하는 보안 서비스입니다. 이는 AWS 서비스 및 지원되는 보안 솔루션에서 AWS Partner Network 보안 데이터를 수집하며 보안 업계 표준 및 모범 사례와 비교하여 환경을 확인할 수 있습니다. 또한 이 서비스는 보안 추세를 분석하고 우선 순위가 가장 높은 보안 문제를 식별하는 데 도움을 줍니다. Security Hub를 사용하면 조직의 보안 태세에 대한 광범위한 분석의 일환으로 Macie의 조사결과를 검토할 수 있습니다. 또한 여러 AWS 리전의 조사 결과를 집계하고 집계된 결과 데이터를 단일 리전에서 모니터링 및 처리할 수 있습니다. 에 대한 자세한 내용은 AWS Security Hub 사용 설명서를 참조하세요.

Macie는 조사 결과를 생성하면 자동으로 해당 결과를 EventBridge에 새 이벤트로 게시합니다. 사용자 계정의 선택한 게시 설정에 따라 Macie는 조사 결과를 Security Hub에 게시할 수도 있습니다. Macie는 조사 결과 처리가 끝난 후 각각의 새로운 조사 결과를 즉시 게시합니다. 기존 정책 조사 결과가 이후에 발생하는 것을 감지하면 조사 결과의 기존 EventBridge 이벤트에 대한 업데이트를 게시합니다. 게시

설정에 따라 Macie는 업데이트를 Security Hub에 게시할 수도 있습니다. Macie는 계정의 게시 설정에 지정된 게시 빈도를 사용하여 이러한 업데이트를 반복적으로 게시합니다.

주제

- Amazon Macie 조사 결과에 대한 게시 설정 구성
- Amazon Macie, Amazon EventBridge와 통합
- Amazon Macie와 통합 AWS Security Hub
- Amazon Macie와 AWS 사용자 알림 통합
- Amazon Macie 조사 결과를 위한 Amazon EventBridge 이벤트 스키마

Amazon Macie 조사 결과에 대한 게시 설정 구성

다른 애플리케이션, 서비스 및 시스템과의 통합을 지원하기 위해 Amazon Macie는 정책 결과와 민감한 데이터 결과를 모두 이벤트로 Amazon에 자동으로 게시합니다. EventBridge 결과를 모니터링하고 처리하는 EventBridge 데 사용할 수 있는 방법에 대한 자세한 내용은 을 참조하십시오. Amazon Macie, Amazon EventBridge와 통합

계정의 게시 설정에서 지정한 대상 옵션을 사용하여 조사 결과를 자동으로 게시하도록 Macie를 구성할 수 AWS Security Hub 있습니다. 이러한 옵션을 사용하여 Security Hub에 정책 조사 결과만 게시하거나, 민감한 데이터 조사 결과만 게시하거나, 정책 및 민감한 데이터 검색 결과를 모두 게시하도록 Macie를 구성할 수 있습니다. 조사 결과를 Security Hub에 게시하지 않도록 Macie를 구성할 수도 있습니다. Security Hub를 사용하여 결과를 모니터링하고 처리하는 방법에 대한 자세한 내용은 Amazon Macie와 통합 AWS Security Hub을(를) 참조하세요.

정책 조사 결과의 경우, Macie가 다른 AWS 서비스 에 검색 결과를 게시하는 시기는 조사 결과가 새로운 것인지 여부와 계정에 지정한 게시 빈도에 따라 달라집니다. 민감한 데이터 조사 결과의 경우, 시기가 항상 즉각적입니다. Macie는 조사 결과 처리가 끝난 후 즉시 민감한 데이터 조사 결과를 게시합니다. 정책 조사 결과와는 달리 Macie는 민감한 데이터 조사 결과를 모두 새로운(고유한) 것으로 취급됩니다.

Macie는 금지 규칙에 의해 자동으로 보관되는 정책 또는 민감한 데이터 조사 결과를 게시하지 않습니다. 다시 말해, Macie는 숨겨진 결과를 다른 AWS 서비스에 공개하지 않습니다.

주제

- 조사 결과에 대한 게시 대상 선택
- 조사 결과에 대한 게시 빈도 설정

- 조사 결과에 대한 게시 빈도 변경

조사 결과에 대한 게시 대상 선택

Amazon AWS Security Hub 외에도 정책 및 민감한 데이터 조사 결과를 자동으로 게시하도록 Amazon Macie를 구성할 수 있습니다. EventBridge 기본적으로 Macie는 신규 및 업데이트된 정책 조사 결과만 Security Hub에 게시합니다. 기본 구성을 변경하거나 확장하려면 계정의 게시 대상 설정을 조정하십시오.

대상 설정을 조정할 때 Macie가 Security Hub에 게시할 검색 결과 범주를 선택합니다. 즉, 정책 조사 결과만, 민감한 데이터 조사 결과만 또는 정책 및 민감한 데이터 검색 결과만 둘 다 선택할 수 있습니다. 조사 결과 범주를 Security Hub에 게시하지 않도록 선택할 수도 있습니다.

대상 설정을 변경하는 경우, 변경 사항은 현재 AWS 리전에만 적용됩니다. 조직의 Macie 관리자인 경우, 변경 사항은 해당 계정에만 적용됩니다. 연결된 회원 계정에는 적용되지 않습니다. 자세한 설명은 여러 계정 관리 섹션을 참조하세요.

조사 결과에 대한 게시 대상을 선택하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 조사 결과 게시 섹션의 대상에서 다음 옵션 중 하나를 선택합니다.

   - Security Hub에 정책 결과 게시 - 새 정책 결과 및 업데이트된 정책 결과를 Security Hub에 자동으로 게시하기 시작하려면 이 확인란을 선택합니다. Security Hub에 대한 신규 및 업데이트된 정책 조사 결과 게시를 중단하려면 이 확인란의 선택을 취소합니다.

     이 확인란을 선택하고 기존 정책 결과가 있는 경우 Macie는 해당 결과를 Security Hub에 자동으로 게시하지 않습니다. 대신 Macie는 변경 내용을 저장한 후 생성하거나 업데이트한 정책 결과만 게시합니다.
   - 민감한 데이터 결과를 Security Hub에 게시 - Security Hub에 새 중요 데이터 탐지 결과를 자동으로 게시하려면 이 확인란을 선택합니다. 새로운 민감한 데이터 결과를 Security Hub에 게시하는 것을 중지하려면 이 확인란의 선택을 취소하십시오.

     이 확인란을 선택하고 기존에 민감한 데이터 탐지 결과가 있는 경우 Macie는 이를 Security Hub에 자동으로 게시하지 않습니다. 대신 Macie는 변경 내용을 저장한 후 생성되는 민감한 데이터 결과만 게시합니다.
4. 저장을 선택합니다.

검색 결과 범주를 Security Hub에 게시하기로 선택한 경우 현재 지역에서도 Security Hub를 활성화하고 Macie의 검색 결과를 수락하도록 구성해야 합니다. 그렇지 않으면 Security Hub에서 조사 결과에 액세스할 수 없습니다. Security Hub에서 조사 결과를 수락하는 방법을 알아보려면 AWS Security Hub 사용 설명서의 제품 통합 관리를 참조하세요.

조사 결과에 대한 게시 빈도 설정

Amazon Macie에서는 각 조사 결과에 고유한 식별자가 있습니다. Macie는 이 식별자를 사용하여 조사 결과를 다른 AWS 서비스에 게시할 시기를 결정합니다.

- 새 조사 결과 – Macie는 신규 정책 또는 민감한 데이터 조사 결과를 만들 때 조사 결과 처리의 일환으로 조사 결과에 고유한 식별자를 할당합니다. Macie는 결과 처리를 완료한 직후 해당 결과를 새 Amazon 이벤트로 게시합니다. EventBridge 사용자 계정의 게시 설정에 따라 Macie는 조사 결과를 새로운 조사 결과로 AWS Security Hub에 게시할 수도 있습니다.
- 업데이트된 조사 결과 – Macie가 기존 정책 검색 결과의 후속 발생을 감지하면 후속 조사 결과에 대한 세부 정보를 추가하고 발생 횟수를 늘려 기존 조사 결과를 업데이트합니다. 또한 Macie는 이러한 업데이트를 기존 EventBridge 이벤트에 게시하고 계정의 게시 설정에 따라 기존 Security Hub 검색 결과에도 게시합니다. Macie는 정책 조사 결과에 대해서만 이 작업을 수행합니다. 민감한 데이터 조사 결과는 정책 조사 결과와는 달리 모두 새로운(고유한) 것으로 취급됩니다.

  기본적으로 Macie는 반복 게시 주기의 일환으로 15분마다 업데이트된 조사 결과를 게시합니다. 즉, 가장 최근의 게시 주기 이후에 업데이트된 모든 정책 조사 결과는 보류되고 필요에 따라 다시 업데이트되며 다음 발행 주기(약 15분 후)에 포함됩니다. 다른 게시 빈도를 선택하여 이 일정을 변경할 수 있습니다. 예를 들어 1시간마다 업데이트된 조사 결과를 게시하도록 Macie를 구성한 후 12시에 게시하는 경우, 12:00 이후에 발생하는 모든 업데이트는 13:00에 게시됩니다.

단, 금지 규칙에 따라 자동으로 보관되는 조사 결과에는 이러한 경우, 모두 적용되지 않습니다. Macie는 숨겨진 결과를 다른 사람에게 게시하지 않습니다. AWS 서비스

조사 결과에 대한 게시 빈도 변경

Amazon Macie가 다른 사이트에 기존 정책 결과에 대한 업데이트를 게시하는 데 사용하는 일정을 변경할 수 있습니다. AWS 서비스기본적으로 Macie는 15분마다 업데이트된 조사 결과를 게시합니다. 이 일정을 변경하면 현재 AWS 리전에만 변경 사항이 적용됩니다. 사용자가 조직의 Macie 관리자인 경우, 변경 내용이 해당 리전의 모든 관련 회원 계정에도 적용됩니다. 자세한 설명은 여러 계정 관리 섹션을 참조하세요.

업데이트된 조사 결과에 대한 게시 빈도를 변경하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 조사 결과 게시 섹션의 정책 조사 결과 업데이트 주기에서 Macie가 업데이트된 정책 결과를 다른 AWS 서비스에 게시할 빈도를 선택합니다.
4. 저장을 선택합니다.

Amazon Macie, Amazon EventBridge와 통합

Amazon EventBridge(전 Amazon CloudWatch Events)는 서버리스 이벤트 버스 서비스입니다. EventBridge는 애플리케이션 및 서비스의 실시간 데이터 스트림을 제공한 다음, 해당 데이터를 AWS Lambda 함수, Amazon Simple Notification Service(SNS) 주제, Amazon Kinesis 스트림 등의 대상으로 라우팅합니다. EventBridge에 대해 자세히 알아보려면 Amazon EventBridge 사용 설명서를 참조하세요.

EventBridge를 사용하면 특정 유형의 이벤트에 대한 모니터링 및 처리를 자동화할 수 있습니다. 여기에는 Amazon Macie가 새로운 정책 조사 결과 및 민감한 데이터 조사 결과에 대해 자동으로 게시하는 이벤트가 포함됩니다. 또한 Macie가 이후에 기존 정책 결과가 발생할 경우를 대비하여 자동으로 게시하는 이벤트도 포함됩니다. Macie가 이러한 이벤트를 게시하는 방법 및 시기에 대한 자세한 내용은 조사 결과에 대한 게시 설정 구성 섹션을 참조하세요.

EventBridge와 Macie가 조사 결과에 대해 게시하는 이벤트를 사용하면 거의 실시간으로 결과를 모니터링하고 처리할 수 있습니다. 그런 다음, 다른 애플리케이션과 서비스를 사용하여 결과에 따라 조치를 취할 수 있습니다. 예를 들어 EventBridge를 사용하여 특정 유형의 새로운 조사 결과를 AWS Lambda 함수에 보낼 수 있습니다. 그러면 Lambda 함수가 데이터를 처리하여 보안 인시던트 및 이벤트 관리(SIEM)시스템으로 전송할 수 있습니다. AWS 사용자 알림을 Macie와 통합하는 경우, 이벤트를 사용하여 지정한 전송 채널을 통해 자동으로 조사 결과에 대한 알림을 받을 수도 있습니다.

자동 모니터링 및 처리 외에도 EventBridge를 사용하면 조사 결과 데이터를 장기간 보존할 수 있습니다. Macie는 조사 결과를 90일 동안 저장합니다. EventBridge를 사용하면 조사 결과 데이터를 선호하는 스토리지 플랫폼으로 보내고 원하는 기간 동안 데이터를 저장할 수 있습니다.

> **Note**
>
> 장기 보존의 경우, 민감한 데이터 검색 결과를 S3 버킷에 저장하도록 Macie를 구성할 수있습니다. 민감한 데이터 검색 결과는 객체에 민감한 데이터가 포함되어 있는지 여부를 확인하기 위

해 Macie가 S3 객체에 대해 수행한 분석에 대한 세부 정보를 기록하는 레코드입니다. 자세한 내용은 민감한 데이터 검색 결과 저장 및 유지(을)를 참조하세요.

주제

- Amazon EventBridge 작업
- 조사 결과에 대한 Amazon EventBridge 규칙 생성

Amazon EventBridge 작업

Amazon EventBridge를 사용하면, 모니터링하려는 이벤트와 해당 이벤트에 대해 자동화된 작업을 수행하려는 대상을 지정하는 규칙을 생성할 수 있습니다. 대상은 EventBridge가 이벤트를 보내는 대상입니다.

조사 결과에 대한 모니터링 및 처리 태스크를 자동화하려면 Amazon Macie 조사 결과 이벤트를 자동으로 감지하고 처리 또는 기타 태스크를 위해 이러한 이벤트를 다른 애플리케이션 또는 서비스로 보내는 EventBridge 규칙을 생성할 수 있습니다. 특정 기준을 충족하는 이벤트만 전송하도록 규칙을 조정할 수 있습니다. 이렇게 하려면 조사 결과에 대한 EventBridge 이벤트 스키마에서 파생된 기준을 지정하세요.

예를 들어, 특정 유형의 새 조사 결과를 AWS Lambda 함수에 보내는 규칙을 생성할 수 있습니다. 그러면 Lambda 함수는 데이터를 처리하여 SIEM 시스템으로 전송하거나, 특정 유형의 서버 측 암호화를 S3 객체에 자동으로 적용하거나, 객체의 액세스 제어 목록(ACL)을 변경하여 S3 객체에 대한 액세스를 제한하는 등의 태스크를 수행할 수 있습니다. 또는 심각도가 높은 새로운 조사 결과를 Amazon SNS 주제에 자동으로 보내는 규칙을 생성하여 인시던트 대응 팀에 결과를 알릴 수 있습니다.

EventBridge는 Lambda 함수를 호출하고 Amazon SNS 주제를 알리는 것 외에도 Amazon Kinesis 스트림에 이벤트를 릴레이하고, AWS Step Functions 상태 시스템을 활성화하고, AWS Systems Manager 실행 명령을 호출하는 등 다른 유형의 대상 및 작업을 지원합니다. 지원되는 대상에 대한 자세한 정보는 Amazon EventBridge 사용 설명서의 Amazon EventBridge 대상을 참조하세요.

조사 결과에 대한 Amazon EventBridge 규칙 생성

다음 절차에서는 Amazon EventBridge 콘솔 및 AWS Command Line Interface(AWS CLI)를 사용하여 Amazon Macie 조사 결과에 대한 EventBridge 규칙을 생성하는 방법에 대해 설명합니다. 규칙은 Macie 조사 결과에 대한 이벤트 스키마 및 패턴을 사용하는 EventBridge 이벤트를 감지한 다음, 처리를 위해 해당 이벤트를 AWS Lambda 함수로 전송합니다.

AWS Lambda는 서버를 프로비저닝하거나 관리하지 않고 코드를 실행하는 데 사용할 수 있는 컴퓨팅 서비스입니다. 코드를 패키징하여 AWS Lambda에 로Lambda 함수로 업로드합니다. 그러면 AWS Lambda에서는 해당 함수가 호출될 때 실행합니다. 함수는 이벤트에 대한 응답으로 또는 애플리케이션 또는 서비스의 요청에 대한 응답으로 사용자가 수동으로 또는 자동으로 호출할 수 있습니다. Lambda 함수에 대한 자세한 내용은 AWS Lambda개발자 가이드를 참조하세요.

Console

이 절차에서는 Amazon EventBridge 콘솔을 사용하여 모든 Macie 조사 결과 이벤트를 Lambda 함수로 자동 전송하여 처리하는 규칙을 생성하는 방법을 설명합니다. 규칙은 특정 이벤트가 수신될 때 실행되는 규칙의 기본 설정을 사용합니다. 규칙 설정에 대한 자세한 내용이나 사용자 지정 설정을 사용하는 규칙을 생성하는 방법을 알아보려면 Amazon EventBridge 사용 설명서의 Creating rules that react to events 섹션을 참조하세요.

> **Tip**
>
> 또한 사용자 지정 이벤트 패턴을 사용하여 Macie 조사 결과 이벤트의 하위 세트만 감지하고 이에 따라 동작하는 규칙을 생성할 수 있습니다. 이 하위 세트는 Macie가 해당 이벤트에 포함하는 특정 필드를 기반으로 할 수 있습니다. 사용 가능한 필드에 대한 자세한 내용은 조사 결과에 대한 EventBridge 이벤트 스키마 섹션을 참조하세요. 이러한 유형의 규칙을 생성하는 방법을 알아보려면 Amazon EventBridge 사용 설명서의 Content filtering in event patterns 섹션을 참조하세요.

규칙을 생성하려면 규칙에서 대상으로 사용하도록 하려는 Lambda 함수를 생성합니다. 규칙을 생성할 때 이 함수를 규칙의 대상으로 지정해야 합니다.

콘솔을 사용하여 이벤트 규칙을 생성하려면

1. https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.
2. 탐색 창의 Events(이벤트) 아래에서 Rules(규칙)를 선택합니다.
3. Rules(규칙) 섹션에서 Create rule(규칙 생성)을 선택합니다.
4. 규칙 세부 정보 정의 페이지에서 다음을 수행합니다.
   - Name(이름)에 규칙 이름을 입력합니다.
   - (선택 사항) 설명에 규칙에 대한 간략한 설명을 입력합니다.
   - 이벤트 버스의 경우 기본값이 선택되어 있고 선택한 이벤트 버스에 대해 규칙 활성화가 켜져 있는지 확인하세요.

- 규칙 유형(Rule type)에서 이벤트 패턴이 있는 규칙(Rule with an event pattern)을 생성합니다.

5. 마쳤으면 Next를 선택합니다.
6. 이벤트 패턴 빌드 페이지에서 다음을 수행합니다.

   - 이벤트 소스에서 AWS 이벤트 또는 EventBridge 파트너를 선택합니다.
   - (선택 사항) 샘플 이벤트의 경우 Macie의 샘플 조사 결과 이벤트를 검토하여 이벤트에 포함될 수 있는 항목을 알아보세요. 이렇게 하려면 AWS 이벤트를 선택하세요. 그런 다음 샘플 이벤트에서 Macie 조사 결과를 선택합니다.
   - 이벤트 패턴섹션에서 이벤트 패턴 양식을 선택합니다. 다음 설정을 입력합니다.
     - 이벤트 소스에서 AWS 서비스를 선택합니다.
     - AWS 서비스에는 Macie를 입력합니다.
     - 이벤트 유형에는 Macie 조사 결과를 입력합니다.
7. 마쳤으면 Next를 선택합니다.
8. 대상 선택 페이지에서 다음을 수행합니다.

   - 대상 유형(Target types)에서 AWS 서비스를 선택합니다.
   - 대상 선택에서 Lambda 함수를 입력합니다. 그런 다음 함수에서 이벤트를 보낼 함수를 선택합니다.
   - 버전/별칭 구성에 대상 Lambda 함수의 버전 및 별칭 설정을 입력합니다.
   - (선택 사항) 추가 설정의 경우 사용자 지정 설정을 입력하여 Lambda 함수로 전송할 이벤트 데이터를 지정합니다. 함수에 성공적으로 전달되지 않은 이벤트를 처리하는 방법도 지정할 수 있습니다.
9. 마쳤으면 Next를 선택합니다.
10. 태그 구성 페이지에서 규칙에 할당할 하나 이상의 태그를 선택적으로 입력합니다. 이후 다음을 선택합니다.
11. 검토 및 생성 페이지에서 규칙의 설정을 검토하고 올바른지 확인합니다.

    설정을 변경하려면, 설정이 포함된 섹션에서 편집을 선택한 다음, 올바른 설정을 입력합니다. 탐색 탭을 사용하여 설정이 포함된 페이지로 이동할 수도 있습니다.
12. 설정 검증을 마치면 생성를 선택합니다.

AWS CLI

이 절차는 AWS CLI을(를) 사용하여 모든 Macie 조사 결과 이벤트를 Lambda 함수로 전송하여 처리하는 EventBridge 규칙을 생성하는 방법을 설명합니다. 규칙은 특정 이벤트가 수신될 때 실행되는 규칙의 기본 설정을 사용합니다. 이 절차에서 명령은 Microsoft Windows용으로 형식이 지정됩니다. Linux, macOS 또는 Linux의 경우 캐럿(^) 행 연속 문자를 백슬래시(\)로 바꿉니다.

규칙을 생성하려면 규칙에서 대상으로 사용하도록 하려는 Lambda 함수를 생성합니다. 함수를 생성할 때 함수의 Amazon 리소스 이름(ARN) 을 기록하세요. 규칙에 대한 대상을 지정할 때 이 ARN을 입력해야 합니다.

AWS CLI을(를) 사용하여 이벤트 규칙 생성

1. Macie가 EventBridge에 게시한 모든 결과에 대한 이벤트를 감지하는 규칙을 만드세요. 이 작업을 수행하려면 EventBridge put-rule 명령을 사용합니다. 예:

```
C:\> aws events put-rule ^
--name MacieFindings ^
--event-pattern "{\"source\":[\"aws.macie\"]}"
```

여기서 *MacieFindings*는 원하는 규칙 이름입니다.

이 명령이 성공적으로 실행되면 EventBridge는 규칙의 ARN을 사용하여 응답합니다. ARN을 적어 두세요. 3단계에서 이 정보가 필요합니다.

> **Tip**
>
> 또한 사용자 지정 이벤트 패턴을 사용하여 Macie 조사 결과 이벤트의 하위 세트만 감지하고 이에 따라 동작하는 규칙을 생성할 수 있습니다. 이 하위 세트는 Macie가 해당 이벤트에 포함하는 특정 필드를 기반으로 할 수 있습니다. 사용 가능한 필드에 대한 자세한 내용은 조사 결과에 대한 EventBridge 이벤트 스키마 섹션을 참조하세요. 이러한 유형의 규칙을 생성하는 방법을 알아보려면 Amazon EventBridge 사용 설명서의 Content filtering in event patterns 섹션을 참조하세요.

2. 규칙의 대상으로 사용할 Lambda 함수를 지정합니다. 이 작업을 수행하려면 EventBridge put-targets 명령을 사용합니다. 예:

```
C:\> aws events put-targets ^
--rule MacieFindings ^
```

```
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-
findings-function
```

위의 명령에서 *MacieFindings*는 1단계에서 규칙에 대해 지정한 이름이고, Arn 파라미터 값은 규칙에서 대상으로 사용하도록 할 함수의 ARN입니다.

3. 규칙이 대상 Lambda 함수를 호출하도록 허용하는 권한을 추가합니다. 이렇게 하려면 Lambda add-permission 명령을 사용합니다. 예:

```
C:\> aws lambda add-permission ^
--function-name my-findings-function ^
--statement-id Sid ^
--action lambda:InvokeFunction ^
--principal events.amazonaws.com ^
--source-arn arn:aws:events:regionalEndpoint:accountId:rule:MacieFindings
```

위치:

- *my-findings-function*은 규칙에서 대상으로 사용하도록 할 Lambda 함수의 이름입니다.
- *Sid*는 Lambda 함수 정책의 명령문을 설명하기 위해 정의하는 고유 식별자입니다.
- source-arn은 EventBridge 규칙의 ARN입니다.

이 명령이 성공적으로 실행되면, 다음과 비슷한 출력이 표시됩니다.

```
{
  "Statement": "{\"Sid\":\"sid\",
    \"Effect\":\"Allow\",
    \"Principal\":{\"Service\":\"events.amazonaws.com\"},
    \"Action\":\"lambda:InvokeFunction\",
    \"Resource\":\"arn:aws:lambda:us-east-1:111122223333:function:my-findings-
function\",
    \"Condition\":
      {\"ArnLike\":
        {\"AWS:SourceArn\":
         \"arn:aws:events:us-east-1:111122223333:rule/MacieFindings\"}}}"
}
```

Statement 값은 Lambda 함수 정책에 추가된 문의 JSON 문자열 버전입니다.

Amazon Macie와 통합 AWS Security Hub

AWS Security Hub 서비스에서는 사용자에게 사용자 AWS 환경에서의 보안 상태를 포괄적으로 제공하며 보안 업계 표준 및 모범 사례와 비교하여 환경을 점검합니다. 이는 부분적으로 AWS 서비스지원되는 AWS Partner Network여러 보안 솔루션에서 얻은 조사 결과를 사용하고, 집계하고, 구성하고, 우선 순위를 정하는 방식으로 이루어집니다. Security Hub는 보안 추세를 분석하고 우선순위가 가장 높은 보안 문제를 분석하는 데 도움이 됩니다. 또한 Security Hub를 사용하여 여러 AWS 리전의 조사 결과를 집계하고 집계된 조사 결과 데이터를 단일 리전에서 모니터링 및 처리할 수도 있습니다. 에 대한 자세한 내용은 AWS Security Hub 사용 설명서를 참조하세요.

Amazon Macie는 Security Hub와 통합되므로 Macie의 조사 결과를 Security Hub에 자동으로 게시할 수 있습니다. 그러면 Security Hub의 보안 태세 분석에 이러한 결과가 포함됩니다. 또한 Security Hub를 사용하여 사용자 AWS 환경에 대한 대규모 집계된 조사 결과 데이터 집합의 일부로 정책 및 민감한 데이터 탐지 결과를 모니터링하고 처리할 수 있습니다. 즉, 조직의 보안 태세를 폭넓게 분석하면서 Macie의 조사 결과를 분석하고 필요에 따라 결과를 수정할 수 있습니다. Security Hub를 사용하면 여러 공급자로부터 많은 양의 조사 결과를 처리해야 하는 복잡성을 줄일 수 있습니다. 또한, Macie의 조사 결과를 포함하여 모든 조사 결과에 대해 표준 형식을 사용합니다. 이 형식인 AWS보안 조사 결과 형식(ASFF)을 사용하면 시간이 많이 걸리는 데이터 변환 작업을 수행할 필요가 없습니다.

주제

- Amazon Macie가 조사 결과를 AWS Security Hub로 게시하는 방법
- AWS Security Hub에서 Amazon Macie 조사 결과의 예
- AWS Security Hub 통합 활성화 및 구성
- AWS Security Hub에 대한 조사 결과 게시 중지

Amazon Macie가 조사 결과를 AWS Security Hub로 게시하는 방법

AWS Security Hub에서, 보안 문제를 조사 결과로서 추적합니다. 일부 조사 결과는 Amazon Macie 와 같은 AWS 서비스에 의해 또는 지원되는 AWS Partner Network 보안 솔루션에서 감지한 문제에서 나옵니다. Security Hub에는 보안 문제를 감지하고 결과를 생성하는 데 사용하는 규칙 집합도 있습니다.

Security Hub는 이러한 모든 출처의 조사 결과를 관리할 도구를 제공합니다. 사용자는 조사 결과 목록을 조회하고 필터링할 수 있으며 주어진 조사 결과의 세부 정보를 조회할 수도 있습니다. 방법을 알아보려면 AWS Security Hub사용 설명서의 조사 결과 목록 및 세부 정보 보기를 참조하세요. 또한 주어진 결과에 대한 조사 상태를 추적할 수도 있습니다. 방법을 알아보려면, AWS Security Hub 사용 설명서에서 조사 결과에 대한 작업 수행을 참조하세요.

Security Hub의 모든 결과는 표준 JSON 형식을 사용합니다. 이를 AWS Security Finding Format(ASFF)이라고 합니다. ASFF에는 문제의 출처, 영향을 받은 리소스와 조사 결과의 현재 상태 등에 관한 세부 정보가 포함됩니다. 자세한 내용은 AWS Security Hub 사용 설명서의 AWS 보안 조사 결과 형식(ASFF)을 참조하세요.

Macie가 게시하는 조사 결과의 유형

Macie 계정에 대해 사용자가 선택한 게시 설정에 따라 Macie는 Security Hub에 생성하는 모든 조사 결과(민감한 데이터 조사 결과 및 정책 조사 결과 모두)를 게시할 수 있습니다. 이 설정과 설정을 변경하는 자세한 내용은 조사 결과에 대한 게시 설정 구성을(를) 참조하세요. 기본적으로 Macie는 신규 및 업데이트된 정책 조사 결과만 Security Hub에 게시합니다. Macie는 Security Hub에 중요한 데이터 조사 결과를 게시하지 않습니다.

민감한 데이터 조사 결과

민감한 데이터 조사 결과를 Security Hub에 게시하도록 Macie를 구성한 경우, Macie는 사용자 계정에 대해 생성한 각 민감한 데이터 조사 결과를 자동으로 게시하고 조사 결과 처리가 완료된 후 즉시 게시합니다. Macie는 억제 규칙에 의해 자동으로 보관되지 않는 모든 민감한 데이터 검색 결과에 대해 이 작업을 수행합니다.

사용자가 조직의 Macie 관리자인 경우, 사용자가 실행한 민감한 데이터 검색 작업에서 얻은 결과와 Macie가 조직을 위해 수행한 민감한 데이터 자동 검색 작업으로 게시가 제한됩니다. 작업을 생성한 계정만 해당 작업이 생성한 민감한 데이터 결과를 게시할 수 있습니다. Macie 관리자 계정만 민감한 데이터 자동 검색을 통해 조직에 제공하는 민감한 데이터 결과를 게시할 수 있습니다.

Macie는 민감한 데이터 조사 결과를 Security Hub에 게시할 때 AWS보안 조사 결과 형식(ASFF) 즉, Security Hub의 모든 조사 결과에 대한 표준 형식을 사용합니다. ASFF에서 `Types` 필드는 조사 결과 유형을 나타냅니다. 이 필드는 Macie의 검색 유형 분류법과 약간 다른 분류법을 사용합니다.

다음 표에는 Macie가 생성할 수 있는 각 유형의 민감한 데이터 조사 결과에 대한 ASFF 검색 유형이 나열되어 있습니다.

Macie 조사 결과 유형.	ASFF 결과 유형
SensitiveData:S3Object/Credentials	Sensitive Data Identifications/Passwords/SensitiveData:S3Object-Credentials
SensitiveData:S3Object/CustomIdentifier	

Macie 조사 결과 유형.	ASFF 결과 유형
	Sensitive Data Identifications/PII/Sensitive Data:S3Object-CustomIdentifier
SensitiveData:S3Object/Financial	Sensitive Data Identifications/Financial/SensitiveData:S3Object-Financial
SensitiveData:S3Object/Multiple	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

정책 조사 결과

정책 조사 결과를 Security Hub에 게시하도록 Macie를 구성한 경우 Macie는 새로 생성한 각 정책 조사 결과를 자동으로 게시하고 조사 결과 처리를 완료한 직후에 게시합니다. Macie는 기존 결과의 후속 발생을 감지하는 경우, Security Hub에서 기존 결과의 후속 발생을 감지하는 경우, 사용자가 계정에 대해 지정한 게시 빈도를 사용하여 Security Hub에 기존 결과의 업데이트를 자동으로 게시합니다. Macie는 억제 규칙에 의해 자동으로 보관되지 않는 모든 정책 결과에 대해 이러한 작업을 수행합니다.

조직의 Macie 관리자인 경우 사용자 계정이 직접 소유한 S3 버킷에 대한 정책 조사 결과만 게시할 수 있습니다. Macie는 조직의 구성원 계정을 위해 생성하거나 업데이트한 정책 결과를 게시하지 않습니다. 이렇게 하면 Security Hub에 조사 결과 데이터가 중복되지 않도록 할 수 있습니다.

민감한 데이터 조사 결과의 경우와 마찬가지로 Security Hub에 신규 및 업데이트된 정책 조사 결과를 게시할 때 Macie는 AWS 보안 조사 결과 형식(ASFF)을 사용합니다. ASFF에서 `Types` 필드는 Macie의 조사 결과 유형 분류법과 약간 다른 분류법을 사용합니다.

다음 표에는 Macie가 생성할 수 있는 각 정책 조사 결과 유형에 대한 ASFF 조사 결과 유형이 나열되어 있습니다. Macie가 2021년 1월 28일 또는 그 이후에 Security Hub에서 정책 조사 결과를 만들거나 업데이트한 경우 Security Hub의 ASFF `Types` 필드에 대한 다음 값 중 하나가 조사 결과에 포함됩니다.

Macie 조사 결과 유형.	ASFF 결과 유형

Macie 조사 결과 유형.	ASFF 결과 유형
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled
Policy:IAMUser/S3BucketEncryptionDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketEncryptionDisabled
Policy:IAMUser/S3BucketPublic	Effects/Data Exposure/Policy:IAMUser-S3BucketPublic
Policy:IAMUser/S3BucketReplicatedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketReplicatedExternally
Policy:IAMUser/S3BucketSharedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedExternally
Policy:IAMUser/S3BucketSharedWithCloudFront	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedWithCloudFront

Macie가 2021년 1월 28일 이전에 정책 조사 결과를 생성했거나 마지막으로 업데이트한 경우, Security Hub의 ASFF `Types` 필드에 대한 다음 값 중 하나가 조사 결과에 포함됩니다.

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

위 목록의 값은 Macie의 검색 유형(type) 필드 값에 직접 매핑됩니다.

> **Note**
>
> Security Hub에서 정책 조사 결과를 검토하고 처리할 때는 다음 예외 사항에 유의하세요.
>
> - 확실히 AWS 리전 Macie는 2021년 1월 25일부터 신규 및 업데이트된 조사 결과에 대해 ASFF 조사 결과 유형을 사용하기 시작했습니다.
> - Macie가 AWS 리전에 있는 ASFF 조사 결과 유형을 사용하기 시작하기 전에 사용자가 Security Hub에서 정책 조사 결과를 적용한 경우, 조사 결과의 ASFF Types 필드 값은 이전 목록에 Macie 조사 결과 유형 중 하나가 됩니다. 이는 위 표의 ASFF 검색 유형 중 하나가 아닐 것입니다. 이는 AWS Security Hub 콘솔이나 BatchUpdateFindings API AWS Security Hub 작업을 사용하여 조치를 취한 정책 조사 결과에 해당됩니다.

조사 결과 게시 지연 시간

Macie는 새 정책 또는 민감한 데이터 조사 결과를 만들면 조사 결과 처리가 완료된 후 즉시 Security Hub에 결과를 게시합니다.

Macie는 기존 정책 조사 결과가 이후에 발생하는 것을 감지하면 기존 Security Hub 조사 결과에 업데이트를 게시합니다. 업데이트 시기는 Macie 계정에 대해 선택한 게시 빈도에 따라 달라집니다. 기본적으로 Macie는 15분마다 업데이트를 게시합니다. 계정 설정을 변경하는 방법 등 자세한 내용은 조사 결과에 대한 게시 설정 구성을(를) 참조하세요.

Security Hub를 사용할 수 없을 때 다시 게시를 시도

Security Hub를 사용할 수 없는 경우 Macie는 Security Hub에서 수신하지 않은 조사 결과 대기열을 생성합니다. 시스템이 복원되면 Macie는 Security Hub에서 조사 결과를 받을 때까지 게시를 다시 시도합니다.

Security Hub에서 기존 결과 업데이트

Macie가 Security Hub에 조사 결과를 게시한 후 Macie는 조사 결과 또는 조사 결과 활동의 추가 발생을 반영하여 조사 결과를 업데이트합니다. Macie는 정책 조사 결과에 대해서만 이 작업을 수행합니다. 민감한 데이터 조사 결과는 정책 조사 결과와는 달리 모두 새로운(고유한) 것으로 취급됩니다.

Macie가 정책 조사 결과에 대한 업데이트를 게시하면 Macie는 조사 결과의 업데이트 날짜(UpdatedAt) 필드 값을 업데이트합니다. 이 값을 사용하여 Macie가 결과를 초래한 잠재적 정책 위반 또는 문제의 후속 발생을 가장 최근에 발견한 시기를 확인할 수 있습니다.

Macie는 해당 필드의 기존 값이 ASFF 조사 결과 유형이 아닌 경우 조사 결과의 유형(Types) 필드 값을 업데이트할 수도 있습니다. 이는 Security Hub에서 그 결과를 바탕으로 조치를 취했는지 여부에 따라 달라집니다. 조사 결과에 따라 조치를 취하지 않은 경우 Macie는 필드 값을 적절한 ASFF 조사 결과 유형으로 변경합니다. AWS Security Hub콘솔이나 API AWS Security Hub 조작BatchUpdateFindings을 사용하여 조사 결과에 따라 조치를 취한 경우 Macie는 필드 값을 변경하지 않습니다.

AWS Security Hub에서 Amazon Macie 조사 결과의 예

Amazon Macie가 조사 결과를 AWS Security Hub에 게시할 때, 그것은 AWS 보안 조사 결과 형식(ASFF)을 사용합니다. Security Hub의 모든 결과의 표준 형식입니다. 다음 예제는 샘플 데이터를 사용하여 Macie가 Security Hub에 다음과 같은 형식으로 게시하는 결과 데이터의 구조와 특성을 보여줍니다.

- 민감한 데이터 조사 결과의 예
- 정책 조사 결과의 예

Security Hub의 민감한 데이터 조사 결과의 예

다음은 Macie가 ASFF를 사용하여 Security Hub에 게시한 민감한 데이터 조사 결과의 예입니다.


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "5be50fce24526e670df77bc00example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types":[
        "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
    ],
    "CreatedAt": "2022-05-11T10:23:49.667Z",
    "UpdatedAt": "2022-05-11T10:23:49.667Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "The S3 object contains personal information.",
```

```
    "Description": "The object contains personal information such as first or last
 names, addresses, or identification numbers.",
    "ProductFields": {
        "JobArn": "arn:aws:macie2:us-east-1:111122223333:classification-
job/698e99c283a255bb2c992feceexample",
        "S3Object.Path": "DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
        "S3Object.Extension": "tsv",
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "OriginType": "SENSITIVE_DATA_DISCOVERY_JOB",
        "S3Object.PublicAccess": "false",
        "S3Object.Size": "14",
        "S3Object.StorageClass": "STANDARD",
        "S3Bucket.allowsUnencryptedObjectUploads": "TRUE",
        "JobId": "698e99c283a255bb2c992feceexample",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/5be50fce24526e670df77bc00example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
            "Type": "AwsS3Bucket",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "Partition": "aws",
            "Region": "us-east-1",
            "Details": {
                "AwsS3Bucket": {
                    "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
                    "OwnerName": "johndoe",
                    "OwnerAccountId": "444455556666",
                    "CreatedAt": "2020-12-30T18:16:25.000Z",
                    "ServerSideEncryptionConfiguration": {
                        "Rules": [
                            {
                                "ApplyServerSideEncryptionByDefault": {
                                    "SSEAlgorithm": "aws:kms",
                                    "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                                }
                            }
                        ]
                    },
                    "PublicAccessBlockConfiguration": {
```

```
                        "BlockPublicAcls": true,
                        "BlockPublicPolicy": true,
                        "IgnorePublicAcls": true,
                        "RestrictPublicBuckets": true
                    }
                }
            }
        },
        {
            "Type": "AwsS3Object",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
            "Partition": "aws",
            "Region": "us-east-1",
            "DataClassification": {
                "DetailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/111122223333/Macie/us-east-1/
                698e99c283a255bb2c992feceexample/111122223333/32b8485d-4f3a-3aa1-be33-
aa3f0example.jsonl.gz",
                "Result":{
                    "MimeType": "text/tsv",
                    "SizeClassified": 14,
                    "AdditionalOccurrences": false,
                    "Status": {
                        "Code": "COMPLETE"
                    },
                    "SensitiveData": [
                        {
                            "Category": "PERSONAL_INFORMATION",
                            "Detections": [
                                {
                                    "Count": 1,
                                    "Type": "USA_SOCIAL_SECURITY_NUMBER",
                                    "Occurrences": {
                                        "Cells": [
                                            {
                                                "Column": 10,
                                                "Row": 1,
                                                "ColumnName": "Other"
                                            }
                                        ]
                                    }
                                }
                            ],
                            "TotalCount": 1
```

```
                        }
                    ],
                    "CustomDataIdentifiers": {
                        "Detections": [
                        ],
                        "TotalCount": 0
                    }
                }
            },
            "Details": {
                "AwsS3Object": {
                    "LastModified": "2022-04-22T18:16:46.000Z",
                    "ETag": "ebe1ca03ee8d006d457444445example",
                    "VersionId": "SlBC72z5hArgexOJifxw_IN57example",
                    "ServerSideEncryption": "aws:kms",
                    "SSEKMSKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                }
            }
        }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
        ]
    },
    "Sample": false,
    "ProcessedAt": "2022-05-11T10:23:49.667Z"
}
```

Security Hub에서의 정책 조사 결과 예시

여기에 Macie가 ASFF에서 Security Hub에 게시한 새로운 정책 조사 결과의 예입니다.

```
{
```

```
    "SchemaVersion": "2018-10-08",
    "Id": "36ca8ba0-caf1-4fee-875c-37760example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-
S3BlockPublicAccessDisabled"
    ],
    "CreatedAt": "2022-04-24T09:27:43.313Z",
    "UpdatedAt": "2022-04-24T09:27:43.313Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "Block Public Access settings are disabled for the S3 bucket",
    "Description": "All Amazon S3 block public access settings are disabled for the
 Amazon S3 bucket. Access to the bucket is
      controlled only by access control lists (ACLs) or bucket policies.",
    "ProductFields": {
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "S3Bucket.allowsUnencryptedObjectUploads": "FALSE",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/36ca8ba0-caf1-4fee-875c-37760example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
        "Type": "AwsS3Bucket",
        "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
        "Partition": "aws",
        "Region": "us-east-1",
        "Tags": {
            "Team": "Recruiting",
            "Division": "HR"
        },
        "Details": {
            "AwsS3Bucket": {
              "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
```

```
              "OwnerName": "johndoe",
              "OwnerAccountId": "444455556666",
              "CreatedAt": "2020-11-25T18:24:38.000Z",
              "ServerSideEncryptionConfiguration": {
                "Rules": [
                    {
                    "ApplyServerSideEncryptionByDefault": {
                        "SSEAlgorithm": "aws:kms",
                        "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                    }
                  }
                ]
              },
              "PublicAccessBlockConfiguration": {
                "BlockPublicAcls": false,
                "BlockPublicPolicy": false,
                "IgnorePublicAcls": false,
                "RestrictPublicBuckets": false
               }
            }
          }
      }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "Software and Configuration Checks/AWS Security Best Practices/
Policy:IAMUser-S3BlockPublicAccessDisabled"
        ]
    },
    "Sample": false
}
```

AWS Security Hub 통합 활성화 및 구성

Amazon Macie와 AWS Security Hub 통합하려면 사용자 전용 Security Hub를 활성화하십시오. AWS 계정 방법을 알아보려면 사용 AWS Security Hub설명서의 Security Hub 활성화를 참조하십시오.

Macie와 Security Hub를 둘 다 활성화하면, 통합이 자동으로 활성화됩니다. 기본적으로 Macie는 신규 및 업데이트된 정책 결과를 Security Hub에 자동으로 게시하기 시작합니다. 통합을 구성하기 위해 추가 단계를 수행할 필요는 없습니다. 통합이 활성화되었을 때 기존 정책 결과가 있는 경우 Macie는 해당 결과를 Security Hub에 게시하지 않습니다. 대신 Macie는 통합이 활성화된 후 생성하거나 업데이트한 정책 결과만 게시합니다.

Macie가 Security Hub에서 정책 조사 결과에 대한 업데이트를 게시하는 빈도를 선택하여 구성을 사용자 정의할 수도 있습니다. 민감한 데이터 결과를 Security Hub에 게시하도록 선택할 수도 있습니다. 자세한 방법은 조사 결과에 대한 게시 설정 구성(을)를 참조하세요.

AWS Security Hub에 대한 조사 결과 게시 중지

AWS Security Hub로의 조사 결과 게시를 중지하려면, Amazon Macie 계정에 대한 게시 설정을 변경할 수 있습니다. 자세한 방법은 조사 결과에 대한 게시 대상 선택(을)를 참조하세요. Security Hub 콘솔 또는 Security Hub API를 사용하여 이 작업을 수행할 수도 있습니다. 그 방법에 대해 알려면, AWS Security Hub 사용 설명서에서 통합(콘솔)에서 조사 결과 흐름 비활성화 및 활성화 또는 통합에서 조사 결과 비활성화(Security Hub API, AWS CLI)를 참조하세요.

Amazon Macie와 AWS 사용자 알림 통합

AWS 사용자 알림은 AWS Management Console에서 AWS 알림을 위한 중앙 위치 역할을 하는 서비스입니다. 여기에는 Amazon CloudWatch 알람, AWS Support 사례 및 다른 AWS 서비스와(과)의 커뮤니케이션과 같은 알림이 포함됩니다. 사용자 알림을 사용하면 특정 유형의 Amazon EventBridge 이벤트에 대한 알림을 수신하기 위한 사용자 지정 규칙과 전송 채널을 구성할 수 있습니다. 전송 채널에는 이메일, AWS Chatbot 채팅 알림 및 AWS Console Mobile Application 푸시 알림이 포함됩니다. AWS 사용자 알림 콘솔에서도 알림을 검토할 수 있습니다. 사용자 알림에 대해 자세히 알아보려면 AWS 사용자 알림 사용 설명서를 참조하세요.

Macie는 AWS 사용자 알림과 통합됩니다. 즉, Macie가 정책 및 민감한 데이터 조사 결과를 위해 EventBridge에 게시하는 이벤트를 알리도록 사용자 알림을 구성할 수 있습니다. 조사 결과 이벤트가 지정한 기준과 일치하는 경우 사용자 알림은 알림을 생성합니다. 알림에는 검색 결과의 유형, 심각도, 영향을 받는 리소스의 이름 등 관련 조사 결과의 주요 세부 정보가 포함됩니다. 사용자 알림은 지정한 하나 이상의 전송 채널에 알림을 보낼 수도 있습니다. 보안 및 규정 준수 워크플로에 맞게 전송 채널을 맞춤 설정할 수 있습니다.

예를 들어, 심각도가 높은 새로운 조사 결과에 대해 특정 유형의 알림을 생성하도록 사용자 알림을 구성할 수 있습니다. AWS Chatbot을(를) 이러한 알림의 전송 채널로 지정할 수도 있습니다. 그런 다음 사용자 알림은 결과에 대한 EventBridge 이벤트를 탐지하고, 결과 데이터를 포함하는 알림을 생성하여 알림을 AWS Chatbot에 보냅니다. 그런 다음 AWS Chatbot은(는) 알림을 Slack 채널 또는 Amazon Chime 채팅방으로 라우팅하여 사고 대응 팀에 알릴 수 있습니다.

주제

AWS 사용자 알림 사용

AWS 사용자 알림을 사용하면, 모니터링하고 알림을 수신하려는 Amazon EventBridge 이벤트 유형을 지정하는 규칙을 생성할 수 있습니다. 규칙은 EventBridge 이벤트가 알림을 생성하기 위해 일치해야 하는 기준을 정의합니다. 규칙에 사용할 하나 이상의 전송 채널을 선택할 수도 있습니다. 전송 채널은 규칙의 기준과 일치하는 이벤트에 대한 알림을 수신할 위치를 지정합니다.

사용자 알림이 규칙 기준과 일치하는 EventBridge 이벤트를 탐지하면 다음과 같은 일반 작업을 수행합니다.

1. 이벤트에서 일부 데이터를 추출합니다.
2. 추출된 데이터가 포함된 알림을 생성합니다.
3. 해당 유형의 이벤트에 대해 지정한 전송 채널에 알림을 보냅니다.

알림의 디자인과 구조는 전송되는 각 전송 채널에 맞게 최적화됩니다.

수신되는 알림의 빈도나 수를 제어하기 위해 규칙에 대한 집계 설정을 구성할 수 있습니다. 이러한 설정을 활성화하면 사용자 알림은 여러 이벤트의 데이터를 단일 알림으로 결합합니다. 이벤트 통합 알림을 빠르고 자주 전송하도록 선택할 수 있는데, 이는 심각도가 높은 조사 결과 이벤트에 유용할 수 있습니다. 또는 알림 수신 빈도를 줄여서 심각도가 낮은 조사 결과 이벤트의 경우에는 이 방법을 사용하는 것이 좋습니다. 이벤트 데이터를 결합하면 AWS 사용자 알림 콘솔을 사용하여 집계된 각 이벤트의 세부 정보를 자세히 검토할 수 있습니다. 여기에서 Amazon Macie 콘솔의 각 관련 조사 결과를 탐색할 수도 있습니다.

Amazon Macie 조사 결과에 대한 AWS 사용자 알림 활성화 및 구성

AWS 사용자 알림에서 Amazon Macie 조사 결과에 대한 알림을 생성할 수 있도록 하려면 사용자 알림에서 Macie에 대한 알림 구성을 생성합니다. 알림 구성은 규칙의 기준을 지정합니다. 또한 규칙 기준과 일치하는 Amazon EventBridge 이벤트에 대한 알림을 모니터링하고 전송하기 위한 전송 채널 및 기타 설정을 지정합니다. 알림 구성 생성에 대한 자세한 내용은 AWS 사용자 알림 사용 설명서의 AWS 사용자 알림 시작하기를 참조하세요.

Macie 조사 결과에 대한 알림 구성을 생성하려면 이벤트 규칙에 대해 다음 옵션을 선택합니다.

- AWS 서비스 이름으로 Macie를 선택합니다.
- 이벤트 유형으로 Macie 조사 결과를 선택합니다.
- 리전의 경우 Macie를 사용하는 조사 결과에 대한 알림을 받으려는 각 AWS 리전를 선택합니다.

이 구성을 사용하면 사용자 알림은 AWS 계정의 EventBridge 이벤트를 모니터링하고 선택한 리전의 모든 Macie 조사 결과 이벤트에 대한 알림을 생성합니다. 이벤트는 다음 기준과 일치합니다.

- `source` equals `aws.macie`
- `detail-type` equals `Macie Finding`

이벤트 규칙의 기본 JSON 패턴은 다음과 같습니다.

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"]
}
```

규칙을 구체화하고 일부 조사 결과에 대해서만 알림을 생성하려면 규칙의 JSON 패턴을 사용자 지정할 수 있습니다. 이렇게 하려면 Macie 조사 결과에 대한 EventBridge 이벤트 스키마에서 파생되는 추가 기준을 지정하십시오.

사용자 지정 JSON 패턴을 사용하는 규칙을 생성하는 경우 Macie 조사 결과에 대한 여러 알림 구성을 만들 수 있습니다. 그런 다음 특정 유형의 조사 결과에 대한 보안 및 규정 준수 워크플로에 맞게 각 구성의 전송 채널 및 기타 설정을 조정할 수 있습니다.

예를 들어, Macie가 Policy:IAMUser/S3BucketPublic 조사사 결과를 생성하거나 업데이트하면 이를 알려주는 규칙을 하나 만들 수 있습니다. 이 경우 규칙의 패턴은 다음과 같을 수 있습니다.

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": ["Policy:IAMUser/S3BucketPublic"]
    }
}
```

또한 Macie가 공개적으로 액세스할 수 있는 S3 버킷에 대해 민감한 데이터 조사 결과를 생성할 경우 이를 알려주는 규칙을 하나 더 만들 수도 있습니다. 이 경우 규칙의 패턴은 다음과 같을 수 있습니다.

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": [ { "prefix": "SensitiveData" } ],
        "resourcesAffected": {
            "effectivePermission": ["PUBLIC"]
        }
    }
}
```

Macie 조사 결과에 대한 알림 구성을 여러 개 만드는 경우 각 구성의 규칙이 고유한지 확인하는 것이 좋습니다. 그렇지 않으면 개별 조사 결과에 대해 중복된 알림을 받을 수 있습니다.

규칙의 이벤트 패턴을 사용자 지정하는 방법에 대해 자세히 알아보려면 AWS 사용자 알림 사용 설명서의 사용자 지정 JSON 이벤트 패턴 사용을 참조하세요.

AWS 사용자 알림 필드를 Amazon Macie 조사 필드에 매핑하기

AWS 사용자 알림은 Amazon Macie 조사 결과에 대한 알림을 생성하면 해당 Amazon EventBridge 이벤트에 있는 필드 하위 집합의 데이터로 알림을 채웁니다. 이러한 필드에는 조사 결과의 유형, 심각도, 영향을 받는 리소스의 이름 등 관련 조사 결과의 주요 세부 정보를 제공합니다.

AWS 사용자 알림 콘솔에서 알림을 검토하면 알림에는 이 필드 하위 집합에 대한 모든 데이터가 포함됩니다. Amazon Macie 콘솔의 관련 조사 결과로 연결되는 링크도 제공합니다. 다른 전송 채널에서 알림을 검토하는 경우 일부 필드에 대한 데이터만 포함되어 있을 수 있습니다. 이는 사용자 알림이 지원하는 각 유형의 전송 채널에 맞게 알림의 디자인과 구조를 조정하기 때문입니다.

다음 표에는 조사 결과 알림에 포함될 수 있는 필드가 나열되어 있습니다. 표의 알림 필드 열은 알림의 필드 이름을 설명 (기울임꼴) 하거나 나타냅니다. 이벤트 필드 찾기 열은 점 표기법을 사용하여 조사 결

과에 대한 EventBridge 이벤트의 해당 JSON 필드 이름을 나타냅니다. 설명 열은 필드에 저장된 데이터를 설명합니다.

알림 필드	조사 결과 이벤트 필드	설명
메시지 헤드라인	`detail.type`	조사 결과 유형입니다. 예: `Policy:IAMUser/S3BucketPublic` 또는 `SensitiveData:S3Object/Financial` .
요약	`detail.title`	조사 결과에 대한 간략한 설명입니다. 예: `The S3 object contains financial information.`
설명	`detail.description`	조사 결과에 대한 전체 설명입니다. 예: `The S3 object contains financial information such as bank account numbers or credit card numbers.`
심각도	`detail.severity.description`	조사 결과의 심각도에 대한 질적 표현: `Low`, `Medium` 또는 `High`.
결과 ID	`detail.id`	조사 결과의 고유 식별자입니다.
생성 완료	`detail.createdAt`	Macie가 조사 결과를 생성한 날짜 및 시간입니다.

알림 필드	조사 결과 이벤트 필드	설명
Updated	`detail.updatedAt`	Macie가 가장 최근에 조사 결과를 업데이트한 날짜 및 시간입니다. 민감한 데이터 조사 결과의 경우 이 값은 생성됨(`detail.createdAt`) 필드의 값과 동일합니다. 모든 민감한 데이터 조사 결과는 새로운 것(고유한 것)으로 간주됩니다.
영향을 받는 S3 버킷	`detail.resourcesAffected.s3Bucket.arn`	영향을 받는 S3 버킷의 Amazon 리소스 이름(ARN)입니다.
영향을 받는 S3 객체	`detail.resourcesAffected.s3Object.path`	영향을 받는 S3 객체의 이름(키) 입니다. 객체를 저장하는 버킷의 이름으로 해당하는 경우 객체의 접두사를 포함합니다. 이 필드는 정책 조사 결과 알림에 포함되지 않습니다.

알림 필드	조사 결과 이벤트 필드	설명

민감한 데이터 감지	`detail.classificationDetails.result.sensitiveData.detections...`
	
	And/Or
	
	`detail.classificationDetails.result.customDataIdentifiers.detections...`
		이는 민감한 데이터 조사 결과를 위해 이벤트의 여러 필드를 결합한 것입니다. 이 필드는 정책 조사 결과 알림에 포함되지 않습니다.
		
		관리형 데이터 식별자가 민감한 데이터를 탐지한 경우 이 필드는 탐지된 민감한 데이터의 범주, 유형 및 발생 횟수(count)를 지정합니다. 예: `PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences .`
		
		사용자 지정 데이터 식별자가 민감한 데이터를 탐지한 경우 이 필드는 사용자 지정 데이터 식별자의 이름과 탐지된 민감한 데이터의 발생 횟수(count)를 지정합니다. 예: `Employee ID 20 occurrences .`
		
		조사 결과 하나가 여러 유형의 민감한 데이터를 보고하는 경우 알림에는 최대 4가지 유형의 데이터가 포함됩니다. 데이터는 먼저 해당하는 사용자 지정 데이터 식별자로 채워진 다음 해당하는 관리 데이터 식별자로 채워집니다.

Amazon Macie 조사 결과에 대한 AWS 사용자 알림 설정 변경

Amazon Macie 조사 결과에 대한 AWS 사용자 알림 설정은 언제든지 변경할 수 있습니다. 이렇게 하려면 사용자 알림에서 알림 구성을 편집합니다. 방법을 알아보려면 AWS 사용자 알림 사용 설명서의 알림 구성 관리를 참조하세요.

Macie 조사 결과에 대한 알림 구성이 여러 개 있는 경우 한 구성의 설정을 변경해도 다른 구성의 설정에는 영향을 주지 않습니다. 전체 또는 일부 구성만 편집할 수 있습니다.

Amazon Macie 조사 결과에 대한 AWS 사용자 알림 비활성화

Amazon Macie의 AWS 사용자 알림 조사 결과에서 알림 생성 및 수신을 중지하려면 사용자 알림에서 알림 구성을 삭제합니다. 방법을 알아보려면 AWS 사용자 알림 사용 설명서의 알림 구성 관리를 참조하세요.

Macie 조사 결과에 대한 알림 구성이 여러 개 있는 경우, 한 구성을 삭제해도 다른 구성에는 영향을 주지 않습니다. 전체 또는 일부 구성만 삭제할 수 있습니다.

Amazon Macie 조사 결과를 위한 Amazon EventBridge 이벤트 스키마

Amazon Macie는 모니터링 또는 이벤트 관리 시스템과 같은 다른 애플리케이션, 서비스 및 시스템과의 통합을 지원하기 위해 Amazon EventBridge에 조사 결과를 이벤트로 자동 게시합니다. EventBridge(전 Amazon CloudWatch Events)는 애플리케이션 및 기타 AWS 서비스의 실시간 데이터 스트림을 AWS Lambda함수, Amazon Simple Notification Service 주제, Amazon Kinesis 스트림과 같은 대상으로 전송하는 서버리스 이벤트 버스 서비스입니다. EventBridge에 대해 자세히 알아보려면 Amazon EventBridge 사용 설명서를 참조하세요.

> **Note**
>
> 현재 CloudWatch Events를 사용하고 있다면 EventBridge와 CloudWatch Event가 동일한 기본 서비스 및 API라는 점에 유의하세요. 그러나 EventBridge에는 서비스형 소프트웨어(SaaS)애플리케이션 및 자체 애플리케이션에서 이벤트를 수신할 수 있는 추가 기능이 포함되어 있습니다. 기본 서비스와 API가 동일하기 때문에 Macie 조사 결과에 대한 이벤트 스키마도 동일합니다.

Macie는 금지 규칙에 따라 자동으로 보관되는 조사 결과를 제외한 모든 새로운 조사 결과와 기존 정책 조사의 후속 결과에 대한 이벤트를 자동으로 게시합니다. 이벤트는 AWS 이벤트에 대한 EventBridge 스키마를 준수하는 JSON 객체입니다. 각 이벤트에는 특정 조사 결과의 JSON 표현이 포함되어 있습니다. 데이터는 EventBridge 이벤트로 구조화되므로 다른 애플리케이션, 서비스, 도구를 사용하여 조사 결과를 더 간편하게 모니터링 및 처리하고 조치를 취할 수 있습니다. Macie가 조사 결과에 대한 이벤트를 게시하는 방법과 시기에 대한 자세한 내용은 조사 결과에 대한 게시 설정 구성 섹션을 참조하세요.

주제

이벤트 스키마

다음 예는 Amazon Macie 조사 결과에 대한 Amazon EventBridge 이벤트의 스키마를 보여줍니다. 조사 결과 이벤트에 포함할 수 있는 필드에 대한 자세한 설명은 Amazon Macie API 참조의 조사 결과 섹션을 참조하세요. 조사 결과 이벤트의 구조 및 필드는 Amazon Macie API의 조사 결과 객체와 밀접하게 매핑됩니다.

```
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "AWS ## ID (string)",
    "time": "event timestamp (string)",
    "region": "AWS ## (string)",
    "resources": [
        <-- ARNs of the resources involved in the event -->
    ],
    "detail": {
        <-- Details of a policy or sensitive data finding -->
    },
    "policyDetails": null, <-- Additional details of a policy finding or null for a
 sensitive data finding -->
    "sample": Boolean,
    "archived": Boolean
}
```

정책 조사 결과를 위한 이벤트 예제

다음 예제에서는 샘플 데이터를 사용하여 정책 조사 결과에 대한 Amazon EventBridge 이벤트의 객체 및 필드 구조 및 특성을 보여줍니다.

이 예제에서 이벤트는 기존 정책 조사 결과가 잇따라 발생했다고 보고합니다. 즉, S3 버킷에 대해 퍼블릭 액세스 차단 설정이 비활성화되었습니다. 다음 필드와 값은 이러한 경우를 판단하는 데 도움이 될 수 있습니다.

- `type` 필드는 `Policy:IAMUser/S3BlockPublicAccessDisabled`로 설정됩니다.
- `createdAt` 및 `updatedAt` 필드는 값이 다릅니다. 이는 이벤트가 기존 정책 조사 결과가 이후에 발생했음을 보고하는 지표 중 하나입니다. 이벤트에서 새로운 조사 결과가 보고한 경우 이러한 필드의 값은 동일합니다.
- `count` 필드는 2로 설정되며, 이는 이 조사 결과가 두 번째로 발생했음을 나타냅니다.
- `category` 필드는 `POLICY`로 설정됩니다.
- `classificationDetails` 필드 값은 `null`인데, 이를 통해 정책 조사 결과에 대한 이 이벤트를 민감한 데이터 조사 결과에 대한 이벤트와 구별할 수 있습니다. 민감한 데이터 검색 결과의 경우, 이 값은 민감한 데이터가 발견된 방법과 유형에 대한 정보를 제공하는 객체 및 필드 세트입니다.

또한 `sample` 필드 값은 `true`임에 유의합니다. 이 값은 이 이벤트가 설명서에서 사용하기 위한 예제 이벤트라는 점을 강조합니다.

```
{
    "version": "0",
    "id": "0948ba87-d3b8-c6d4-f2da-732a1example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2021-04-30T23:12:15Z",
    "region":"us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "64b917aa-3843-014c-91d8-937ffexample",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "Policy:IAMUser/S3BlockPublicAccessDisabled",
        "title": "Block public access settings are disabled for the S3 bucket",
```

```
        "description": "All bucket-level block public access settings were disabled for
 the S3 bucket. Access to the bucket is controlled by account-level block public access
 settings, access control lists (ACLs), and the bucket's bucket policy.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2021-04-29T15:46:02Z",
        "updatedAt": "2021-04-30T23:12:15Z",
        "count": 2,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
                "name": "DOC-EXAMPLE-BUCKET1",
                "createdAt": "2020-04-03T20:46:56.000Z",
                "owner":{
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags": [
                    {
                        "key": "Division",
                        "value": "HR"
                    },
                    {
                        "key": "Team",
                        "value": "Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy": {
                                "allowsPublicReadAccess": false,
```

```
                                "allowsPublicWriteAccess": false
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "FALSE"
            },
            "s3Object": null
        },
        "category": "POLICY",
        "classificationDetails": null,
        "policyDetails": {
            "action": {
                "actionType": "AWS_API_CALL",
                "apiCallDetails": {
                    "api": "PutBucketPublicAccessBlock",
                    "apiServiceName": "s3.amazonaws.com",
                    "firstSeen": "2021-04-29T15:46:02.401Z",
                    "lastSeen": "2021-04-30T23:12:15.401Z"
                }
            },
            "actor": {
                "userIdentity": {
                    "type": "AssumedRole",
                    "assumedRole": {
                        "principalId": "AROA1234567890EXAMPLE:AssumedRoleSessionName",
                        "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
                        "accountId": "111122223333",
```

```
                        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                        "sessionContext": {
                            "attributes": {
                                "mfaAuthenticated": false,
                                "creationDate": "2021-04-29T10:25:43.511Z"
                            },
                            "sessionIssuer": {
                                "type": "Role",
                                "principalId": "AROA1234567890EXAMPLE",
                                "arn": "arn:aws:iam::123456789012:role/
RoleToBeAssumed",
                                "accountId": "123456789012",
                                "userName": "RoleToBeAssumed"
                            }
                        }
                    },
                    "root": null,
                    "iamUser": null,
                    "federatedUser": null,
                    "awsAccount": null,
                    "awsService": null
                },
                "ipAddressDetails":{
                    "ipAddressV4": "192.0.2.0",
                    "ipOwner": {
                        "asn": "-1",
                        "asnOrg": "ExampleFindingASNOrg",
                        "isp": "ExampleFindingISP",
                        "org": "ExampleFindingORG"
                    },
                    "ipCountry": {
                        "code": "US",
                        "name": "United States"
                    },
                    "ipCity": {
                        "name": "Ashburn"
                    },
                    "ipGeoLocation": {
                        "lat": 39.0481,
                        "lon": -77.4728
                    }
                },
                "domainDetails": null
            }
```

```
        },
        "sample": true,
        "archived": false
    }
}
```

민감한 데이터 조사 결과에 대한 이벤트 예제

다음 예제에서는 샘플 데이터를 사용하여 민감한 데이터 조사 결과에 대한 Amazon EventBridge 이벤트의 객체 및 필드 구조 및 특성을 보여줍니다.

이 예제에서 이벤트는 새로운 민감한 데이터 발견을 보고합니다. Amazon Macie는 S3 객체에서 하나 이상의 민감한 데이터 범주를 발견했습니다. 다음 필드와 값은 이러한 경우를 판단하는 데 도움이 될 수 있습니다.

- `type` 필드는 `SensitiveData:S3Object/Multiple`로 설정됩니다.
- `createdAt` 및 `updatedAt` 필드의 값은 동일합니다. 정책 조사 결과와 달리 민감한 데이터 조사 결과의 경우에는 항상 그렇습니다. 모든 민감한 데이터 조사 결과는 새로운 것으로 간주됩니다.
- `count` 필드가 `1`로 설정되면 이는 새로운 조사 결과임을 나타냅니다. 정책 조사 결과와 달리 민감한 데이터 조사 결과의 경우에는 항상 그렇습니다. 모든 민감한 데이터 조사 결과는 고유한 것(새로운 것)으로 간주됩니다.
- `category` 필드는 `CLASSIFICATION`로 설정됩니다.
- `policyDetails` 필드 값은 `null`인데, 이를 통해 민감한 데이터 검색 결과에 대한 이 이벤트를 정책 결과에 대한 이벤트와 구별할 수 있습니다. 정책 조사 결과의 경우 이 값은 S3 버킷의 보안 또는 개인 정보 보호 관련 잠재적 정책 위반 또는 문제에 대한 정보를 제공하는 객체 및 필드 세트입니다.

또한 `sample` 필드 값은 `true`임에 유의합니다. 이 값은 이 이벤트가 설명서에서 사용하기 위한 예제 이벤트라는 점을 강조합니다.

```
{
    "version": "0",
    "id": "14ddd0b1-7c90-b9e3-8a68-6a408example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2022-04-20T08:19:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
```

```
        "schemaVersion": "1.0",
        "id": "4ed45d06-c9b9-4506-ab7f-18a57example",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "SensitiveData:S3Object/Multiple",
        "title": "The S3 object contains multiple categories of sensitive data",
        "description": "The S3 object contains more than one category of sensitive
 data.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2022-04-20T18:19:10Z",
        "updatedAt": "2022-04-20T18:19:10Z",
        "count": 1,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "name": "DOC-EXAMPLE-BUCKET2",
                "createdAt": "2020-05-15T20:46:56.000Z",
                "owner": {
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
```

```
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy":{
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "TRUE"
            },
            "s3Object":{
                "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "key": "2022 Sourcing.csv",
                "path": "DOC-EXAMPLE-BUCKET2/2022 Sourcing.csv",
                "extension": "csv",
                "lastModified": "2022-04-19T22:08:25.000Z",
                "versionId": "",
                "serverSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "size": 4750,
                "storageClass": "STANDARD",
                "tags":[
                    {
```

```
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "publicAccess": false,
                "etag": "6bb7fd4fa9d36d6b8fb8882caexample"
            }
        },
        "category": "CLASSIFICATION",
        "classificationDetails": {
            "jobArn": "arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample",
            "jobId": "3ce05dbb7ec5505def334104bexample",
            "result": {
                "status": {
                    "code": "COMPLETE",
                    "reason": null
                },
                "sizeClassified": 4750,
                "mimeType": "text/csv",
                "additionalOccurrences": true,
                "sensitiveData": [
                    {
                        "category": "PERSONAL_INFORMATION",
                        "totalCount": 65,
                        "detections": [
                            {
                                "type": "USA_SOCIAL_SECURITY_NUMBER",
                                "count": 30,
                                "occurrences": {
                                    "lineRanges": null,
                                    "offsetRanges": null,
                                    "pages": null,
                                    "records": null,
                                    "cells": [
                                        {
                                            "row": 2,
                                            "column": 1,
                                            "columnName": "SSN",
                                            "cellReference": null
```

```
                                    },
                                    {
                                        "row": 3,
                                        "column": 1,
                                        "columnName": "SSN",
                                        "cellReference": null
                                    },
                                    {
                                        "row": 4,
                                        "column": 1,
                                        "columnName": "SSN",
                                        "cellReference": null
                                    }
                                ]
                            }
                        },
                        {
                            "type": "NAME",
                            "count": 35,
                            "occurrences": {
                                "lineRanges": null,
                                "offsetRanges": null,
                                "pages": null,
                                "records": null,
                                "cells": [
                                    {
                                        "row": 2,
                                        "column": 3,
                                        "columnName": "Name",
                                        "cellReference": null
                                    },
                                    {
                                        "row": 3,
                                        "column": 3,
                                        "columnName": "Name",
                                        "cellReference": null
                                    }
                                ]
                            }
                        }
                    ]
                },
                {
                    "category": "FINANCIAL_INFORMATION",
```

```
                        "totalCount": 30,
                        "detections": [
                            {
                                "type": "CREDIT_CARD_NUMBER",
                                "count": 30,
                                "occurrences": {
                                    "lineRanges": null,
                                    "offsetRanges": null,
                                    "pages": null,
                                    "records": null,
                                    "cells": [
                                        {
                                            "row": 2,
                                            "column": 14,
                                            "columnName": "CCN",
                                            "cellReference": null
                                        },
                                        {
                                            "row": 3,
                                            "column": 14,
                                            "columnName": "CCN",
                                            "cellReference": null
                                        }
                                    ]
                                }
                            }
                        ]
                    }
                ],
                "customDataIdentifiers": {
                    "totalCount": 0,
                    "detections": []
                }
            },
            "detailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/123456789012/Macie/us-east-1/3ce05dbb7ec5505def334104bexample/
d48bf16d-0deb-3e49-9d8c-d407cexample.jsonl.gz",
            "originType": "SENSITIVE_DATA_DISCOVERY_JOB"
        },
        "policyDetails": null,
        "sample": true,
        "archived": false
    }
```

```
}
```

Amazon Macie 비용 예측 및 모니터링

Amazon Macie를 사용하는 데 드는 비용을 예측하고 모니터링할 수 있도록 Macie는 사용자 계정의 예상 사용 비용을 계산하여 제공합니다. 이 데이터를 사용하여 서비스 사용 또는 계정 할당량 조정 여부를 결정할 수 있습니다. 현재 Macie의 30일 무료 평가판에 참여 중인 경우 이 데이터를 사용하여 무료 평가판 종료 후 Macie를 사용하는 데 드는 비용을 추정할 수 있습니다. 또한 평가판 상태를 확인할 수도 있습니다.

Amazon Macie 콘솔에서 예상 사용 비용을 검토하고 Amazon Macie API를 사용하여 프로그래밍 방식으로 이용할 수 있습니다. 조직의 Macie 관리자인 경우 조직의 집계 데이터와 조직 내 계정에 대한 데이터 분석을 모두 검토하고 액세스할 수 있습니다.

Macie에서 제공하는 예상 사용 비용 외에도 를 사용하여 AWS Billing and Cost Management실제 비용을 검토하고 모니터링할 수 있습니다. AWS Billing and Cost Management 계정 또는 조직의 비용을 추적 및 분석하고 예산을 관리하는 데 도움이 되도록 설계된 기능을 제공합니다. AWS 서비스또한 과거 데이터를 기반으로 사용자가 사용 비용을 예측하는 데 도움이 되는 기능을 제공합니다. 자세한 내용은 AWS Billing 사용 설명서를 참조하세요.

주제

- Amazon Macie의 예상 사용 비용 계산 방법 이해
- Amazon Macie의 예상 사용 비용 검토
- Amazon Macie 무료 평가판에 참여하기

Amazon Macie의 예상 사용 비용 계산 방법 이해

Amazon Macie 가격 책정은 다음 기준을 기반으로 합니다.

예방적 제어 모니터링

이러한 비용은 Amazon Simple Storage Service (Amazon S3) 범용 버킷의 인벤토리를 유지 관리하고 보안 및 액세스 제어를 위해 버킷을 평가 및 모니터링하는 데서 발생합니다. 자세한 정보는 Macie가 Amazon S3 데이터 보안을 모니터링하는 방법을 참조하세요.

Macie가 계정에 대해 모니터링하는 S3 범용 버킷의 총 개수를 기준으로 요금이 부과됩니다. 요금은 일별로 비례 할당으로 계산됩니다.

민감한 데이터 자동 검색을 위한 객체 모니터링

이러한 비용은 민감한 데이터 자동 검색으로 분석할 수 있는 S3 객체를 식별하기 위해 S3 버킷 인벤토리를 모니터링하고 평가하는 데서 발생합니다. 자세한 정보는 민감한 데이터 자동 검색의 작동 방식을 참조하세요.

Macie가 사용자 계정에서 모니터링하는 범용 버킷의 총 S3 객체 수를 기준으로 요금이 부과됩니다. 요금은 일별로 비례 할당으로 계산됩니다.

민감한 데이터 검색 작업 및 민감한 데이터 자동 검색을 통한 객체 분석

이러한 비용은 S3 객체를 분석하고 Macie가 객체에서 발견한 민감한 데이터를 보고할 때 발생합니다. 여기에는 민감한 데이터 검색 작업과 민감한 데이터 자동 검색을 통한 분석 및 보고가 포함됩니다. 자세한 정보는 민감한 데이터 검색을 참조하세요.

Macie가 S3 객체에서 분석한 압축되지 않은 데이터의 양을 기준으로 요금이 부과됩니다. 지원되지 않는 Amazon S3 스토리지 클래스 사용, 지원되지 않는 파일 또는 스토리지 형식 사용 또는 권한 설정과 같은 이유로 Macie가 분석할 수 없는 객체에는 요금이 부과되지 않습니다. 또한 이러한 비용은 작업이나 민감한 데이터 자동 검색을 통해 생성된 민감한 데이터 검색의 수에 따라 달라지지 않습니다.

민감한 데이터 자동 검색 비용을 관리하기 위해 개별 S3 버킷을 분석에서 제외할 수 있습니다. 예를 들어 조직의 보안 및 규정 준수 요구 사항을 충족하는 것으로 알려진 버킷을 제외할 수 있습니다. 계정이 여러 Macie 계정을 중앙에서 관리하는 조직의 일부인 경우 추가 옵션은 조직의 개별 계정에 대해 자동 민감한 데이터 검색을 선택적으로 활성화하거나 비활성화하는 것입니다. 자세한 정보는 민감한 데이터 자동 검색 구성을 참조하세요.

민감한 데이터 검색 작업에 드는 비용은 사용자 계정의 월간 민감 데이터 검색 할당량에 따라 제한됩니다. (기본 할당량은 5TB의 데이터입니다.) 작업이 실행 중이고 적합한 개체에 대한 분석 결과가 이 할당량에 도달하면 Macie는 다음 달이 시작될 때까지 작업을 자동으로 일시 중지하고 계정에 대한 월별 할당량이 재설정되거나 계정의 할당량을 늘립니다.

조직의 Macie 관리자인 경우 데이터를 분석하는 각 계정의 월별 중요 데이터 검색 할당량에 따라 민감한 데이터 검색 작업에 드는 비용이 제한됩니다. 구성원 계정 할당량은 한 달 동안 작업과 구성원 계정의 작업에서 계정에 대해 분석할 수 있는 최대 데이터 양을 정의합니다. 작업이 실행 중이고 적합한 개체에 대한 분석 결과가 멤버 계정에 대한 이 할당량에 도달하면 Macie는 계정이 소유한 버킷의 개체 분석을 중단합니다. Macie는 할당량을 충족하지 못한 다른 모든 계정의 객체 분석을 마치면 자동으로 작업을 일시 중지합니다. 일회성 작업인 경우 Macie는 다음 달이 시작되거나 영향을 받는 모든 계정의 할당량이 늘어나는 시점(둘 중 먼저 발생하는 날짜)에 자동으로 작업을 재개합니다. 정기 작업인 경우 Macie는 다음 실행이 시작되거나 다음 달이 시작될 때(둘 중 먼저 발생하는

날짜) 작업을 자동으로 재개합니다. 다음 달이 시작되기 전에 예약된 실행이 시작되거나 영향을 받는 계정의 할당량이 증가하면 Macie는 계정이 소유한 버킷의 객체를 분석하지 않습니다.

> **Tip**
>
> 민감한 데이터 검색 비용을 관리하거나 줄이는 방법에 대한 유용한 팁은 보안 블로그AWS의 Amazon Macie를 사용하여 민감한 데이터를 검색하는 데 드는 비용을 줄이는 방법 블로그 게시물을 참조하세요.

사용 비용에 대한 자세한 내용 및 예는 Amazon Macie 가격 책정을 참조하세요.

Macie를 사용하여 예상 사용 비용을 검토할 때는 예상 비용이 어떻게 계산되는지 이해하는 것이 중요합니다. 다음을 고려하세요.

- 예상치는 미국 달러로 표시되며 현재 AWS 리전 에만 해당됩니다. 여러 리전에서 Macie를 사용하는 경우 Macie를 사용하는 모든 리전의 데이터가 집계되지는 않습니다.
- 콘솔에서는 이번 달 누계를 기준으로 예상치가 표시됩니다. Amazon Macie API를 사용하여 프로그래밍 방식으로 데이터를 쿼리하는 경우 예상치에 포함되는 시간 범위를 선택할 수 있습니다. 이는 이전 30일의 롤링 시간 범위 또는 현재 월별 누계일 수 있습니다.
- 예상치에는 계정에 적용될 수 있는 모든 할인이 반영되어 있지는 않습니다. Amazon Macie 요금 책정에 설명된 대로 리전별 대량 구매 요금 계층에서 파생되는 할인은 예외입니다. 계정에 이러한 유형의 할인이 적용되는 경우 예상치에는 해당 할인이 반영됩니다.
- 사용자가 조직의 Macie 관리자인 경우 예상치에는 조직의 총 사용량 할인이 반영되지 않습니다. 이러한 할인에 대한 자세한 내용은 AWS Billing 사용 설명서의 대량 구매 할인을 참조하세요.
- 예방적 통제 모니터링의 경우 예상치는 해당 시간 범위의 일일 평균 비용을 기반으로 합니다. 비용은 일별로 비례 배분됩니다.
- 민감한 데이터 자동 검색의 경우 전체 예상치는 객체 모니터링의 일일 평균 비용(일별 비례 배분)과 Macie가 해당 기간 동안 지금까지 분석한 압축되지 않은 데이터의 양을 기반으로 합니다. 조직의 Macie 관리자로서 구성원 계정에 대한 민감한 데이터 자동 검색을 활성화한 경우 해당 활동의 예상 비용이 해당하는 각 구성원 계정의 추정치에 포함됩니다.
- 민감한 데이터 검색 작업의 경우 해당 기간 동안 작업에서 지금까지 분석한 압축되지 않은 데이터의 양을 기준으로 예상치가 책정됩니다. 조직의 Macie 관리자로서 회원 계정의 데이터를 분석하는 작업을 수행하는 경우 해당 작업의 예상 비용이 각 해당 구성원 계정의 추정치에 포함됩니다.

- 계정이 조직의 구성원 계정이고 Macie 관리자가 민감한 데이터 자동 검색을 수행하거나 민감한 데이터 검색 작업을 실행하여 데이터를 분석하는 경우, 해당 활동의 예상 비용이 계정 추정치에 포함됩니다.
- 예상치에는 특정 Macie 기능과 AWS 서비스 함께 다른 기능을 사용할 때 발생하는 비용은 포함되지 않습니다. 예를 들어, 민감한 데이터가 있는지 검사하려는 S3 객체의 암호를 AWS KMS keys 해독하기 위해 Customer Managed 명령을 사용하는 경우를 예로 들 수 있습니다.

또한 Macie는 민감한 데이터 검색 작업과 민감한 데이터 자동 검색을 통해 S3 객체를 분석할 수 있는 월별 프리 티어를 제공합니다. 매달 최대 1GB의 데이터를 분석하여 S3 객체에서 민감한 데이터를 발견하고 보고하는 데 드는 비용은 없습니다. 한 달에 1GB가 넘는 데이터를 분석하면 처음 1GB의 데이터를 사용한 이후에 민감한 데이터 검색 요금이 계정에 누적되기 시작합니다. 지정된 달에 분석된 데이터가 1GB 미만이면 다음 달로 이월되지 않습니다. 계정이 통합 결제를 사용하는 조직의 일부인 경우 무료 등급은 조직에 대해 분석된 데이터 양을 합산하여 적용됩니다. 즉, 조직의 모든 계정에 대해 매월 최대 1GB의 데이터를 분석하는 데 드는 비용은 없습니다.

Amazon Macie의 예상 사용 비용 검토

Amazon Macie의 현재 예상 사용 비용을 검토하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 콘솔과 API 모두 Macie 요금 기준에 대한 예상 비용을 제공합니다. 현재 30일 무료 평가판에 참여 중인 경우 이 데이터를 사용하여 무료 평가판 종료 후 Macie 사용 비용을 추정할 수 있습니다. Macie 가격 기준 및 고려 사항에 대한 자세한 내용은 예상 사용 비용 계산 방법의 이해을 참조하세요. 사용 비용에 대한 자세한 내용 및 예는 Amazon Macie 가격 책정을 참조하세요.

Macie의 경우 예상 사용 비용은 미국 달러로 보고되며 현재 AWS 리전에만 적용됩니다. 데이터 검토를 위해 콘솔을 사용할 경우, 비용 추산은 현재 캘린더 월부터 현재의 날(포함)까지 누계입니다. Amazon Macie API를 사용하여 프로그래밍 방식으로 데이터를 쿼리하는 경우, 이전 30일의 롤링 시간 범위 또는 현재 월별 누계 중에서 예상치에 대한 포함 시간 범위를 지정할 수 있습니다.

주제

- Amazon Macie 콘솔의 예상 사용 비용 검토
- Amazon Macie API를 사용하여 예상 사용 비용 쿼리

Amazon Macie 콘솔의 예상 사용 비용 검토

Amazon Macie 콘솔에서는 예상 비용이 다음과 같이 구성되어 있습니다.

- 예방적 제어 모니터링 — Amazon Simple Storage Service (Amazon S3) 범용 버킷의 인벤토리를 유지 관리하고 보안 및 액세스 제어를 위해 버킷을 평가 및 모니터링하는 데 드는 예상 비용입니다.
- 민감한 데이터 검색 작업 - 사용자가 실행한 민감한 데이터 검색 작업의 예상 비용입니다.
- 민감한 데이터 자동 검색 - 민감한 데이터 자동 검색을 수행하는 데 드는 예상 비용입니다. 여기에는 분석에 적합한 S3 객체를 식별하기 위한 S3 버킷 인벤토리 모니터링 및 평가가 포함됩니다. 또한 적격 객체 분석, 민감한 데이터 통계, 결과 및 기타 유형의 결과 보고도 포함됩니다. 이 추정치를 검토하려면 계정이 조직의 Macie 관리자 계정이거나 독립형 Macie 계정이어야 합니다.

다음 단계에 따라 Amazon Macie 콘솔을 사용하여 예상 사용 비용을 검토하세요.

콘솔에서 예상 사용 비용을 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 예상 비용을 검토하려는 지역을 선택합니다.
3. 탐색 창에서 사용량을 선택합니다.

독립 실행형 Macie 계정을 가지고 있거나 계정이 조직의 구성원 계정인 경우 사용 페이지에 계정의 예상 사용 비용 내역이 표시됩니다.

조직의 Macie 관리자인 경우 사용 페이지에 조직의 계정이 나열됩니다. 테이블에서

- 서비스 할당량 - 계정이 소유한 버킷의 S3 객체를 분석하기 위해 민감한 데이터 검색 작업을 실행하기 위한 현재 월간 할당량입니다.
- 무료 평가판 - 이 필드는 계정이 현재 예방적 제어 모니터링 또는 자동화된 민감한 데이터 검색을 위한 무료 평가판에 참여하고 있는지 여부를 나타냅니다. 계정에 대한 해당 무료 평가판이 종료된 경우 무료 평가판 필드는 비어 있습니다.
- 합계 — 계정당 총 예상 비용입니다.

예상 비용 섹션에는 조직의 총 예상 비용과 해당 비용의 내역이 표시됩니다. 조직의 특정 계정에 대한 추정 비용의 분석 내용을 검토하려면 표에서 해당 계정을 선택합니다. 그러면 추정 비용 섹션에 이 내역이 표시됩니다. 다른 계정의 이 데이터를 표시하려면 표에서 계정을 선택하세요. 선택을 지우려면, 계정 ID 옆에 있는 X를 선택합니다.

Amazon Macie API를 사용하여 예상 사용 비용 쿼리

예상 사용 비용을 프로그래밍 방식으로 쿼리하려면 Amazon Macie API의 다음 작업을 사용할 수 있습니다.

- GetUsageTotals - 이 작업을 수행하면 계정의 총 예상 사용 비용이 사용량 지표별로 그룹화되어 반환됩니다. 조직의 Macie 관리자인 경우 이 작업을 수행하면 조직의 모든 계정에 대해 집계된 예상 비용이 반환됩니다. 이 작업에 대해 자세히 알아보려면 Amazon Macie API 참조의 총 사용량을 참조하세요.
- GetUsageStatistics - 이 작업은 계정에 대한 사용 통계 및 관련 데이터를 계정별로 그룹화한 다음 사용량 지표별로 그룹화하여 반환합니다. 데이터에는 총 예상 사용 비용과 현재 계정 할당량이 포함됩니다. 해당하는 경우 Macie와 민감한 데이터 자동 검색에 대한 30일 무료 평가판이 시작된 시기도 표시됩니다. 사용자가 조직의 Macie 관리자인 경우, 이 작업을 수행하면 조직의 모든 계정에 대해 데이터 내역이 반환됩니다. 쿼리 결과를 정렬하고 필터링하여 쿼리를 사용자 지정할 수 있습니다. 이 작업에 대해 자세히 알아보려면 Amazon Macie API 참조의 사용 통계를 참조하세요.

두 작업 중 하나를 사용하는 경우 데이터에 대한 포함 시간 범위를 선택적으로 지정할 수 있습니다. 이 시간 범위는 이전 30일의 롤링 시간 범위(PAST_30_DAYS) 또는 현재 월별 누계(MONTH_TO_DATE) 일 수 있습니다. 시간 범위를 지정하지 않으면, Macie 에서는 이전 30일 동안의 데이터를 반환합니다.

다음 예제는(AWS Command Line InterfaceAWS CLI)를 사용하여 예상 사용 비용 및 통계를 쿼리하는 방법을 보여줍니다. 최신 버전의 다른 AWS 명령줄 도구 또는 AWS SDK를 사용하거나 Macie에 직접 HTTPS 요청을 보내 데이터를 쿼리할 수도 있습니다. AWS 도구 및 SDK에 대한 자세한 내용은 빌드할 도구를 참조하십시오. AWS

예

- 예 1: 총 예상 사용 비용 쿼리
- 예 2: 사용 통계 쿼리

예 1: 총 예상 사용 비용 쿼리

를 사용하여 총 예상 사용 비용을 쿼리하려면 get-usage-totals명령어를 실행하고 선택적으로 데이터의 시간 범위를 지정하십시오. AWS CLI예:

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

*MONTH_TO_DATE*Where는 현재 달력 월 누계를 데이터의 시간 범위로 지정합니다.

이 명령이 성공적으로 실행되면 다음과 비슷한 출력이 표시됩니다.

```
{
    "timeRange": "MONTH_TO_DATE",
    "usageTotals": [
        {
            "currency": "USD",
            "estimatedCost": "153.45",
            "type": "SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "65.18",
            "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "1.51",
            "type": "DATA_INVENTORY_EVALUATION"
        },
        {
            "currency": "USD",
            "estimatedCost": "0.98",
            "type": "AUTOMATED_OBJECT_MONITORING"
        }
    ]
}
```

어디에`estimatedCost` 관련 사용량 지표(`type`)의 총 예상 사용 비용이 있습니까?

- `SENSITIVE_DATA_DISCOVERY`, 민감한 데이터 검색 작업이 있는 S3 객체를 분석할 수 있습니다.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, 민감한 데이터 자동 검색을 통해 S3 객체를 분석할 수 있습니다.
- `DATA_INVENTORY_EVALUATION`, 보안 및 액세스 제어를 위한 S3 범용 버킷을 모니터링하고 평가하는 데 사용됩니다.
- `AUTOMATED_OBJECT_MONITORING`, 민감한 데이터 자동 검색을 통해 분석할 수 있는 S3 객체를 식별하기 위해 S3 버킷 인벤토리를 평가 및 모니터링하는 데 사용됩니다.

예 2: 사용 통계 쿼리

를 사용하여 사용 통계를 쿼리하려면 get-usage-statistics명령을 실행합니다. AWS CLI선택적으로 쿼리 결과의 정렬, 필터링 및 시간 범위를 지정할 수 있습니다. 다음 예에서는 지난 30일 동안의 Macie 관리자 계정 사용 통계를 검색합니다. 결과는 ID를 기준으로 오름차순으로 AWS 계정 정렬됩니다.

Linux, macOS 또는 Unix의 경우, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws macie2 get-usage-statistics \
--sort-by '{"key":"accountId","orderBy":"ASC"}' \
--time-range PAST_30_DAYS
```

Microsoft Windows의 경우 캐럿(^) 줄 연속 문자를 사용하여 가독성을 개선합니다.

```
C:\> aws macie2 get-usage-statistics ^
--sort-by={\"key\":\"accountId\",\"orderBy\":\"ASC\"} ^
--time-range PAST_30_DAYS
```

위치:

- *accountId*는 결과를 정렬하는 데 사용할 필드를 지정합니다.
- *ASC*는 지정된 필드의 값(*accountId*)을 기준으로 결과에 적용할 정렬 순서입니다.
- *PAST_30_DAYS*는 이전 30일을 데이터의 시간 범위로 지정합니다.

이 명령이 성공적으로 실행되면 Macie는 `records` 배열을 반환합니다. 배열에는 쿼리 결과에 포함된 각 계정의 객체가 포함됩니다. 예:


```
{
    "records": [
        {
            "accountId": "111122223333",
            "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-20T12:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.51",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
```

```
                    "currency": "USD",
                    "estimatedCost": "65.18",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "153.45",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "0.98",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        },
        {
            "accountId": "444455556666",
            "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-18T16:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.58",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "63.13",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "145.12",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
```

```
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "1.02",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        }
    ],
    "timeRange": "PAST_30_DAYS"
}
```

어디에 `estimatedCost` 계정의 관련 사용량 지표(`type`)에 대한 총 예상 사용 비용이 있습니까?

- `DATA_INVENTORY_EVALUATION`, 보안 및 액세스 제어를 위한 S3 범용 버킷을 모니터링하고 평가하는 데 사용됩니다.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, 민감한 데이터 자동 검색을 통해 S3 객체를 분석할 수 있습니다.
- `SENSITIVE_DATA_DISCOVERY`, 민감한 데이터 검색 작업이 있는 S3 객체를 분석할 수 있습니다.
- `AUTOMATED_OBJECT_MONITORING`, 계정의 S3 버킷 인벤토리를 평가 및 모니터링하여 민감한 데이터 자동 검색을 통해 분석할 수 있는 S3 객체를 식별하는 데 사용됩니다.

Amazon Macie 무료 평가판에 참여하기

Amazon Macie를 처음 활성화하면 Macie의 30일 무료 평가판에 자동으로 AWS 계정 등록됩니다. 여기에는 조직의 개인 회원 계정이 포함됩니다. AWS Organizations

무료 평가판 기간 동안에는 다음과 같은 용도에만 AWS 리전 Macie를 사용할 경우 요금이 부과되지 않습니다.

- 예방적 제어 모니터링 수행 — 여기에는 리전에서 Amazon Simple Storage Service (Amazon S3) 범용 버킷의 인벤토리를 생성하고 유지 관리하는 작업이 포함됩니다. 또한 보안 및 액세스 제어를 위한 버킷의 평가 및 모니터링도 포함됩니다.

  자세한 정보는 Macie가 Amazon S3 데이터 보안을 모니터링하는 방법을 참조하세요.
- 민감한 데이터 자동 검색 수행 - 여기에는 해당 리전의 S3 버킷 인벤토리를 모니터링하고 평가하여 분석에 적합한 S3 객체를 식별하는 것이 포함됩니다. 또한 적격 객체 분석, 민감한 데이터 통계, 결과 및 기타 유형의 결과 보고도 포함됩니다. 이 기능을 구성하고 관리하려면 계정이 조직의 Macie 관리

자 계정이거나 독립형 Macie 계정이어야 합니다. 조직의 Macie 관리자인 경우 이 기능을 사용하여 구성원 계정이 소유한 S3 버킷의 객체를 분석할 수 있습니다.

자세한 정보는 민감한 데이터 자동 검색의 작동 방식을 참조하세요.

현재 Macie를 사용할 수 있는 모든 리전 목록은 AWS 일반 참조의 Amazon Macie 및 엔드포인트 및 할당량을 참조하세요.

무료 평가판은 30일 연속으로 실행됩니다. 시작한 후에는 일시 중지할 수 없습니다. 무료 평가판이 종료되면 예방적 제어 모니터링 수행에 대한 요금이 부과되기 시작합니다. 민감한 데이터 자동 검색을 수행하는 경우에도 요금이 부과되기 시작합니다. 조직의 Macie 관리자인 경우 조직의 각 계정에 해당하는 만큼 요금이 부과됩니다. Macie를 사용하여 조직 내 개별 계정의 예상 사용 비용 내역을 검토할 수 있습니다.

> **참고**
>
> 무료 평가판 기간 중에는 특정 Macie 기능과 함께 사용하는 다른 AWS 서비스 기능에 대해 요금이 부과될 수 있습니다. 예를 들어, 민감한 데이터가 있는지 검사하려는 S3 객체의 암호를 AWS KMS keys 해독하는 고객 관리형 기능을 사용하는 경우 요금이 부과될 수 있습니다.
> 무료 평가판에는 민감한 데이터 검색 작업별 S3 객체 분석은 포함되지 않습니다. 무료 평가판 기간 동안 1GB가 넘는 압축되지 않은 데이터를 분석하는 민감한 데이터 검색 작업을 생성하고 실행하면 요금이 부과됩니다. (Macie는 민감한 데이터 검색을 위한 월간 프리 티어를 제공합니다. 매달 S3 객체에 있는 최대 1GB의 압축되지 않은 데이터를 분석하는 데는 요금이 부과되지 않습니다. 처음 1GB의 데이터를 사용한 후에는 비용이 발생합니다.)

무료 평가판 기간 동안 평가판 상태를 확인하고 계정의 예상 사용 비용을 검토할 수 있습니다. 예상 비용은 무료 평가판 기간 동안 지금까지 Macie를 사용한 것을 기준으로 합니다. 평가판 종료 후 발생할 수 있는 사용 비용을 이해하는 데 도움이 될 수 있습니다. Macie가 이러한 값을 계산하는 방법에 대한 자세한 내용은 예상 사용 비용 계산 방법의 이해을 참조하세요.

무료 평가판 사용 중 상태 및 예상 비용 확인

다음 단계에 따라 Amazon Macie 콘솔을 사용하여 평가판 상태를 확인하고 예상 사용 비용을 검토하십시오. Amazon Macie API의 GetUsageStatistics작업을 사용하여 프로그래밍 방식으로 이 데이터에 액세스할 수도 있습니다.

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.

2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 무료 평가판 상태 및 예상 사용 비용을 확인하려는 지역을 선택합니다.
3. 탐색 창에서 사용량을 선택합니다.

사용량 페이지에는 무료 평가판의 남은 일수가 표시됩니다. 또한 미국 달러 기준 예상 사용 비용의 내역도 표시됩니다.

- 예방적 제어 모니터링 - S3 범용 버킷의 인벤토리를 유지 관리하고 무료 평가판 종료 후 보안 및 액세스 제어를 위해 버킷을 평가 및 모니터링하는 데 드는 총 예상 비용입니다.
- 민감한 데이터 검색 작업 - 실행한 모든 민감한 데이터 검색 작업의 총 예상 비용입니다. 민감한 데이터 검색 작업은 무료 평가판에 포함되지 않습니다.
- 민감한 데이터 자동 검색 - 무료 평가판 종료 후 민감한 데이터 자동 검색을 수행하는 데 드는 총 예상 비용을 가격 차원(객체 모니터링 및 객체체 분석) 별로 분류한 값입니다. 이 추정치를 검토하려면 계정이 조직의 Macie 관리자 계정이거나 독립형 Macie 계정이어야 합니다.

조직의 Macie 관리자인 경우 사용 페이지에 조직의 Macie 계정에 대한 세부 정보가 제공됩니다. 테이블에서

- 서비스 할당량 — 계정이 소유한 버킷의 S3 객체를 분석하기 위한 민감한 데이터 검색 작업을 실행하기 위한 현재 월간 할당량입니다.
- 무료 평가판 - 이 필드는 계정이 현재 예방적 제어 모니터링 또는 자동화된 민감한 데이터 검색을 위한 무료 평가판에 참여하고 있는지 여부를 나타냅니다. 계정에 대한 해당 무료 평가판이 종료된 경우 무료 평가판 필드는 비어 있습니다.
- 합계 — 계정당 총 예상 비용입니다.

추정 비용 섹션에는 조직 전체의 추정 비용이 표시됩니다. 조직의 특정 계정에 대한 추정 비용의 분석 내용을 검토하려면 표에서 해당 계정을 선택합니다. 그러면 추정 비용 섹션에 이 내역이 표시됩니다. 다른 계정의 이 데이터를 표시하려면 표에서 계정을 선택하세요. 선택을 지우려면, 계정 ID 옆에 있는 X를 선택합니다.

> **참고**
>
> Amazon S3에 150TB가 넘는 데이터를 저장하는 계정의 경우, 민감한 데이터 자동 검색에 대한 계정의 예상 비용과 실제 비용은 Macie가 30일 무료 평가판 기간 동안 제공하는 예상 비용보다 높을 수 있습니다. 이는 무료 평가판에 등록된 계정에 대해 150GB의 압축되지 않은 데이터를 분석하면 민감한 데이터 자동 검색을 통한 객체 분석이 일시 중지되기 때문입니다. 무료 평가

판 사용이 종료되면 계정에 대한 객체 분석이 재개됩니다. Amazon S3에 150TB가 넘는 데이터를 저장하는 계정의 비용을 예측하는 데 도움이 필요하면 AWS Support에 문의하세요.
무료 평가판 종료 후 민감한 데이터 자동 검색에 드는 비용을 관리하기 위해 개별 S3 버킷을 후속 분석에서 제외할 수 있습니다. 조직의 Macie 관리자인 경우 조직의 개별 계정에 대해 민감한 데이터 자동 검색을 선택적으로 활성화하거나 비활성화할 수 있는 추가 옵션이 있습니다. 이러한 옵션에 대한 자세한 내용은 민감한 데이터 자동 검색 구성 섹션을 참조하세요.

여러 Amazon Macie 계정 관리

AWS 환경에 여러 계정이 있는 경우, Amazon Macie 계정을 사용자 환경에서 연결하고 Macie에서의 조직으로 해당 계정들을 중앙에서 관리할 수 있습니다. 이 구성을 사용하면, 지정된 Macie 관리자가 조직의 Amazon Simple Storage Service(S3) 데이터 자산의 전반적인 보안 태세를 평가 및 모니터링하고 조직의 S3 버킷에서 민감한 데이터를 발견할 수 있습니다. 또한 관리자는 예상 사용 비용 모니터링 및 계정 할당량 평가와 같은 다양한 계정 관리 및 관리 작업을 대규모로 수행할 수 있습니다.

Macie에서, 조직은 지정된 Macie 관리자 계정과 하나 이상의 관련 멤버 계정으로 구성됩니다. Macie를 AWS Organizations와(과) 통합하거나 Macie에서 멤버 초대를 보내고 수락하는 두 가지 방법으로 계정을 연결할 수 있습니다. Macie를 AWS Organizations와(과) 통합하는 것이 좋습니다.

AWS Organizations은(는) AWS 관리자가 여러 AWS 계정을(를) 통합하고 중앙에서 관리할 수 있는 글로벌 계정 관리 서비스입니다. 예산, 보안 및 규정 준수 요구 사항을 지원하도록 설계된 계정 관리 및 통합 결제 기능을 제공합니다. 추가 비용 없이 제공되며 Macie, AWS Security Hub 및 Amazon GuardDuty를 포함한 여러 AWS 서비스와(과) 통합됩니다. 자세한 내용은 AWS Organizations 사용 설명서를 참조하세요.

AWS Organizations을(를) 사용하지 않은 상태로 여러 Macie 계정을 중앙에서 관리하고 싶다면 멤버십 초대를 대신 사용할 수 있습니다. 초대를 보내고 다른 계정에서 초대를 수락하면 계정이 다른 계정의 Macie 관리자가 됩니다. 초대를 받고 수락하면 해당 계정은 Macie 멤버 계정이 되며 Macie 관리자 계정으로 Macie 계정의 특정 설정, 데이터 및 리소스에 액세스하고 이를 관리할 수 있습니다.

주제

- Amazon Macie 관리자 및 멤버 계정 간의 관계 이해
- AWS Organizations를 통한 Amazon Macie 계정 관리
- 초대를 통한 Amazon Macie 계정 관리

Amazon Macie 관리자 및 멤버 계정 간의 관계 이해

조직으로서 여러 Amazon Macie 계정을 중앙에서 관리하는 경우, Macie 관리자는 Amazon Simple Storage Service(S3) 인벤토리 데이터, 정책 조사 결과, 관련 멤버 계정의 특정 Macie 설정 및 리소스에 액세스할 수 있습니다. 또한 관리자는 민감한 데이터 자동 검색을 활성화하고 민감한 데이터 검색 작업을 실행하여 구성원 계정이 소유한 S3 버킷의 민감한 데이터를 탐지할 수 있습니다. 특정 작업에 대한 지원은 Macie 관리자 계정이 초대를 통해 멤버 계정에 연결되었는지 AWS Organizations 또는 초대를 통해 연결되었는지에 따라 달라집니다.

다음 표는 Macie 관리자 및 멤버 계정 간의 관계에 대한 세부 정보를 제공합니다. 이는 각 계정 유형에 대한 기본 권한을 나타냅니다. Macie 기능 및 작업에 대한 액세스를 추가로 제한하려면 사용자 정의 AWS Identity and Access Management (IAM) 정책을 사용할 수 있습니다.

테이블에서

- 자신은 해당 계정이 관련 계정에 대해 작업을 수행할 수 없음을 나타냅니다.
- 누구나는 해당 계정이 개별 관련 계정에 대해 작업을 수행할 수 있음을 나타냅니다.
- 모두은 해당 계정이 작업을 수행할 수 있고 작업이 모든 관련 계정에 적용됨을 나타냅니다.

대시(-)는 해당 계정이 작업을 수행할 수 없음을 나타냅니다.

작업	를 통해 AWS Organizations		초대장별	
	관리자	멤버	관리자	멤버
메이시를 활성화하세요	모두	–	본인	본인
조직의 계정 인벤토리 검토 1	모두	–	모두	–
회원 계정 추가	모두	–	모두	–
S3 버킷의 통계 및 메타데이터를 검토하십시오.	모두	본인	모두	본인
정책 조사 결과 검토	모두	본인	모두	본인
정책 결과 표시 안 함 (아카이브) 2	모두	–	모두	–
정책 결과 게시 3	본인	본인	본인	본인
민감한 데이터 검색 결과를 위한	본인	본인	본인	본인

리포지토리 구성 [4]				
허용 목록 생성 및 사용	본인	본인	본인	본인
사용자 지정 데이터 식별자 생성 및 사용	본인	본인	본인	본인
자동화된 민감 데이터 검색 설정을 구성합니다.	모두	–	모두	–
민감한 데이터 자동 검색을 활성화 또는 비활성화합니다.	모두	–	모두	–
자동화된 민감 데이터 검색 통계, 데이터 및 결과를 검토하십시오.	모두	–	모두	–
민감한 데이터 검색 작업 생성 및 실행 [5]	모두	본인	모두	본인
민감한 데이터 검색 작업의 세부 정보 검토 [6]	본인	본인	본인	본인
민감한 데이터 조사 결과 검토 [7]	본인	본인	본인	본인
민감한 데이터 조사 결과 제외 (보관) 7	본인	본인	본인	본인

민감한 데이터 조사 결과 게시 7	본인	본인	본인	본인
Macie를 구성하여 민감한 데이터 샘플을 검색하여 조사 결과를 얻도록 설정하세요.	본인	본인	본인	본인
민감한 데이터 샘플에서 검색 결과 8을 검색하십시오.	본인	본인	본인	본인
조사 결과에 대한 출판 대상 설정	본인	본인	본인	본인
조사 결과의 게시 빈도를 설정합니다.	모두	본인	모두	본인
샘플 조사 결과 만들기	본인	본인	본인	본인
계정 할당량 및 예상 사용 비용을 검토하세요.	모두	본인	모두	본인
Macie 9 일시 중지	모두	–	모두	본인
메이시 10을 비활성화하세요	본인	본인	본인	본인
회원 계정 제거(연결 해제)	모두	–	모두	–
관리자 계정과의 연결 해제	–	–	–	본인

다른 계정과의 연결 삭제 11	모두	–	모두	본인

1. 내 조직의 관리자는 Macie를 활성화하지 않은 계정을 포함하여 조직의 모든 계정을 AWS Organizations 검토할 수 있습니다. 초대 기반 조직의 관리자는 관리자가 자신의 인벤토리에 추가하는 해당 계정만 검토할 수 있습니다.
2. 관리자만 정책 조사 결과를 금지할 수 있습니다. 관리자가 금지 규칙을 생성하는 경우, 특정 계정을 제외하도록 규칙을 구성하지 않는 한 Macie는 조직의 모든 계정에 대한 정책 조사 결과에 규칙을 적용합니다. 멤버가 금지 규칙을 만들면 Macie는 멤버 계정에 대한 정책 조사 결과에 규칙을 적용하지 않습니다.
3. 영향을 받는 리소스를 소유한 계정만 리소스에 대한 정책 결과를 게시할 수 있습니다. AWS Security Hub관리자 및 멤버 계정 모두 영향을 받는 리소스에 대한 정책 결과를 Amazon에 자동으로 EventBridge 게시합니다.
4. 관리자가 민감한 데이터 자동 검색을 활성화하거나 멤버 계정이 소유한 S3 버킷의 객체를 분석하도록 작업을 구성하는 경우, Macie는 민감한 데이터 검색 결과를 관리자 계정의 리포지토리에 저장합니다.
5. 멤버는 자신의 계정이 소유한 S3 버킷의 객체만 분석하도록 작업을 구성할 수 있습니다. 관리자는 자신의 계정이 소유하거나 멤버 계정이 소유한 버킷의 객체를 분석하도록 작업을 구성할 수 있습니다. 다수 계정 작업에 대한 할당량 적용 및 비용 계산 방법에 대한 자세한 내용은 예상 사용 비용 계산 방법의 이해(을)를 참조하세요.
6. 작업을 생성한 계정만 작업 세부 정보에 액세스할 수 있습니다. 여기에는 S3 버킷 인벤토리의 작업 관련 세부 정보가 포함됩니다.
7. 작업을 생성하는 계정만 해당 작업이 생성하는 민감한 데이터 조사 결과를 액세스, 제한, 게시할 수 있습니다. 관리자만 민감한 데이터 자동 검색이 생성하는 민감한 데이터 조사 결과를 액세스, 제한, 게시할 수 있습니다.
8. 민감한 데이터 조사 결과가 멤버 계정이 소유한 S3 객체에 적용되는 경우 관리자는 조사 결과에 의해 보고된 민감한 데이터의 샘플을 검색할 수 있습니다. 이는 조사 결과의 출처, 관리자 계정, 멤버

계정의 구성 설정과 리소스에 따라 달라집니다. 자세한 내용은 민감한 데이터 샘플을 검색하기 위한 구성 옵션 및 요구 사항을 참조하세요.

9. 관리자가 자신의 계정에 대해 Macie를 일시 중단하려면, 관리자는 먼저 모든 멤버 계정에서 자신의 계정을 연결 해제해야 합니다.

10. 관리자가 자신의 계정에 대해 Macie를 비활성화하려면, 관리자는 먼저 모든 멤버 계정에서 자신의 계정을 연결 해제하고, 자신의 계정과 모든 해당 계정 간의 연결을 삭제해야 합니다. 조직의 관리자는 조직의 관리 계정을 사용하여 다른 계정을 관리자 계정으로 지정함으로써 이 작업을 수행할 AWS Organizations 수 있습니다.

    AWS Organizations 조직 구성원이 Macie를 비활성화하려면 관리자는 먼저 구성원 계정을 관리자 계정에서 분리해야 합니다. 초대 기반 조직의 경우 멤버는 관리자 계정에서 자신의 계정을 연결 해제한 다음 Macie를 비활성화할 수 있습니다.

11. 에 있는 조직의 관리자는 관리자 계정에서 계정 연결을 해제한 후 구성원 계정과의 연결을 삭제할 AWS Organizations 수 있습니다. 계정이 관리자 계정 인벤토리에 계속 나타나지만, 상태는 해당 내용이 멤버 계정이 아닌 것으로 나타납니다. 초대 기반 조직에서는 관리자와 멤버가 다른 계정과 연결 해제한 후 다른 계정과의 연결을 삭제할 수 있습니다. 그러면 해당 계정 인벤토리에 다른 계정이 더 이상 표시되지 않습니다.

AWS Organizations를 통한 Amazon Macie 계정 관리

AWS Organizations를 사용하여 여러 AWS 계정를 중앙에서 관리하는 경우 Amazon Macie를 AWS Organizations와 통합한 다음 조직의 Macie를 중앙에서 관리할 수 있습니다. 이 구성을 사용하면 지정된 Macie 관리자가 최대 10,000개의 계정에 대해 Macie를 활성화하고 관리할 수 있습니다. 또한 관리자는 Amazon Simple Storage Service(S3) 인벤토리 데이터에 액세스하여 계정이 소유하고 있는 S3 버킷에서 민감한 데이터를 검색할 수 있습니다. 관리자가 수행할 수 있는 작업에 대한 자세한 내용은 Amazon Macie 관리자 및 멤버 계정 간의 관계 이해 단원을 참조하세요.

Macie를 AWS Organizations와 통합하려면 먼저 계정을 조직의 위임된 Macie 관리자 계정으로 지정합니다. 그런 다음 Macie 관리자는 조직의 다른 계정에 대해 Macie를 활성화하고, 해당 계정을 Macie 멤버 계정으로 추가하고, 계정에 대한 Macie 설정 및 리소스를 구성합니다.

> **Tip**
>
> 초대를 사용하여 Macie 관리자 계정을 멤버 계정과 이미 연결한 경우, AWS Organizations에서 해당 계정을 조직의 위임된 Macie 관리자 계정으로 지정할 수 있습니다. 이렇게 하면 현재 연

결된 모든 멤버 계정이 멤버으로 유지되므로 AWS Organizations를 사용하여 계정 관리의 이점을 최대한 활용할 수 있습니다. 자세한 내용은 초대 기반 조직에서 전환 섹션을 참조하세요.

이 섹션의 항목에서는 Macie를 조직 내 AWS Organizations와 통합하는 방법과 Macie를 관리하는 방법에 대해 설명합니다.

주제

- Amazon Macie와 함께 사용하기 위한 고려 사항 및 권장 사항 AWS Organizations
- Amazon Macie에서의 조직 통합 및 구성
- 조직의 Amazon Macie 계정 검토
- 조직의 Amazon Macie 멤버 계정 관리
- 조직의 다른 Amazon Macie 관리자 계정 지정
- AWS Organizations와 Amazon Macie의 통합 비활성화

Amazon Macie와 함께 사용하기 위한 고려 사항 및 권장 사항 AWS Organizations

Amazon Macie를 Macie와 AWS Organizations 통합하고 조직을 Macie에서 구성하기 전에 다음 요구 사항 및 권장 사항을 고려하십시오. Macie 관리자 계정과 멤버 계정 간 관계를 이해해야 합니다.

주제

- Macie 관리자 계정 지정하기
- Macie 관리자 계정 지정 변경 또는 제거
- Macie 멤버 계정 추가 및 제거
- 초대 기반 조직에서 전환

Macie 관리자 계정 지정하기

조직의 위임된 Macie 관리자 계정으로 사용할 계정을 결정할 때에는 다음 사항에 유의하십시오.

- 조직은 위임된 Macie 관리자 계정만 하나만 보유할 수 있습니다.
- 계정은 Macie 관리자 계정이면서 동시에 멤버 계정일 수 없습니다.
- 조직의 AWS Organizations 관리 계정만 조직의 위임된 Macie 관리자 계정을 지정할 수 있습니다. 이후에 관리 계정만 해당 지정을 변경하거나 제거할 수 있습니다.

- 조직의 AWS Organizations 관리 계정은 조직의 위임된 Macie 관리자 계정일 수도 있습니다. 하지만 AWS 보안 모범 사례 및 최소 권한 원칙에 따라 이 구성은 권장되지 않습니다. 청구 목적으로 관리 계정에 액세스할 수 있는 사용자는 정보 보안 목적으로 Macie에 액세스해야 하는 사용자와 다를 수 있습니다.

  이 구성을 선호하는 경우 조직의 관리 계정을 위임된 Macie 관리자 계정으로 AWS 리전 지정하기 전에 최소한 하나 이상의 조직 관리 계정에 대해 Macie를 활성화해야 합니다. 그렇지 않으면 해당 계정은 멤버 계정의 Macie 설정 및 리소스에 액세스하고 관리할 수 없습니다.

- 이와 AWS Organizations달리 Macie는 지역 서비스입니다. 즉, Macie 관리자 계정 지정은 리전별로 지정해야 합니다. 이는 또한 Macie 관리자와 멤버 계정 간 연결이 리전별로 이루어진다는 의미이기도 합니다. 예를 들어, 관리 계정에서 미국 동부(버지니아 북부) 리전의 Macie 관리자 계정을 지정하면 Macie 관리자는 해당 리전의 멤버 계정에서만 Macie를 관리할 수 있습니다.

  여러 AWS 리전 Macie 계정을 중앙에서 관리하려면 조직에서 현재 Macie를 사용하거나 사용할 각 지역에 관리 계정을 로그인한 다음 각 지역의 Macie 관리자 계정을 지정해야 합니다. 그러면 Macie 관리자 계정이 해당 리전 각각에서 조직을 구성할 수 있습니다. 현재 Macie를 사용할 수 있는 모든 리전 목록은 AWS 일반 참조의 Amazon Macie 및 엔드포인트 및 할당량을 참조하세요.

- 멤버 계정은 한 번에 하나의 Macie 관리자 계정만 연결할 수 있습니다. 만약 조직이 여러 리전에서 Macie를 사용하는 경우, 지정된 Macie 관리자 계정은 모든 리전에서 동일해야 합니다. 단, 조직의 관리 계정은 각 리전에서 관리자 계정을 별도로 지정해야 합니다.

- 계정은 한 번에 한 조직의 위임된 Macie 관리자 계정일 수 있습니다. 에서 AWS Organizations여러 조직을 관리하는 경우 조직마다 다른 Macie 관리자 계정을 지정해야 합니다. AWS Organizations 이는 요구 사항 때문입니다. 계정은 한 번에 한 조직의 구성원만 될 수 있습니다.

Macie 관리자가 일시 중지, 격리 또는 폐쇄되면 관련된 모든 Macie 구성원 계정이 Macie 회원 계정으로 자동 제거되지만 Macie는 해당 계정에 계속 활성화됩니다. AWS 계정 하나 이상의 구성원 계정에 대해 민감한 데이터 자동 검색 기능이 활성화된 경우 해당 계정에서는 비활성화됩니다. 또한 이렇게 하면 Macie가 계정에 대한 자동 검색을 수행하는 동안 생성하고 직접 제공한 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다. 이 데이터에 대한 액세스를 복원하려면 30일 이내에 다음과 같은 상황이 발생해야 합니다.

1. Macie 관리자의 계정이 AWS 계정 복원되었습니다.
2. AWS Organizations 관리 계정은 해당 계정을 다시 Macie 관리자 계정으로 지정합니다.
3. Macie 관리자가 조직을 구성하고 해당 계정을 자동으로 검색할 수 있도록 다시 활성화합니다.

30일이 지나면 Macie는 해당 계정에 대해 자동 검색을 수행하는 동안 이전에 생성하여 직접 제공한 데이터를 영구적으로 삭제합니다.

Macie 관리자 계정 지정 변경 또는 제거

조직의 AWS Organizations 관리 계정만 조직의 위임된 Macie 관리자 계정 지정을 변경하거나 제거할 수 있습니다.

관리 계정이 지정을 변경하거나 제거하는 경우:

- 연결된 모든 회원 계정은 Macie 회원 계정으로 제거되지만 Macie는 해당 계정에 계속 활성화됩니다. 계정은 독립형 Macie 계정이 됩니다. Macie 사용을 일시 중지하거나 중단하려면 멤버 계정 사용자가 해당 계정에 대해 Macie를 일시 중지 (일시 중지) 하거나 비활성화 (중지) 해야 합니다.
- 민감한 데이터 자동 검색은 활성화된 각 계정에 대해 비활성화됩니다. 또한 이렇게 하면 Macie가 각 계정에 대해 자동 검색을 수행하는 동안 생성하고 직접 제공한 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다. 이 데이터에 대한 액세스를 복원하려면 관리 계정이 30일 이내에 동일한 Macie 관리자 계정을 다시 지정해야 합니다. 또한 Macie 관리자는 조직을 다시 구성하고 30일 이내에 각 계정에 대해 자동 검색을 다시 활성화해야 합니다. 30일이 지나면 데이터가 만료되고 Macie는 데이터를 영구 삭제합니다.

Macie 멤버 계정 추가 및 제거

조직의 멤버 계정을 추가, 제거 및 기타 방식으로 관리할 때 다음 사항에 유의하십시오.

- Macie 관리자 계정은 각 AWS 리전에서 10,000개 이하의 활성(활성화된) Macie 멤버 계정과 연결할 수 있습니다. 조직에서 이 할당량을 초과하는 경우 Macie 관리자는 해당 리전에서 필요한 수의 기존 멤버 계정을 제거할 때까지 멤버 계정을 추가할 수 없습니다. 조직이 이 할당량을 충족하면 해당 계정에 대한 Amazon CloudWatch 이벤트를 AWS Health 생성하여 Macie 관리자에게 알립니다. 이 알림은 계정과 연결된 이메일 주소로도 전송됩니다.

  조직의 Macie 관리자인 경우 Amazon Macie 콘솔의 계정 페이지 또는 ListMembersAmazon Macie API를 사용하여 현재 계정에 연결된 활성 멤버 계정 수를 확인할 수 있습니다. 자세한 정보는 조직의 Amazon Macie 계정 검토을 참조하세요.
- 멤버 계정은 한 번에 하나의 Macie 관리자 계정만 연결할 수 있습니다. 즉, 계정이 이미 AWS Organizations에서 조직의 Macie 관리자 계정과 연결되어 있는 경우 다른 계정에서 보낸 Macie 초대를 수락할 수 없습니다.

마찬가지로 계정이 이미 초대를 수락한 경우 조직의 Macie 관리자는 계정을 Macie 회원 계정으로 추가할 AWS Organizations 수 없습니다. 해당 계정은 먼저 초대 기반 현재 관리자 계정과 연결을 끊어야 합니다.

- AWS Organizations 관리 계정을 Macie 회원 계정으로 추가하려면 관리 계정 사용자가 먼저 해당 계정에 대해 Macie를 활성화해야 합니다. Macie 관리자는 관리 계정에서 Macie를 활성화할 수 없습니다.
- Macie 관리자가 Macie 회원 계정을 제거하는 경우:
  - Macie는 계정에 계속 활성화되어 있습니다. 계정은 독립형 Macie 계정이 됩니다. Macie 사용을 일시 중지하거나 중지하려면 계정 사용자가 해당 계정의 Macie를 일시 중지 (일시 중지) 하거나 비활성화 (중지) 해야 합니다.
  - 민감한 데이터 자동 검색이 활성화되어 있으면 해당 계정에 대해 자동 민감 데이터 검색이 비활성화됩니다. 또한 이렇게 하면 Macie가 계정에 대한 자동 검색을 수행하는 동안 생성하고 직접 제공한 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다.
- 멤버 계정은 Macie 관리자 계정에서 연결을 해제할 수 없습니다. Macie 관리자만 Macie 멤버 계정으로 계정을 제거할 수 있습니다.

초대 기반 조직에서 전환

Macie 멤버십 초대를 사용하여 이미 Macie 관리자 계정을 멤버 계정과 연결한 경우, 해당 계정을 AWS Organizations에서 조직의 위임된 Macie 관리자 계정으로 지정하는 것이 좋습니다. 이렇게 하면 초대 기반 조직에서 전환이 간편해집니다.

이렇게 하면 현재 연결된 모든 멤버 계정이 계속 유지됩니다. 멤버 계정이 조직의 일원인 경우 계정 AWS Organizations연결은 초대를 통해서에서 Macie의 Via로 자동 변경됩니다. AWS Organizations멤버 계정이 AWS Organizations에서 조직의 일부가 아닌 경우 해당 계정 연결은 초대로 계속 유지됩니다. 두 경우 모두 계정은 위임된 Macie 관리자 계정과 멤버 계정으로 계속 연결됩니다.

한 계정을 둘 이상의 Macie 관리자 계정과 동시에 연결할 수 없으므로 이 방법을 사용하는 것이 좋습니다. 에서 AWS Organizations다른 계정을 조직의 Macie 관리자 계정으로 지정하는 경우 지정된 관리자는 초대를 통해 다른 Macie 관리자 계정과 이미 연결된 계정을 관리할 수 없습니다. 각 멤버 계정은 먼저 초대 기반 현재 관리자 계정과 연결을 끊어야 합니다. 그래야 AWS Organizations 에서 조직의 Macie 관리자가 해당 계정을 Macie 멤버 계정으로 추가하고 해당 계정에 대한 관리를 시작할 수 있습니다.

Macie를 Macie와 AWS Organizations 통합하고 Macie에서 조직을 구성한 후에는 필요에 따라 조직에 다른 Macie 관리자 계정을 지정할 수 있습니다. 또한 계속해서 초대를 사용하여 AWS Organizations에서 조직에 속하지 않은 멤버 계정을 연결하고 관리할 수도 있습니다.

Amazon Macie에서의 조직 통합 및 구성

Amazon Macie를 사용하여 시작하려면 조직의 AWS Organizations 관리 계정이 계정을 조직의 위임된 Macie 관리자 계정으로 지정합니다. AWS Organizations이를 통해 Macie는 에서 신뢰할 수 있는 서비스가 될 수 있습니다. AWS Organizations또한 현재 AWS 리전 에서 Macie는 지정된 관리자 계정을 사용할 수 있게 되며, 지정된 관리자 계정은 해당 리전의 조직 내 다른 계정에 대해 Macie를 활성화하고 관리할 수 있습니다. 이러한 권한이 부여되는 방법에 대한 자세한 내용은 사용 설명서의AWS Organizations 다른 AWS OrganizationsAWS 서비스사람과 함께 사용을 참조하십시오.

그런 다음, 위임된 Macie 관리자는 주로 조직의 계정을 해당 리전의 Macie 멤버 계정으로 추가하여 Macie에서 조직을 구성합니다. 그러면 관리자는 해당 리전의 해당 계정에 대한 특정 Macie 설정, 데이터 및 리소스에 액세스할 수 있습니다. 또한 민감한 데이터를 자동으로 검색하고 민감한 데이터 검색 작업을 실행하여 계정이 소유한 Amazon Simple Storage Service (Amazon S3) 버킷의 민감한 데이터를 탐지할 수 있습니다.

이 항목에서는 조직의 위임된 Macie 관리자를 지정하는 방법과 조직의 계정을 Macie 멤버 계정으로 추가하는 방법에 대해 설명합니다. 이러한 작업을 수행하기 전에 관리자 계정과 멤버 계정 간의 관계를 이해해야 합니다. Macie와 함께 사용할 때의 고려 사항 및 권장 사항을 검토하는 것도 좋습니다. AWS Organizations

Tasks

- 1단계: 권한 확인
- 2단계: 조직의 마스터 계정만 위임된 Macie 관리자 지정
- 3단계: 새 조직 계정을 Macie 멤버 계정으로 자동으로 추가하고 활성화
- 4단계: 기존 조직 계정을 Macie 멤버 계정으로 활성화하고 추가

조직을 여러 지역으로 통합하고 구성하려면 AWS Organizations 관리 계정과 위임된 Macie 관리자가 각 추가 지역에서 이 단계를 반복합니다.

1단계: 권한 확인

조직의 위임된 Macie 관리자 계정을 지정하기 전에 AWS Organizations 관리 계정의 사용자로서 다음과 같은 Macie 작업을 수행할 수 있는지 확인하십시오.

`macie2:EnableOrganizationAdminAccount` 이 작업을 수행하면 Macie를 사용하여 조직의 위임된 Macie 관리자 계정을 지정할 수 있습니다.

또한 다음 작업을 수행할 수 있는지 확인하십시오. AWS Organizations

- `organizations:DescribeOrganization`
- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:RegisterDelegatedAdministrator`

이러한 작업을 통해 조직에 대한 정보를 검색하고, Macie를 통합하고, 통합한 정보를 검색하고, 조직에 위임된 Macie 관리자 계정을 지정할 수 있습니다 AWS Organizations. AWS Organizations AWS 서비스

이러한 권한을 부여하려면 계정의 AWS Identity and Access Management (IAM) 정책에 다음 내용을 포함하세요.

```
{
   "Sid": "Grant permissions to designate a delegated Macie administrator",
   "Effect": "Allow",
   "Action": [
      "macie2:EnableOrganizationAdminAccount",
      "organizations:DescribeOrganization",
      "organizations:EnableAWSServiceAccess",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:RegisterDelegatedAdministrator"
   ],
   "Resource": "*"
}
```

AWS Organizations 관리 계정을 조직의 위임된 Macie 관리자 계정으로 지정하려면 계정에 다음과 같은 IAM 작업을 수행할 수 있는 권한도 필요합니다. `CreateServiceLinkedRole` 이 작업을 통해 관리 계정에 대해 Macie를 활성화할 수 있습니다. 하지만 AWS 보안 모범 사례와 최소 권한 원칙에 따라 이렇게 하지 않는 것이 좋습니다.

이 권한을 부여하려면 AWS Organizations 관리 계정의 IAM 정책에 다음 설명을 추가하세요.

```
{
   "Sid": "Grant permissions to enable Macie",
```

```
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "macie.amazonaws.com"
        }
    }
}
```

명세서에서 *111122223333*을 관리 계정의 계정 ID로 바꿉니다.

옵트인 AWS 리전 (기본적으로 비활성화된 지역) 으로 Macie를 관리하려면 요소 및 조건의 Macie 서비스 보안 주체 값도 업데이트하십시오Resource. iam:AWSServiceName 값은 해당 리전의 리전 코드를 지정해야 합니다. 예를 들어, 리전 코드가 me-south-1인 중동(바레인) 리전에서 Macie를 관리하려면 다음과 같이 하세요.

- Resource 요소의 경우 다음을 변경합니다.

  arn:aws:iam::*111122223333*:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie

  with

  arn:aws:iam::*111122223333*:role/aws-service-role/macie.*me-south-1*.amazonaws.com/AWSServiceRoleForAmazonMacie

  여기서 *111122223333*은 관리 계정의 계정 ID를 지정하고 *me-south-1*은 해당 리전의 리전 코드를 지정합니다.

- iam:AWSServiceName 조건에서 macie.amazonaws.com을 macie.*me-south-1*.amazonaws.com으로 바꿉니다. 여기서 *me-south-1*은 해당 리전의 리전 코드를 지정합니다.

현재 Macie를 사용할 수 있는 리전 목록 및 각 리전의 지역 코드는 AWS 일반 참조의 Amazon Macie 엔드포인트 및 할당량을 참조하세요. 옵트인 리전에 대한 자세한 내용은 AWS Account Management 참조 안내서에서 Specifying which AWS 리전 your account can use를 참조하세요.

2단계: 조직의 마스터 계정만 위임된 Macie 관리자 지정

권한을 확인한 후에는 AWS Organizations 관리 계정의 사용자로서 조직의 위임된 Macie 관리자 계정을 지정할 수 있습니다.

조직의 위임된 Macie 관리자 계정을 지정하려면

조직의 위임된 Macie 관리자 계정을 지정하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. AWS Organizations 관리 계정의 사용자만 이 작업을 수행할 수 있습니다.

Console

위임된 Macie 관리자를 지정하고 Amazon Macie 콘솔을 사용하여 멤버 계정을 추가하려면 다음 단계를 수행하세요.

위임된 Macie 관리자 계정을 지정하려면

1. AWS Organizations 관리 계정을 AWS Management Console 사용하여 로그인합니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 조직의 위임된 Macie 관리자 계정을 지정할 지역을 선택합니다.
3. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
4. 현재 리전의 관리 계정에 대해 Macie가 활성화되어 있는지 여부에 따라 다음 중 하나를 수행합니다.
   - Macie가 활성화되지 않은 경우 시작 페이지에서 시작하기를 선택합니다.
   - Macie가 활성화된 경우 탐색 창에서 설정을 선택합니다.
5. 위임된 관리자에서 Macie 관리자 계정으로 AWS 계정 지정하려는 12자리 계정 ID를 입력합니다.
6. 위임을 선택합니다.

조직을 Macie와 통합하려는 각각의 추가 리전에 대해 이전 단계를 반복합니다. 각 리전에서 동일한 Macie 관리자 계정을 지정해야 합니다.

API

위임된 Macie 관리자 계정을 프로그래밍 방식으로 지정하려면 Amazon Macie API의 EnableOrganizationAdminAccount작업을 사용하십시오. 계정을 여러 리전으로 지정하려면 조직을 Macie와 통합하려는 각 리전에 대해 계정을 지정하여 제출합니다. 각 리전에서 동일한 Macie 관리자 계정을 지정해야 합니다.

지정을 제출할 때는 필수 `adminAccountId` 매개 변수를 사용하여 조직의 Macie 관리자 계정으로 지정할 12자리 계정 ID를 지정하십시오. AWS 계정 또한 지정이 적용되는 리전을 지정해야 합니다.

AWS Command Line Interface (AWS CLI) 를 사용하여 Macie 관리자 계정을 지정하려면 명령을 실행합니다. enable-organization-admin-account `admin-account-id`매개 변수에 대해 지정할 12자리 계정 ID를 지정합니다. AWS 계정 `region` 파라미터를 사용하여 지정이 적용되는 리전을 지정합니다. 예:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333
```

여기서 *us-east-1*은 지정이 적용되는 리전(미국 동부(버지니아 북부) 리전)이고 *111122223333*은 지정할 계정의 계정 ID입니다.

조직의 Macie 관리자 계정을 지정한 후, Macie 관리자는 Macie에서 조직 구성을 시작할 수 있습니다.

3단계: 새 조직 계정을 Macie 멤버 계정으로 자동으로 추가하고 활성화

기본적으로, Macie는 새 계정을 AWS Organizations의 조직에 추가할 때 새 계정이 자동으로 활성화되지 않습니다. 또한 계정은 Macie 멤버 계정으로 자동으로 추가되지 않습니다. 계정은 Macie 관리자의 계정 인벤토리에 표시됩니다. 하지만 Macie가 반드시 계정에 활성화되어 있는 것은 아니며 Macie 관리자가 계정의 Macie 설정, 데이터 및 리소스에 반드시 액세스할 수 있는 것도 아닙니다.

조직의 위임 Macie 관리자인 경우 이 구성 설정을 변경할 수 있습니다. 조직의 자동 활성화 기능을 켤 수 있습니다. 이렇게 하면 계정이 조직에 추가될 때 Macie가 새 계정을 자동으로 사용할 수 있게 되며 AWS Organizations, 해당 계정은 구성원 계정으로 Macie 관리자 계정에 자동으로 연결됩니다. 이 설정을 켜도 조직의 기존 계정에는 영향을 주지 않습니다. 기존 계정에 대해 Macie를 활성화하고 관리하려면 계정을 Macie 멤버 계정으로 수동으로 추가해야 합니다. 다음 단계에서는 이 작업을 수행하는 방법을 설명합니다.

> **참고**
>
> 자동 활성화를 켜는 경우 다음 예외 사항에 유의하십시오.
>
> - 새 계정이 이미 다른 Macie 관리자 계정과 연결되어 있는 경우 Macie는 해당 계정을 조직의 멤버 계정으로 자동으로 추가하지 않습니다.

계정을 현재 Macie 관리자 계정에서 분리해야 Macie에 있는 조직의 일부가 될 수 있습니다. 그런 다음, 계정을 수동으로 추가할 수 있습니다. 이러한 경우에 해당하는 계정을 식별하려면 조직의 계정 인벤토리를 검토하면 됩니다.

- 조직의 Macie 구성원 계정 할당량이 10,000개에 도달하면 Macie는 AWS 리전해당 지역에서 이 설정을 자동으로 끕니다.

  이 경우 Macie 관리자 계정을 위한 Amazon CloudWatch 이벤트를 AWS Health 생성하여 알려드립니다. 또한 해당 계정과 연결된 주소로도 이메일을 보내 드립니다. 이후 총 계정 수가 10,000개 미만으로 줄어들면 Macie는 자동으로 설정을 다시 설정합니다.

새 조직 계정을 Macie 멤버 계정으로 자동으로 활성화하고 추가하려면

새 계정을 Macie 멤버 계정으로 자동으로 활성화하고 추가하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 조직의 위임된 Macie 관리자만 이 작업을 수행할 수 있습니다.

Console

콘솔을 사용하여 이 작업을 수행하려면 다음 AWS Organizations `organizations:ListAccounts` 작업을 수행할 수 있어야 합니다. 이 작업을 통해 조직의 계정에 대한 정보를 검색하고 표시할 수 있습니다. 이러한 권한이 있는 경우 다음 단계에 따라 새 조직 계정을 Macie 멤버 계정으로 자동으로 활성화하고 추가합니다.

새 조직 계정을 자동으로 활성화하고 추가하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 자동으로 활성화하려는 지역을 선택하고 새 계정을 Macie 회원 계정으로 추가합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다.
4. 계정 페이지의 새 계정 섹션에서 편집을 선택합니다.
5. 새 계정의 설정 편집 대화 상자에서 Macie 활성화를 선택합니다.

   또한 새 구성원 계정에 대해 민감한 데이터 자동 검색을 활성화하려면 민감한 데이터 자동 검색 활성화를 선택합니다. 계정에 이 기능을 활성화하면 Macie는 계속해서 계정의 S3 버킷에서 샘플 객체를 선택하고 객체를 분석하여 민감한 데이터가 포함되어 있는지 확인합니다. 자세한 정보는 민감한 데이터 자동 검색 수행을 참조하세요.
6. 저장(Save)을 선택합니다.

Macie에서 조직을 구성하려는 각각의 추가 리전에 대해 이전 단계를 반복합니다.

이후에 이러한 설정을 변경하려면 이전 단계를 반복하고 각 설정의 확인란을 지우십시오.

API

프로그래밍 방식으로 새 Macie 회원 계정을 자동으로 활성화하고 추가하려면 Amazon Macie UpdateOrganizationConfigurationAPI의 작업을 사용하십시오. 요청을 제출할 때 `autoEnable` 파라미터 값을 `true`로 설정합니다. (기본값은 `false`입니다.) 또한 해당 요청이 적용되는 리전을 지정해야 합니다. 추가 리전에서 새 계정을 자동으로 활성화하고 추가하려면 각 추가 리전에 대한 요청을 제출하세요.

를 사용하여 요청을 AWS CLI 제출하는 경우, update-organization-configuration명령을 실행하고 새 계정을 자동으로 활성화하고 추가하는 `auto-enable` 파라미터를 지정합니다. 예:

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

여기서 *us-east-1*은 새 계정을 자동으로 활성화하고 추가하는 리전, 즉 미국 동부(버지니아 북부) 리전을 나타냅니다.

이후에 이 설정을 변경하고 새 계정을 자동으로 활성화하거나 추가하는 것을 중지하려면 동일한 명령을 다시 실행하고 해당하는 각 리전에서 `auto-enable` 파라미터 대신 `no-auto-enable` 파라미터를 사용하세요.

새 회원 계정에 대해 민감한 데이터 자동 검색을 자동으로 활성화할 수도 있습니다. 계정에 이 기능을 활성화하면 Macie는 계속해서 계정의 S3 버킷에서 샘플 객체를 선택하고 객체를 분석하여 민감한 데이터가 포함되어 있는지 확인합니다. 자세한 정보는 민감한 데이터 자동 검색 수행을 참조하세요. 멤버 계정에 대해 이 기능을 자동으로 활성화하려면 UpdateAutomatedDiscoveryConfiguration작업을 사용하거나, 를 사용하는 경우 명령을 실행하십시오. AWS CLIupdate-automated-discovery-configuration

4단계: 기존 조직 계정을 Macie 멤버 계정으로 활성화하고 추가

Macie와 AWS Organizations통합할 때 Macie는 조직의 기존 계정 중 일부가 자동으로 활성화되지 않습니다. 또한 계정은 Macie 멤버 계정으로 위임된 Macie 관리자 계정에 자동으로 연결되지 않습니다. 따라서 Macie에서 조직을 통합하고 구성하는 마지막 단계는 기존 조직 계정을 Macie 멤버 계정으로 추가하는 것입니다. 기존 계정을 Macie 멤버 계정으로 추가하면 해당 계정이 자동으로 활성화되고 위임된 Macie 관리자인 사용자는 계정의 특정 Macie 설정, 데이터 및 리소스에 액세스할 수 있습니다.

현재 다른 Macie 관리자 계정과 연결되어 있는 계정은 추가할 수 없다는 점에 유의하세요. 계정을 추가하려면 먼저 계정 소유자와 협의해 현재 관리자 계정에서 계정 연결을 해제하세요. 또한 Macie가 현재 해당 계정에 대해 일시 중단 상태인 경우 기존 계정을 추가할 수 없습니다. 계정 소유자는 먼저 계정에 대해 Macie를 다시 활성화해야 합니다. 마지막으로, AWS Organizations 관리 계정을 멤버 계정으로 추가하려면 해당 계정의 사용자가 먼저 해당 계정에 대해 Macie를 활성화해야 합니다.

기존 조직 계정을 Macie 멤버 계정으로 활성화하고 추가하려면

기존 조직 계정을 Macie 멤버 계정으로 활성화하고 추가하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 조직의 위임된 Macie 관리자만 이 작업을 수행할 수 있습니다.

Console

콘솔을 사용하여 이 작업을 수행하려면 다음 AWS Organizations 작업을 수행할 수 있어야 합니다. `organizations:ListAccounts` 이 작업을 통해 조직의 계정에 대한 정보를 검색하고 표시할 수 있습니다. 이러한 권한이 있는 경우 다음 단계에 따라 기존 계정을 Macie 멤버 계정으로 활성화하고 추가하세요.

기존 조직 계정을 활성화하고 추가하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 활성화하려는 지역을 선택하고 기존 계정을 Macie 회원 계정으로 추가합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다.

   계정 페이지가 열리고 Macie 계정과 연결된 계정 테이블이 표시됩니다. 계정이 조직의 일부인 경우 유형은 AWS Organizations Via입니다. AWS Organizations 계정이 이미 Macie 회원 계정인 경우 상태는 활성화됨으로 표시됩니다.
4. 계정 테이블에서, Macie 멤버 계정으로 추가하려는 각 계정의 확인란을 선택합니다.
5. 작업 메뉴에서 멤버 추가를 선택합니다.
6. 선택한 계정 수를 멤버 계정으로 추가할 것임을 확인합니다.

선택한 계정의 추가를 확인하면 계정 상태가 활성화 진행 중으로 변경되고 다시 활성화됨으로 변경됩니다. 멤버 계정을 추가한 후 계정에 대해 민감한 데이터 자동 검색을 활성화할 수도 있습니다. 계정 테이블에서 활성화할 각 계정의 확인란을 선택한 다음 작업 메뉴에서 민감한 데이터 자동 검색 활성화를 선택합니다. 계정에 대해 이 기능을 활성화하면 Macie는 계속해서 계정의 S3 버킷에서 샘플 객체를 선택하고 객체를 분석하여 민감한 데이터가 포함되어 있는지 확인합니다. 자세한 정보는 민감한 데이터 자동 검색 수행을 참조하세요.

Macie에서 조직을 구성하려는 각각의 추가 리전에 대해 이전 단계를 반복합니다.

API

하나 이상의 기존 계정을 프로그래밍 방식으로 활성화하고 Macie 멤버 계정으로 추가하려면 Amazon Macie CreateMemberAPI의 작업을 사용하십시오. 요청을 제출할 때 지원되는 매개 변수를 사용하여 활성화하고 AWS 계정 추가할 각 계정의 12자리 계정 ID와 이메일 주소를 지정합니다. 또한 요청이 적용되는 리전을 지정합니다. 추가 리전에서 기존 계정을 활성화하고 추가하려면 각 추가 리전에 대한 요청을 제출하세요.

활성화 및 추가할 계정 ID 및 이메일 주소를 검색하려면 선택적으로 Amazon Macie API ListMembers작업을 사용할 수 있습니다. AWS 계정 이 작업을 수행하면 Macie 멤버 계정이 아닌 계정을 포함하여 Macie 계정과 연결된 계정에 대한 세부 정보가 제공됩니다. 계정의 `relationshipStatus` 속성 값이 `Enabled`가 아닌 경우 해당 계정은 Macie 멤버 계정이 아닙니다.

를 사용하여 기존 계정을 하나 이상 활성화하고 추가하려면 create-member 명령을 실행합니다. AWS CLI`region` 파라미터를 사용하여 계정을 활성화하고 추가할 리전을 지정합니다. `account`매개변수를 사용하여 추가할 각 AWS 계정 계정의 계정 ID와 이메일 주소를 지정합니다. 예:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

여기서 *us-east-1*은 계정을 Macie 멤버 계정으로 활성화하고 추가할 수 있는 리전(미국 동부(버지니아 북부) 리전)이고, `account` 파라미터는 계정의 계정 ID(*123456789012*)와 이메일 주소(*janedoe@example.com*)를 지정합니다.

요청이 성공하면 지정된 계정의 상태(`relationshipStatus`)가 계정 인벤토리에서 `Enabled`로 변경됩니다.

또한 하나 이상의 계정에 대해 민감한 데이터 자동 검색을 활성화하려면 BatchUpdateAutomatedDiscoveryAccounts작업을 사용하거나, 를 사용하는 경우 batch-update-automated-discovery-accounts 명령을 실행하십시오. AWS CLI계정에 대해 이 기능을 활성화하면 Macie는 계속해서 계정의 S3 버킷에서 샘플 객체를 선택하고 객체를 분석하여 민감한 데이터가 포함되어 있는지 확인합니다. 자세한 내용은 민감한 데이터 자동 검색 수행을(를) 참조하세요.

조직의 Amazon Macie 계정 검토

Amazon Macie에서 AWS Organizations 조직을 통합 및 구성한 후 위임된 Macie 관리자는 Macie에 있는 조직 계정의 인벤토리에 액세스할 수 있습니다. 조직의 Macie 관리자는 이 인벤토리를 사용하여

AWS 리전에서 조직의 Macie 계정에 대한 통계 및 세부 정보를 한 번에 검토할 수 있습니다. 또한 이를 사용하여 계정에 대한 특정 관리 작업을 수행할 수 있습니다.

조직의 Macie 계정을 검토하려면

조직의 계정을 검토하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 콘솔을 사용하려는 경우 다음 AWS Organizations 작업을 수행할 수 있어야 `organizations:ListAccounts` 합니다. 이 작업을 통해 AWS Organizations의 조직에 속한 계정에 대한 정보를 검색하고 표시할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 조직의 Macie 계정을 검토하려면 다음 단계를 따르세요.

조직의 계정 검토

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 조직의 계정을 검토하려는 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다.

계정 페이지가 열리고 집계된 통계와 현재 AWS 리전에 Macie 계정과 연결된 계정 표가 표시됩니다.

계정 페이지 상단에는 다음과 같은 집계된 통계가 표시됩니다.

를 통해 AWS Organizations

Active는 현재 조직의 Macie 회원 계정을 통해 사용자 AWS Organizations 계정과 연결되어 있는 총 계정 수를 보고합니다. Macie는 이러한 계정에서 활성화되어 있으며, 해당 계정의 Macie 관리자입니다.

모든 보고서는 현재 Macie 회원 계정이 아닌 계정을 포함하여 사용자 계정과 연결된 총 계정 수를 보고합니다. AWS Organizations

초대장별

활성은 Macie 초대를 통해 내 계정과 연결되어 있으며 현재 Macie 멤버 계정인 총 계정 수를 보고합니다. 이러한 계정은 아직 사용자 계정과 연결되어 있지 않습니다. AWS Organizations Macie는 이러한 계정에서 활성화되어 있으며, 해당 계정이 Macie 멤버십 초대를 수락했으므로 사용자는 해당 계정의 Macie 관리자입니다.

모두은 초대에 응답하지 않은 계정을 포함하여 Macie 초대를 통해 내 계정에 연결된 총 계정 수를 보고합니다.

활성/모두

활성 보고서는 Macie 초대를 통해 AWS Organizations 또는 Macie 초대를 통해 현재 사용자 계정의 Macie 회원 계정인 총 계정 수를 나타냅니다. Macie는 이러한 계정에서 활성화되어 있으며, 해당 계정의 Macie 관리자입니다.

모든 보고서는 Macie 초대를 통해 AWS Organizations 또는 Macie 초대를 통해 사용자 계정과 연결된 총 계정 수를 보고합니다. 여기에는 현재 Macie 회원 계정이 아닌 조직에 AWS Organizations 속해 있는 계정과 Macie 멤버십 초대에 응답하지 않은 모든 계정이 포함됩니다.

표에서 현재 리전에 있는 각 계정에 대한 세부 정보를 확인할 수 있습니다. 이 표에는 Macie 초대를 통해 AWS Organizations 또는 Macie 초대를 통해 Macie 계정과 연결된 모든 계정이 포함됩니다.

계정 ID

AWS 계정의 계정 ID 및 이메일 주소입니다.

이름

AWS 계정의 계정 이름입니다. 이 값은 일반적으로 Macie 초대를 통해 내 계정과 연결된 계정의 경우 N/A입니다.

Type

Macie 초대 또는 AWS Organizations 을(를) 통해 내 계정과 계정을 연결하는 방법입니다.

상태

사용자 계정과 계정 간의 관계 상태입니다. AWS Organizations 조직 내 계정 (유형은 Via AWS Organizations) 의 경우 가능한 값은 다음과 같습니다.

- 계정이 일시 중지됨 - AWS 계정 는 일시 중지되어 있습니다.
- 생성됨/활성화 - Macie는 계정을 Macie 멤버 계정으로 활성화하고 추가하는 요청을 처리 중입니다.
- 활성화됨 - 계정이 Macie 멤버 계정입니다. Macie는 계정에서 활성화되어 있으며, 해당 계정의 Macie 관리자입니다.
- 구성원 아님 - 계정이 조직의 AWS Organizations 일부이지만 Macie 회원 계정은 아닙니다.
- 중지됨 (일시 중지) - 멤버 계정이지만 Macie는 현재 해당 계정에서 일시 중지 상태입니다.

- 지역 비활성화 — 계정이 속한 조직의 AWS Organizations 일부이지만 현재 지역은 사용할 수 없습니다. AWS 계정
- 제거됨(연결 해제됨) - 이 계정은 이전에 Macie 멤버 계정이었으나 이후에 멤버 계정으로 제거되었습니다. Macie 관리자 계정에서 계정 연결을 해제했습니다. Macie는 계정에 계속 활성화되어 있습니다.

마지막 상태 업데이트

사용자 또는 관련 계정이 가장 최근에 계정 간 관계에 영향을 미치는 작업을 수행한 시점입니다.

민감한 데이터 자동 검색

계정에 대해 민감한 데이터 자동 검색이 현재 활성화되어 있는지 또는 비활성화되어 있는지 여부.

특정 필드를 기준으로 테이블을 정렬하려면 해당 필드의 열 제목을 선택합니다. 정렬 순서를 변경하려면 열 제목을 다시 선택합니다. 표를 필터링하려면 필터 상자에 커서를 놓고 필드에 필터 조건을 추가합니다. 결과를 더 세분화하려면 추가 필드에 필터 조건을 추가합니다.

API

프로그래밍 방식으로 조직의 계정을 검토하려면 Amazon Macie API ListMembers작업을 사용하고 요청이 적용되는 지역을 지정하십시오. 추가 리전의 계정을 검토하려면 각 추가 리전에서 요청을 제출합니다.

요청을 제출할 때 `onlyAssociated` 파라미터를 사용하여 응답에 포함시킬 계정을 지정합니다. 기본적으로 Macie는 Macie 초대를 통해 AWS Organizations 또는 Macie 초대를 통해 지정된 지역의 Macie 멤버 계정인 계정에 대한 세부 정보만 반환합니다. 멤버 계정이 아닌 계정을 포함하여 Macie 계정과 연결된 모든 계정의 세부 정보를 검색하려면 요청에 파라미터를 포함하고 `onlyAssociated` 파라미터 값을 `false`로 설정합니다.

AWS Command Line Interface (AWS CLI)를 사용하여 조직의 계정을 검토하려면 list-members 명령을 실행합니다. `only-associated` 파라미터에 연결된 모든 계정을 포함할지, 아니면 Macie 멤버 계정만 포함할지 지정합니다. 멤버 계정만 포함시키려면 이 파라미터를 생략하거나 파라미터 값을 `true`로 설정합니다. 모든 계정을 포함시키려면 이 값을 `false`(으)로 설정합니다. 예:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

여기서 *us-east-1*은 요청이 적용되는 리전, 즉 미국 동부 (버지니아 북부) 리전을 나타냅니다.

요청이 성공하면 Macie는 `members` 배열을 반환합니다. 배열에는 요청에 지정된 기준을 충족하는 각 계정에 대한 `member` 객체가 포함됩니다. 해당 객체에서 `relationshipStatus` 필드는 내 계정과 지정된 리전의 다른 계정 간의 관계의 현재 상태를 나타냅니다. AWS Organizations 조직 내 계정의 경우 가능한 값은 다음과 같습니다.

- `AccountSuspended`— 일시 중지되었습니다. AWS 계정
- `Created` - Macie는 계정을 Macie 멤버 계정으로 활성화하고 추가하는 요청을 처리 중입니다.
- `Enabled` - 해당 계정은 Macie 멤버 계정입니다. Macie는 계정에서 활성화되어 있으며, 해당 계정의 Macie 관리자입니다.
- `Paused` - 해당 계정은 Macie 멤버 계정이지만 현재 해당 계정에 대해 Macie가 일시 중지 상태입니다.
- `RegionDisabled`— 계정이 내 조직의 AWS Organizations 일부이지만 현재 지역은 사용할 수 없습니다 AWS 계정.
- `Removed` - 이 계정은 이전에 Macie 멤버 계정이었으나 이후 멤버 계정으로 제거되었습니다. Macie 관리자 계정에서 계정 연결을 해제했습니다. Macie는 계정에 계속 활성화되어 있습니다.

`member` 객체의 다른 필드에 대한 자세한 내용은 Amazon Macie API 참조에서 멤버를 참조하십시오.

조직의 Amazon Macie 멤버 계정 관리

AWS Organizations 조직이 Amazon Macie에 통합 및 구성되면 조직의 위임된 Macie 관리자는 구성원 계정의 특정 Macie 설정, 데이터 및 리소스에 액세스할 수 있습니다.

조직의 Macie 관리자는 Macie에서 특정 계정 관리 및 관리 작업을 중앙에서 수행할 수 있습니다. 예:

- Macie 멤버 계정 추가 및 제거
- 개별 계정의 Macie 상태 관리(예: 계정에 대한 Macie 활성화 또는 일시 중지)
- 개별 계정 및 조직 전체의 Macie 할당량 및 예상 사용 비용 모니터링

Macie 멤버 계정에 대한 Amazon Simple Storage Service(S3)의 인벤토리 데이터 및 정책 조사 결과를 검토할 수도 있습니다. 또한 계정이 소유한 S3 버킷에서 민감한 데이터를 발견할 수 있습니다. 수행할 수 있는 작업의 세부 목록은 Amazon Macie 관리자 및 멤버 계정 간의 관계 이해 단원을 참조하세요.

기본적으로 Macie에서는 조직의 모든 Macie 멤버 계정에 대한 관련 데이터 및 리소스를 확인할 수 있습니다. 또한 드릴다운하여 개별 계정의 데이터와 리소스를 검토할 수 있습니다. 예를 들어 요약 대시

보드를 사용하여 조직의 Amazon S3 보안 상태를 평가하는 경우 계정별로 데이터를 필터링할 수 있습니다. 마찬가지로 예상 사용 비용을 모니터링하는 경우 개별 멤버 계정의 예상 비용 내역에 액세스할 수 있습니다.

관리자 계정과 멤버 계정에 공통으로 적용되는 작업 외에도 조직의 다양한 관리 작업을 수행할 수 있습니다.

Tasks

- 조직에 Amazon Macie 멤버 계정 추가
- 조직의 멤버 계정에 대한 Amazon Macie의 일시 중지
- 조직에서 Amazon Macie 멤버 계정 제거

조직의 Macie 관리자는 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 이러한 작업을 수행할 수 있습니다. 콘솔을 사용하려는 경우 다음 작업을 수행할 수 있어야 합니다. AWS Organizations `organizations:ListAccounts` 이 작업을 통해 AWS Organizations의 조직에 속한 계정에 대한 정보를 검색하고 표시할 수 있습니다.

조직에 Amazon Macie 멤버 계정 추가

경우에 따라 계정을 Macie 멤버 계정으로 수동으로 추가해야 할 수도 있습니다. 이전에 멤버 계정으로 제거(연결 해제)한 계정이 여기에 해당합니다. 조직에서 계정을 추가할 때 새 구성원 계정을 자동으로 활성화하고 추가하도록 Macie를 구성하지 않은 경우에도 마찬가지입니다. AWS Organizations

계정을 Macie 회원 계정으로 추가하는 경우:

- Macie는 해당 지역에서 아직 활성화되지 않은 AWS 리전경우 현재 계정을 사용할 수 있습니다.
- 계정은 해당 지역의 구성원 계정으로서 Macie 관리자 계정과 연결되어 있습니다. 계정 간에 이러한 관계를 설정했다는 초대장이나 기타 알림이 멤버 계정에는 수신되지 않습니다.
- 해당 지역의 계정에 대해 민감한 데이터 자동 검색이 활성화되어 있을 수 있습니다. 이는 조직에 지정한 구성 설정에 따라 달라집니다. 자세한 정보는 민감한 데이터 자동 검색 구성을 참조하세요.

이미 다른 Macie 관리자 계정과 연결되어 있는 계정은 추가할 수 없다는 점에 유의하세요. 먼저 계정을 현재 관리자 계정에서 분리해야 합니다. 또한 Macie가 해당 계정에 대해 이미 활성화되어 있지 않는 한 AWS Organizations 관리 계정을 구성원 계정으로 추가할 수 없습니다. 추가 요구 사항에 대한 자세한 내용은 Amazon Macie와 함께 사용하기 위한 고려 사항 및 권장 사항 AWS Organizations 단원을 참조하세요.

조직에 Macie 멤버 계정을 추가하려면

조직에 Macie 멤버 계정을 하나 이상 추가하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하면 됩니다.

Console

Amazon Macie 콘솔을 사용하여 Macie 멤버 계정을 하나 이상 추가하려면 다음 단계를 따르세요.

Macie 멤버 계정을 추가하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 회원 계정을 추가할 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 계정과 연결된 계정 테이블이 표시됩니다.
4. (선택 사항) 조직에 속해 있는 AWS Organizations 계정과 Macie 구성원 계정이 아닌 계정을 더 쉽게 식별하려면 계정 테이블 위의 필터 상자를 사용하여 다음 필터 조건을 추가하십시오.

   - 유형 = 조직
   - 상태 = 멤버가 아님

   이전에 제거했는데 멤버 계정으로 추가하려는 계정도 표시하려면 상태 = 제거됨 필터 조건도 추가하세요.
5. 계정 테이블에서 멤버 계정으로 추가할 각 계정의 확인란을 선택합니다.
6. 작업 메뉴에서 멤버 추가를 선택합니다.
7. 선택한 계정 수를 멤버 계정으로 추가할 것임을 확인합니다.

선택을 확인하면 선택한 계정의 상태가 활성화 진행 중으로 변경되고 계정 인벤토리에서 활성화됨으로 변경됩니다.

멤버 계정을 추가하려는 각각의 추가 리전에 대해 이전 단계를 반복합니다.

API

프로그래밍 방식으로 Macie 회원 계정을 하나 이상 추가하려면 Amazon Macie CreateMemberAPI의 작업을 사용하십시오.

요청을 제출할 때 지원되는 매개 변수를 사용하여 추가하려는 각 AWS 계정 계정의 12자리 계정 ID와 이메일 주소를 지정하십시오. 또한 요청이 적용되는 리전을 지정합니다. 추가 리전에 계정을 추가하려면 각 추가 리전에서 요청을 제출하세요.

추가할 계정의 계정 ID와 이메일 주소를 검색하려면 API 작업의 출력과 Amazon Macie AWS Organizations API의 ListAccountsListMembers작업을 상호 연관시킬 수 있습니다. Macie API의 ListMembers 작업의 경우 요청에 파라미터를 포함하고 `onlyAssociated` 파라미터 값을 `false`로 설정하세요. 작업이 성공하면 Macie는 현재 멤버 계정이 아닌 계정을 포함하여 지정된 리전의 Macie 관리자 계정과 연결된 모든 계정에 대한 세부 정보를 제공하는 `members` 배열을 반환합니다. 배열에서 다음을 참고하세요.

- 계정의 `relationshipStatus` 속성 값이 `Enabled`가 아닌 경우 해당 계정은 사용자 계정과 연결되어 있지만 Macie 멤버 계정은 아닙니다.
- 계정이 배열에는 포함되어 있지 않지만 AWS Organizations API의 ListAccounts 작업 결과에는 포함되어 있는 경우 해당 계정은 AWS Organizations 에서 조직의 일부이지만 사용자 계정과 연결되어 있지 않으므로 Macie 멤버 계정이 아닙니다.

를 사용하여 멤버 계정을 추가하려면 AWS CLIcreate-member 명령을 실행합니다. `region` 파라미터를 사용하여 계정을 추가할 리전을 지정합니다. `account` 파라미터를 사용하여 추가할 각 계정의 계정 ID와 이메일 주소를 지정합니다. 예:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

여기서 *us-east-1*은 계정을 멤버 계정으로 추가할 수 있는 리전(미국 동부(버지니아 북부) 리전)이고, `account` 파라미터는 계정의 계정 ID(*123456789012*) 및 이메일 주소(*janedoe@example.com*)를 지정합니다.

요청이 성공하면 지정된 계정의 상태(`relationshipStatus`)가 계정 인벤토리에서 `Enabled`로 변경됩니다.

조직의 멤버 계정에 대한 Amazon Macie의 일시 중지

내 AWS Organizations조직의 Macie 관리자는 조직의 구성원 계정에 대해 Macie를 일시 중단할 수 있습니다. 이렇게 하면 나중에 해당 계정에 대해 Macie를 다시 활성화할 수도 있습니다.

멤버 계정에 대해 Macie를 정지하는 경우:

- Macie는 현재 AWS 리전에 있는 계정의 Amazon S3 데이터 액세스 권한을 상실하고, 해당 메타데이터 제공을 중단합니다.

- Macie는 리전에서 계정에 대한 모든 활동을 중지합니다. 여기에는 보안 및 액세스 제어를 위한 S3 버킷 모니터링, 민감한 데이터 자동 검색 수행, 현재 진행 중인 민감한 데이터 검색 작업 실행 등이 포함됩니다.
- Macie는 리전 내 계정에서 생성한 모든 민감한 데이터 검색 작업을 취소합니다. 취소된 작업은 다시 시작하거나 재개할 수 없습니다. 멤버 계정이 소유하고 있는 데이터를 분석하기 위해 작업을 생성한 경우, Macie는 작업을 취소하지 않습니다. 대신 작업은 계정에서 소유한 리소스를 건너뜁니다.

계정이 일시 중지되는 동안 Macie는 해당 리전의 계정에 대한 Macie 세션 식별자, 설정 및 리소스를 유지합니다. 예를 들어 계정의 검색 결과는 그대로 유지되며 최대 90일 동안 영향을 받지 않습니다. Macie가 해당 리전의 계정에 대해 일시 중지되는 동안 조직에서는 해당 리전의 계정에 대해 Macie 요금이 부과되지 않습니다.

조직의 멤버 계정에 대해 Macie를 일시 중지하려면

조직의 멤버 계정에 대해 Macie를 일시 중지하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 멤버 계정의 Macie를 일시 중지하려면 다음 단계를 수행합니다.

멤버 계정에서 Macie를 일시 중지하는 방법

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 구성원 계정에 대해 Macie를 일시 중단하려는 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 계정과 연결된 계정 테이블이 표시됩니다.
4. 계정 테이블에서 일시 중지하려는 계정의 확인란을 선택합니다.
5. 작업 메뉴에서 Macie 일시 중지를 선택합니다.
6. Macie 를 일시 중지할지 확인합니다.

일시 중지를 확인하면 계정 인벤토리에서 계정 상태가 중지됨(일시 중지됨)으로 변경됩니다.

Macie 계정을 이용 정지하려는 각 리전마다 앞의 단계를 반복합니다.

API

회원 계정의 Macie를 프로그래밍 방식으로 일시 중지하려면 Amazon Macie UpdateMemberSessionAPI의 작업을 사용하십시오.

요청을 제출할 때 `id` 파라미터를 사용하여 Macie를 일시 중단하려는 계정의 12자리 계정 ID를 지정하십시오. AWS 계정 `status` 파라미터의 경우 Macie 계정의 새 상태를 PAUSED로 지정합니다. 또한 요청이 적용되는 리전을 지정합니다. 추가로 다른 리전에서 계정을 일시 중지하려면 각 추가 리전에 대해 요청을 제출합니다.

일시 중지할 계정의 계정 ID를 검색하려면 Amazon Macie API의 ListMembers작업을 사용할 수 있습니다. 이렇게 하려면 요청에 `onlyAssociated` 파라미터를 포함하여 결과를 필터링하는 것을 고려해 보십시오. 이 파라미터의 값을 `true`(으)로 설정하면 현재 멤버 계정인 계정에 대한 세부 정보만 제공하는 `members` 배열을 반환합니다.

를 사용하여 멤버 계정의 Macie를 일시 AWS CLI중지하려면 명령을 실행합니다. update-member-session `region`매개 변수를 사용하여 Macie를 일시 중단할 지역을 지정하고, `id` 매개 변수를 사용하여 Macie를 일시 AWS 계정 중단할 계정 ID를 지정합니다. `status` 파라미터에서 PAUSED를 지정합니다. 예:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

여기서 *us-east-1*은 Macie를 일시 중지할 리전(미국 동부 (버지니아 북부) 리전)이고, *123456789012*는 Macie를 일시 중지할 계정의 계정 ID이며, PAUSED은(는) 해당 계정에서 Macie의 새로운 상태입니다.

요청이 성공하면 Macie는 빈 응답을 반환하고 지정된 계정의 상태는 계정 인벤토리에서 Paused로 변경됩니다.

조직에서 Amazon Macie 멤버 계정 제거

멤버 계정의 Macie 설정, 데이터 및 리소스에 액세스하는 것을 중지하려면 Macie 멤버 계정인 계정을 제거하면 됩니다. Macie 관리자 계정에서 계정 연결을 해제하면 됩니다. 단, 멤버 계정에 대해서는 본인만 이 작업을 수행할 수 있습니다. AWS Organizations 구성원 계정은 Macie 관리자 계정과의 연결을 해제할 수 없습니다.

Macie 멤버 계정을 제거해도 Macie는 현재 AWS 리전에서 계정을 사용할 수 있는 상태로 유지됩니다. 하지만 이 계정은 Macie 관리자 계정과의 연결이 끊어지고 독립 실행형 Macie 계정이 됩니다. 즉, 계정

의 Amazon S3 데이터에 대한 메타데이터 및 정책 조사 결과를 포함하여 계정의 모든 Macie 설정, 데이터 및 리소스에 액세스할 수 없게 됩니다. 또한 이는 더 이상 Macie를 사용하여 계정이 소유한 S3 버킷의 민감한 데이터를 검색할 수 없음을 의미합니다. 이를 위해 민감한 검색 작업을 이미 생성한 경우 해당 작업은 계정이 소유한 버킷을 건너뛰게 됩니다. 계정에 대해 민감한 데이터 자동 검색 기능을 활성화한 경우, 계정 자동 검색을 수행하는 동안 Macie가 생성하고 직접 제공한 통계 데이터, 인벤토리 데이터 및 기타 정보에 사용자와 회원 계정 모두 액세스할 수 없게 됩니다.

Macie 멤버 계정을 제거한 후에도 해당 계정은 계정 인벤토리에 계속 표시됩니다. Macie는 계정 소유자에게 계정 삭제 사실을 알리지 않습니다. 나중에 조직에 계정을 다시 추가할 수 있습니다. 계정을 추가하고 30일 이내에 민감한 데이터 자동 검색을 활성화하면 Macie가 계정에 대한 자동 검색을 수행하는 동안 이전에 생성하여 직접 제공한 데이터 및 정보에도 다시 액세스할 수 있습니다.

조직에서 Macie 멤버 계정 제거

조직에서 Macie 멤버 계정을 제거하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 Macie 멤버 계정을 제거하려면 다음 단계를 따르세요.

Macie 멤버 계정을 제거하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 회원 계정을 제거하려는 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 계정과 연결된 계정 테이블이 표시됩니다.
4. 계정 테이블에서 멤버 계정에서 삭제하려는 계정의 확인란을 선택합니다.
5. 작업 메뉴에서 계정 연결 해제를 선택합니다.
6. 선택한 계정을 멤버 계정에서 제거할 것인지 확인합니다.

선택을 확인하면 계정 인벤토리에서 계정 상태가 제거됨(연결 해제됨)으로 변경됩니다.

멤버 계정을 제거할 추가적인 각 리전마다 이전 단계를 반복합니다.

API

프로그래밍 방식으로 Macie 회원 계정을 제거하려면 Amazon Macie DisassociateMemberAPI의 작업을 사용하십시오.

요청을 제출할 때 `id` 파라미터를 사용하여 제거할 회원 계정의 12자리 AWS 계정 ID를 지정합니다. 또한 요청이 적용되는 리전을 지정합니다. 다른 리전에 계정을 삭제하려면 각 리전에서 요청을 제출합니다.

제거할 멤버 계정의 계정 ID를 검색하려면 Amazon Macie API의 ListMembers작업을 사용할 수 있습니다. 이렇게 하려면 요청에 `onlyAssociated` 파라미터를 포함하여 결과를 필터링하는 것을 고려해 보십시오. 이 파라미터의 값을 `true`(으)로 설정하면 현재 Macie 멤버 계정인 계정에 대한 세부 정보만 제공하는 `members` 배열을 반환합니다.

를 사용하여 Macie 멤버 계정을 제거하려면 AWS CLIdisassociate-member 명령을 실행합니다. `region` 파라미터를 사용하여 계정을 제거할 리전을 지정합니다. `id` 파라미터를 사용하여 제거할 멤버 계정의 계정 ID를 지정합니다. 예:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

여기서 *us-east-1*은 계정을 제거할 리전(미국 동부 (버지니아 북부) 리전)이고 *123456789012*는 제거할 계정의 계정 ID입니다.

요청이 성공하면 Macie는 빈 응답을 반환하고 지정된 계정의 상태는 계정 인벤토리에서 `Removed`로 변경됩니다.

조직의 다른 Amazon Macie 관리자 계정 지정

AWS Organizations 조직이 Amazon Macie에 통합 및 구성되면 AWS Organizations 관리 계정은 다른 계정을 조직의 위임된 Macie 관리자 계정으로 지정할 수 있습니다.

조직의 AWS Organizations 관리 계정 사용자는 조직에 다른 Macie 관리자 계정을 지정하기 전에 다음 권한 요구 사항을 충족하는지 확인하십시오.

- 조직의 Macie 관리자 계정을 처음 지정하는 데 필요했던 것과 동일한 권한이 있어야 합니다. 또한 다음 AWS Organizations 작업을 수행할 수 있어야 합니다. `organizations:DeregisterDelegatedAdministrator` 이 추가 작업을 통해 현재 지정을 제거할 수 있습니다.
- 현재 사용자 계정이 Macie 회원 계정인 경우, 현재 Macie 관리자와 협력하여 Macie 회원 계정에서 사용자의 계정을 제거하세요. 그렇지 않으면 다른 관리자 계정을 지정하기 위한 Macie 작업에 액세스할 수 없습니다. 새 관리자 계정을 지정하면 새 Macie 관리자가 해당 계정을 Macie 회원 계정으로 다시 추가할 수 있습니다.

조직에서 Macie를 여러 번 AWS 리전사용하는 경우 조직에서 Macie를 사용하는 각 지역의 위임된 Macie 관리자 계정도 변경해야 합니다. 위임된 Macie 관리자 계정은 모든 지역에서 동일해야 합니다. 에서 AWS Organizations여러 조직을 관리하는 경우 한 계정은 한 번에 한 조직의 위임된 Macie 관리자 계정으로만 사용할 수 있다는 점도 참고하세요. 추가 요구 사항에 대한 자세한 내용은 Amazon Macie와 함께 사용하기 위한 고려 사항 및 권장 사항 AWS Organizations 단원을 참조하세요.

> **Note**
>
> 조직에 다른 Macie 관리자 계정을 지정하면 Macie가 조직 내 계정에 대한 민감한 데이터 자동 검색을 수행하는 동안 생성하여 직접 제공한 기존 통계 데이터, 인벤토리 데이터 및 기타 정보에 대한 액세스도 비활성화됩니다. 새 Macie 관리자 계정은 기존 데이터에 액세스할 수 없습니다. 지정을 변경하고 새 Macie 관리자가 계정에 대한 자동 검색을 활성화하면 Macie는 계정에 대한 자동 검색을 수행할 때 새 데이터를 생성하고 유지 관리합니다.

조직의 다른 Amazon Macie 관리자 계정을 지정하려면

조직에 다른 Macie 관리자 계정을 지정하려면 Amazon Macie 콘솔 또는 Amazon Macie와 API의 조합을 사용할 수 있습니다. AWS Organizations AWS Organizations 관리 계정의 사용자만 조직의 지정을 변경할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 지정을 변경하려면 다음 단계를 따릅니다.

다른 Macie 관리자 계정을 지정하려면

1. AWS Organizations 관리 계정을 AWS Management Console 사용하여 로그인합니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 지정을 변경할 지역을 선택합니다.
3. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
4. 현재 리전의 관리 계정에 대해 Macie가 활성화되어 있는지 여부에 따라 다음 중 하나를 수행합니다.
   - Macie가 활성화되지 않은 경우 시작 페이지에서 시작하기를 선택합니다.
   - Macie가 활성화된 경우 탐색 창에서 설정을 선택합니다.
5. 위임된 관리자에서 제거를 선택합니다. 지정을 변경하려면 먼저 현재 지정을 제거해야 합니다.
6. 현재 지정을 제거할 것인지 확인합니다.

7. 위임된 관리자 아래에 조직의 새 Macie 관리자 AWS 계정 계정으로 지정할 12자리 계정 ID를 입력합니다.
8. 위임을 선택합니다.

Macie와 AWS Organizations를 통합하려는 각각의 추가 리전에 대해 이전 단계를 반복합니다.

API

프로그래밍 방식으로 지정을 변경하려면 Amazon Macie API의 두 가지 작업과 API의 AWS Organizations 한 가지 작업을 사용합니다. 이는 새 지정을 제출하기 AWS Organizations 전에 Macie와 두 곳 모두에서 현재 지정을 제거해야 하기 때문입니다.

현재 지정을 제거하려면:

1. Macie API의 DisableOrganizationAdminAccount작업을 사용하십시오. 필수 `adminAccountId` 매개 변수에는 현재 조직의 Macie 관리자 계정으로 지정된 계정의 12자리 계정 ID를 지정하십시오. AWS 계정
2. API DeregisterDelegatedAdministrator작업을 사용하십시오. AWS Organizations `AccountId` 파라미터의 경우 조직의 Macie 관리자 계정으로 지정된 계정의 12자리 계정 ID를 지정합니다. 이 값은 이전 Macie 요청에서 지정한 계정 ID와 일치해야 합니다. `ServicePrincipal` 파라미터에 Macie 서비스 주체(`macie.amazonaws.com`)를 지정하세요.

현재 지정을 제거한 후에는 Macie API의 EnableOrganizationAdminAccount작업을 사용하여 새 지정을 제출하십시오. 필수 `adminAccountId` 매개 변수에 대해 조직의 새 Macie 관리자 계정으로 지정할 12자리 계정 ID를 지정하십시오. AWS 계정

를 사용하여 지정을 변경하려면 Macie API의 disable-organization-admin-account명령과 API의 deregister-delegated-administrator명령을 실행합니다. AWS CLI AWS Organizations 이 명령은 각각 Macie와 AWS Organizations의 현재 지정을 제거합니다. `admin-account-id`및 `account-id` 매개 변수의 경우 AWS 계정 제거하려는 12자리 계정 ID를 현재 Macie 관리자 계정으로 지정합니다. `region` 파라미터를 사용하여 제거에 적용할 리전을 지정합니다. 예:

```
C:\> aws macie2 disable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333 && aws organizations deregister-delegated-administrator --
region us-east-1 --account-id 111122223333 --service-principal macie.amazonaws.com
```

위치:

- *`us-east-1`*은 제거가 적용되는 리전, 즉 미국 동부(버지니아 북부) 리전을 나타냅니다.

- *111122223333*은 Macie 관리자 계정으로서 제거할 계정의 계정 ID입니다.
- `macie.amazonaws.com`은(는) Macie 서비스 보안 주체입니다.

현재 지정을 제거한 후에는 Macie API의 enable-organization-admin-account명령을 실행하여 새 지정을 제출하십시오. `admin-account-id`매개 변수에 대해 조직의 새 Macie 관리자 AWS 계정 계정으로 지정할 12자리 계정 ID를 지정합니다. `region` 파라미터를 사용하여 지정이 적용되는 리전을 지정합니다. 예:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 444455556666
```

여기서 *us-east-1*은 지정이 적용되는 리전(미국 동부(버지니아 북부) 리전)이고 *444455556666*은 새 Macie 관리자 계정으로 지정할 계정의 계정 ID입니다.

AWS Organizations와 Amazon Macie의 통합 비활성화

AWS Organizations 조직이 Amazon Macie와 통합된 후에는 AWS Organizations 관리 계정이 통합을 비활성화할 수 있습니다. AWS Organizations 관리 계정 사용자는 Macie in에 대한 신뢰할 수 있는 서비스 액세스를 비활성화하여 이 작업을 수행할 수 있습니다. AWS Organizations

Macie에 대한 신뢰할 수 있는 서비스 액세스를 비활성화하면 다음과 같은 상황이 발생합니다.

- Macie는 에서 신뢰할 수 있는 서비스로서의 지위를 잃습니다. AWS Organizations
- 조직의 Macie 관리자 계정은 모든 AWS 리전에서 모든 Macie 멤버 계정의 모든 Macie 설정, 데이터 및 리소스에 대한 액세스 권한을 모두 잃게 됩니다.
- 모든 Macie 멤버 계정은 독립형 Macie 계정이 됩니다. Macie가 하나 이상의 리전에서 멤버 계정에 대해 활성화된 경우, Macie는 해당 리전에서 해당 계정을 계속 사용할 수 있습니다. 하지만 계정은 더 이상 어떤 리전의 Macie 관리자 계정과도 연결되지 않습니다. 또한 해당 계정은 Macie가 계정에 대해 민감한 데이터를 자동으로 검색하는 동안 생성하여 직접 제공한 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다.

신뢰할 수 있는 서비스 액세스를 비활성화한 결과에 대한 자세한 내용은 사용 AWS Organizations 설명서의 다른 AWS OrganizationsAWS 서비스사람과 함께 사용을 참조하십시오.

Macie에 대한 신뢰할 수 있는 서비스를 비활성화하려면

신뢰할 수 있는 서비스 액세스를 비활성화하려면 AWS Organizations 콘솔 또는 AWS Organizations API를 사용할 수 있습니다. AWS Organizations 관리 계정의 사용자만 Macie에 대한 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다. 필요한 권한에 대한 자세한 내용은 AWS Organizations 사용 설명서의 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한을 참조하세요.

신뢰할 수 있는 서비스 액세스를 비활성화하기 전에 필요에 따라 조직의 위임된 Macie 관리자에게 문의하여 멤버 계정의 Macie를 일시 중단 또는 비활성화하고 해당 계정의 Macie 리소스를 정리할 수도 있습니다.

Console

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면 다음 단계를 따르십시오.

신뢰할 수 있는 서비스를 비활성화하려면

1. AWS Organizations 관리 계정을 AWS Management Console 사용하여 로그인합니다.
2. https://console.aws.amazon.com/organizations/ 에서 AWS Organizations 콘솔을 엽니다.
3. 탐색 창에서 서비스를 선택합니다.
4. 통합 서비스에서 Amazon Macie를 선택합니다.
5. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 신뢰할 수 있는 액세스를 비활성화할지 확인합니다.

API

신뢰할 수 있는 서비스 액세스를 프로그래밍 방식으로 비활성화하려면 AWS Organizations API 비활성화 AWSServiceAccess 작업을 사용하십시오. `ServicePrincipal` 파라미터에 Macie 서비스 주체(`macie.amazonaws.com`)를 지정하세요.

AWS Command Line Interface (AWS CLI) 를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면 AWS Organizations API의 disable-aws-service-access명령을 실행합니다. `service-principal` 파라미터에 Macie 서비스 주체(`macie.amazonaws.com`)를 지정하세요. 예:

```
C:\> aws organizations disable-aws-service-access --service-principal
 macie.amazonaws.com
```

초대를 통한 Amazon Macie 계정 관리

Macie를 AWS Organizations와 통합하거나 멤버십 초대를 사용하는 이 두 가지 방법으로 여러 Amazon Macie 계정을 중앙에서 관리할 수 있습니다. 멤버십 초대를 사용하는 경우, 지정된 Macie 관리자가 최대 1,000개의 계정의 Macie를 관리할 수 있습니다. 또한 관리자는 Amazon Simple Storage Service(S3) 인벤토리 데이터에 액세스하여 계정이 소유하고 있는 S3 버킷에서 민감한 데이터를 검색할 수 있습니다. 관리자가 수행할 수 있는 작업에 대한 자세한 내용은 Amazon Macie 관리자 및 멤버 계정 간의 관계 이해 섹션을 참조하세요.

초대 기반 조직에서는 Macie에서 회원 초대를 보내고 수락하여 Macie 계정을 서로 연결할 수 있습니다. 초대를 보내고 다른 계정에서 초대를 수락하면 다른 계정의 Macie 관리자가 되고 다른 계정은 조직의 멤버 계정이 됩니다. 초대를 받고 수락하면 해당 계정은 멤버 계정이 되며 Macie 관리자는 계정의 특정 Macie 설정, 데이터 및 리소스에 액세스할 수 있습니다.

> **Tip**
>
> Macie에서 초대 기반 조직을 만든 경우, 나중에 AWS Organizations을 대신 사용하도록 전환할 수 있습니다. 두 가지 방법을 동시에 사용하여 여러 Macie 계정을 관리할 수도 있습니다. 예를 들어 AWS 환경에 테스트 계정이 포함된 경우, AWS Organizations에서 해당 계정을 조직에서 제외하고 초대를 통해 별도로 관리할 수 있습니다.

이 섹션의 주제에서는 초대 기반 조직을 만들고 참여하는 방법과 조직에 대한 다양한 관리 태스크를 수행하는 방법을 설명합니다.

주제

- Amazon Macie의 초대 기반 조직에 대한 고려 사항 및 권장 사항
- Amazon Macie에서 초대 기반 조직 생성 및 관리
- 초대 기반 조직의 Amazon Macie 계정 검토
- 초대 기반 조직을 위한 다른 Amazon Macie 관리자 계정 지정
- Amazon Macie에서 초대 기반 조직 관리

Amazon Macie의 초대 기반 조직에 대한 고려 사항 및 권장 사항

Amazon Macie에서 초대 기반 조직을 만들거나 관리를 시작하기 전에 다음 요구 사항 및 권장 사항을 고려하십시오. Macie 관리자 계정과 멤버 계정 간 관계를 이해해야 합니다.

주제

Macie 관리자 계정 선택

조직의 Macie 관리자 계정으로 사용할 계정을 결정할 때는 다음 사항을 고려하십시오.

- 조직은 하나의 Macie 관리자 계정만 보유할 수 있습니다.
- 계정은 Macie 관리자 계정이면서 동시에 멤버 계정일 수 없습니다.
- Macie는 리전 서비스입니다. 즉, Macie 관리자 계정과 구성원 계정 간의 연결은 지역적입니다. 즉, 초대를 보내고 수락한 계정에서만 연결이 존재합니다. AWS 리전 예를 들어, Macie 관리자가 미국 동부(버지니아 북부) 리전에서 초대를 보냈고 해당 초대가 수락된 경우 Macie 관리자는 해당 리전에 있는 멤버 계정만 관리할 수 있습니다.
- 여러 AWS 리전 Macie 계정을 중앙에서 관리하려면 Macie 관리자는 조직에서 현재 Macie를 사용하거나 사용할 계획이 있는 각 지역에 로그인하여 각 지역의 적절한 계정으로 초대장을 보내야 합니다. 현재 Macie를 사용할 수 있는 모든 리전 목록은 AWS 일반 참조의 Amazon Macie 및 엔드포인트 및 할당량을 참조하세요.
- 멤버 계정은 한 번에 하나의 Macie 관리자 계정만 연결할 수 있습니다. 여러 리전의 조직에서 Macie를 사용하는 경우 Macie 관리자 계정이 모든 리전에서 동일해야 함을 의미합니다. 단, 관리자 계정과 멤버 계정은 각 리전에서 별도로 초대를 보내고 수락해야 합니다.

Macie 관리자의 AWS 계정 계정이 일시 중지, 격리 또는 폐쇄된 경우 연결된 모든 회원 계정이 자동으로 구성원 계정으로 제거되지만 Macie는 해당 계정에 계속 활성화됩니다. 계정은 독립형 Macie 계정이 됩니다. 회원 계정에 민감한 데이터 자동 검색이 활성화된 경우 해당 계정에서는 비활성화됩니다. 또한 이렇게 하면 Macie가 계정에 대한 자동 검색을 수행하는 동안 생성하고 직접 제공한 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다. 30일이 지나면 이 데이터는 만료되며 Macie는 이 데이터를 영구 삭제합니다. 만료되기 전에 데이터에 대한 액세스를 복원하려면 Macie 관리자의 AWS 계정계정을 복원한 다음 해당 계정을 사용하여 조직을 다시 만들고 구성하십시오.

초대장 발송 및 Macie 멤버 계정 관리

초대 기반 조직의 Macie 관리자는 초대장을 보내고 조직의 계정을 관리할 때 다음 사항에 주의해야 합니다.

- 초대를 보내면 관련 데이터가 다른 사람에게 전송될 수 있습니다. AWS 리전이는 Macie가 미국 동부(버지니아 북부) 리전에서만 운영되는 이메일 인증 서비스를 사용하여 수신 계정의 이메일 주소를 확인하기 때문입니다.
- Macie를 활성화하지 않은 계정을 포함하여 활성 AWS 계정상태인 모든 계정에 초대를 보낼 수 있습니다. 하지만 초대를 수락하거나 거절하려면 초대를 받은 계정에서 초대를 보낸 리전에서 Macie를 활성화해야 합니다.
- Macie 관리자 계정은 각 AWS 리전에서 1,000개 이하의 계정과 연결할 수 있습니다. 여기에는 아직 초대에 응답하지 않은 계정도 포함됩니다. 계정이 이 할당량을 충족하는 경우 필요한 수의 관련 계정을 제거하거나, 필요한 수만큼 초대 거절을 받거나 이 둘을 함께 받을 때까지 계정을 추가하거나 초대할 수 없습니다.

  현재 계정에 연결된 계정 수를 확인하려면 Amazon Macie 콘솔의 계정 페이지 또는 Amazon Macie API의 ListMembers작동을 사용할 수 있습니다. 자세한 정보는 초대 기반 조직의 Amazon Macie 계정 검토을 참조하세요.
- 멤버 계정은 한 번에 하나의 Macie 관리자 계정만 연결할 수 있습니다. 즉, 계정이 이미 다른 Macie 관리자 계정과 연결되어 있는 경우 초대를 수락할 수 없습니다. 먼저 계정을 현재 Macie 관리자 계정에서 연결을 해제해야 합니다.
- 초대 기반 조직에서는 멤버 계정은 Macie 관리자 계정과 언제든지 연결을 해제할 수 있습니다. 이 경우 Macie는 해당 계정을 계속 사용할 수 있지만 계정은 독립형 Macie 계정이 됩니다. Macie는 멤버 계정이 관리자 계정과 연결이 끊어져도 알림을 보내지 않습니다. 하지만 해당 계정은 계정 인벤토리에 계속 표시되며 멤버 탈퇴로 유지됩니다.
- 조직에서 구성원 계정을 제거해도 Macie는 해당 계정을 계속 사용할 수 있습니다. 계정은 독립형 Macie 계정이 됩니다.

멤버십 초대 응답 및 관리

초대를 받는 사람 또는 초대 기반 조직의 멤버는 받은 초대에 응답하고 관리할 때 다음 사항을 주의합니다.

- 초대장을 보내기 전에 Macie 관리자 계정과 멤버 계정 간 관계를 이해해야 합니다.
- 내 계정은 한 번에 하나의 Macie 관리자 계정만 연결할 수 있습니다. 초대를 수락한 후 초대를 통해 다른 조직에 가입하려면 먼저 현재 AWS Organizations Macie 관리자 계정에서 계정 연결을 끊어야 합니다. 이후에 다른 조직에 가입할 수 있습니다.
- 초대를 수락하거나 거절하려면 초대장을 보낸 AWS 리전 에서 Macie를 활성화해야 합니다. 초대장을 보낸 계정에서는 해당 리전에서 Macie를 활성화할 수 없습니다. 초대를 거절하는 것은 선택 사항입니다. 초대를 거절하는 경우, 초대를 거절한 후 해당 리전에서 Macie를 비활성화할 수 있습니다.

- Macie 관리자는 멤버 계정 초대를 수락할 수 없으며, 하나의 계정은 동시에 Macie 관리자와 멤버 계정이 될 수 없습니다. 멤버 계정이 되려면 먼저 현재 조직에서 모든 멤버 계정을 제거하여 모든 멤버 계정과 연결 해제해야 합니다.
- Macie는 리전 서비스입니다. 초대를 수락하면 사용자 계정과 Macie 관리자 계정 간의 연결은 지역적이므로 초대를 보내고 수락한 AWS 리전 계정에서만 연결됩니다.
- 여러 리전에서 Macie를 사용하는 경우 사용자 계정에 대한 Macie 관리자 계정은 모든 리전에서 동일해야 합니다. 하지만 Macie 관리자는 각 리전에서 개별적으로 초대를 보내야 하며 사용자는 각 리전에서 개별적으로 초대를 수락해야 합니다.
- 언제든지 Macie 관리자 계정과 연결을 해제할 수 있습니다. 마찬가지로 Macie 관리자는 언제든지 조직에서 사용자 계정을 제거할 수 있습니다. 둘 중 하나가 발생하는 경우:
  - Macie는 계속해서 해당 계정을 사용할 수 있습니다. 계정은 독립형 Macie 계정이 됩니다.
  - 계정에 대해 민감한 데이터 자동 검색 기능이 활성화되어 있으면 비활성화됩니다. 또한 이렇게 하면 Macie가 사용자 계정에 대한 자동 검색을 수행하는 동안 생성하고 직접 제공한 기존 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다. 계정에 대한 자동 검색을 다시 활성화할 수 있습니다. 하지만 이렇게 해도 기존 데이터에 대한 액세스는 복원되지 않습니다. 대신 Macie는 계정에 대한 자동 검색을 수행하는 동안 새 데이터를 생성하고 유지합니다.

AWS Organizations으로 전환

Macie에서 초대 기반 조직을 만든 후 대신 사용하도록 전환할 수 있습니다. AWS Organizations 전환을 간소화하려면 기존의 초대 기반 관리자 계정을 AWS Organizations에서 조직의 Macie 관리자 계정으로 지정하는 것이 좋습니다.

이렇게 하면 현재 연결된 모든 멤버 계정이 계속 유지됩니다. 멤버 계정이 의 조직에 속해 있는 경우 계정 연결은 초대를 통해서에서 Macie의 Via로 자동 변경됩니다. AWS Organizations AWS Organizations 멤버 계정이 AWS Organizations에서 조직의 일부가 아닌 경우 해당 계정 연결은 초대로 계속 유지됩니다. 두 경우 모두 계정이 멤버 계정으로 Macie 관리자 계정과 계속 연결됩니다.

멤버 계정은 한 번에 하나의 Macie 관리자 계정만 연결할 수 있으므로 이러한 접근을 추천합니다. 에서 AWS Organizations조직의 Macie 관리자 계정으로 다른 계정을 지정하는 경우 지정된 관리자는 초대를 통해 다른 Macie 관리자 계정에 이미 연결된 계정을 관리할 수 없습니다. 각 멤버 계정은 먼저 초대 기반 현재 관리자 계정과 연결을 끊어야 합니다. 그래야만 조직의 Macie 관리자가 AWS Organizations 조직에 구성원 계정을 추가하고 계정에 대한 Macie를 관리하기 시작할 수 있습니다.

Macie를 Macie와 AWS Organizations 통합하고 Macie에서 조직을 구성한 후 필요에 따라 조직에 다른 Macie 관리자 계정을 지정할 수 있습니다. 또한 계속해서 초대를 사용하여 AWS Organizations에서 조직에 속하지 않은 멤버 계정을 연결하고 관리할 수도 있습니다.

Macie와 통합하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS OrganizationsAWS Organizations를 통한 Amazon Macie 계정 관리

Amazon Macie에서 초대 기반 조직 생성 및 관리

Amazon Macie에서 초대 기반 조직을 만들려면 먼저 조직의 Macie 관리자 계정으로 사용할 계정을 정합니다. 그런 다음 해당 계정을 사용하여 구성원 계정을 추가합니다. 다른 AWS 계정사람에게 멤버십 초대를 보내고 해당 계정을 현재 Macie 회원 계정으로 기관에 가입하도록 초대합니다. AWS 리전여러 지역에 조직을 만들려면 다른 계정에서 현재 Macie를 사용 중이거나 사용할 계획이 있는 각 지역에서 멤버십 초대장을 보내십시오.

계정에서 초대를 수락하면 해당 계정은 해당 리전의 Macie 관리자 계정과 연결된 Macie 멤버 계정이 됩니다. 그러면 Macie 관리자 계정으로 해당 리전의 멤버 계정에 대한 Macie 설정, 데이터 및 리소스에 액세스할 수 있습니다.

초대 기반 조직의 Macie 관리자는 멤버 계정에 대한 Amazon Simple Storage Service(S3) 인벤토리 데이터 및 정책 결과를 검토할 수 있습니다. 또한 민감한 데이터 자동 검색을 활성화하고 민감한 데이터 검색 작업을 실행하여 구성원 계정이 소유한 S3 버킷의 민감한 데이터를 탐지할 수 있습니다. 수행할 수 있는 작업의 세부 목록은 Amazon Macie 관리자 및 멤버 계정 간의 관계 이해(을) 참조하십시오.

기본적으로 Macie는 조직 전체의 관련 데이터 및 리소스에 대한 가시성을 제공합니다. 또한 드릴다운하여 조직의 개별 계정에 대한 데이터와 리소스를 검토할 수도 있습니다. 예를 들어 요약 대시보드를 사용하여 조직의 Amazon S3 보안 상태를 평가하는 경우 계정별로 데이터를 필터링할 수 있습니다. 마찬가지로 예상 사용 비용을 모니터링하는 경우 개별 멤버 계정의 예상 비용 내역에 액세스할 수 있습니다.

관리자 계정과 멤버 계정에 공통으로 적용되는 작업 외에도 조직의 다양한 관리 작업을 중앙에서 수행할 수 있습니다. 이러한 작업을 수행하기 전에 Macie에서 초대 기반 조직을 관리하기 위한 고려 사항 및 권장 사항을 검토하는 것이 좋습니다.

Tasks

- 초대 기반 조직에 Amazon Macie 멤버 계정 추가
- 초대 기반 조직의 멤버 계정에 대한 Amazon Macie 일시 중지
- 초대 기반 조직에서 Amazon Macie 멤버 계정 제거
- 다른 계정과 연결 삭제

초대 기반 조직에 Amazon Macie 멤버 계정 추가

초대 기반 조직의 Macie 관리자는 다음 두 가지 기본 단계를 수행하여 조직에 멤버 계정을 추가할 수 있습니다.

1. Macie의 계정 인벤토리에 계정을 추가합니다. 이렇게 하면 계정이 관리자 계정과 연결됩니다.
2. 계정에 멤버십 초대장을 보냅니다.

다른 계정으로부터 온 초대를 수락하면 사용자 계정이 멤버 계정이 됩니다.

1단계: 계정 추가

계정 인벤토리에 하나 이상의 계정을 추가할 때 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하면 됩니다.

Console

Amazon Macie 콘솔을 사용하면 한 번에 하나의 계정을 추가하거나 쉼표로 구분된 값(CSV) 파일을 업로드하여 여러 계정을 동시에 추가할 수 있습니다. 콘솔을 사용하여 하나 이상의 계정을 추가하려면 다음 단계를 따릅니다.

하나의 계정을 추가하는 방법

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 계정을 추가할 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 현재 계정과 연결된 계정 테이블이 표시됩니다.
4. [Add accounts]를 선택합니다.
5. 계정 세부 정보 입력 섹션에서 계정 추가를 선택합니다. 뒤이어 다음과 같이 하십시오.
   - 계정 ID에 AWS 계정 추가할 12자리 계정 ID를 입력합니다.
   - 이메일 주소에 AWS 계정 추가할 이메일 주소를 입력합니다.
6. 추가를 선택합니다.
7. 페이지 하단에서 다음(Next)을 선택합니다.

Macie가 계정 인벤토리에 계정을 추가합니다. 계정 유형은 초대이며, 상태는 생성됨입니다. 계정을 추가하려는 각 리전마다 앞의 단계를 반복합니다.

여러 계정을 추가하는 방법

1. 텍스트 편집기를 사용하여 다음과 같이 CSV 파일을 생성합니다.

   a. 파일의 첫 번째 줄에 `Account ID,Email` 헤더를 추가합니다.

   b. 각 계정에 대해 AWS 계정 추가할 12자리 계정 ID와 계정의 이메일 주소가 포함된 새 줄을 만드십시오. 항목을 쉼표로 구분합니다. 예: `111111111111,janedoe@example.com`

      이메일 주소는 AWS 계정와 연결된 이메일 주소와 일치해야 합니다.

   c. 세 개의 계정에 대한 필수 헤더와 정보가 포함된 다음 예시와 같이 파일 내용의 형식이 지정되었는지 확인합니다.

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

   d. 파일을 컴퓨터에 저장합니다.

2. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
3. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 계정을 추가할 지역을 선택합니다.
4. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 현재 계정과 연결된 계정 테이블이 표시됩니다.
5. [Add accounts]를 선택합니다.
6. 계정 세부 정보 입력 섹션에서 목록 업로드 (CSV) 를 선택합니다.
7. 검색을 선택한 다음 1단계에서 생성한 CSV 파일을 선택합니다.
8. [Add accounts]를 선택합니다.
9. 페이지 하단에서 다음(Next)을 선택합니다.

Macie의 계정 인벤토리에 계정을 추가합니다. 유형은 초대이며 상태는 생성됨으로 표시됩니다. 계정을 추가하려는 각 8개 리전마다 앞의 3단계를 반복합니다.

API

프로그래밍 방식으로 하나 이상의 계정을 추가하려면 Amazon Macie CreateMemberAPI의 작업을 사용하십시오. 요청을 제출할 때 지원되는 매개변수를 사용하여 추가할 각 AWS 계정 계정의 12자리 계정 ID와 이메일 주소를 지정합니다. 또한 요청이 적용되는 리전을 지정합니다. 다른 리전에 계정을 추가하려면 각 리전에서 요청을 제출합니다.

AWS Command Line Interface (AWS CLI)를 사용하여 계정을 추가하려면 create-member 명령을 실행합니다. region 파라미터를 사용하여 계정을 추가할 리전을 지정합니다. account 파라미터를 사용하여 추가할 각 AWS 계정 의 계정 ID와 이메일 주소를 지정합니다. 예:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"111111111111\",\"email\":\"janedoe@example.com\"}
```

여기서 *us-east-1*은 계정을 추가할 리전(미국 동부 (버지니아 북부) 리전)이고, account 파라미터는 추가할 계정의 계정 ID(*111111111111*) 및 이메일 주소(*janedoe@example.com*)를 지정합니다.

요청이 성공하면 Macie는 상태가 Created인 계정 인벤토리에 각 계정을 추가하고 다음과 비슷한 결과를 받게 됩니다.

```
{
    "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"
}
```

여기서 arn는 계정과 추가한 계정 간 연결을 위해 생성된 리소스의 Amazon 리소스 이름(ARN)입니다. 이 예에서 123456789012(은)는 연결을 생성한 계정의 계정 ID이고, 111111111111(은)는 추가된 계정의 계정 ID입니다.

2단계: 계정에 멤버십 초대장 보내기

계정 인벤토리에 계정을 추가한 후 해당 계정을 Macie 멤버 계정으로 조직에 가입하도록 초대할 수 있습니다. 이렇게 하려면 해당 계정으로 멤버십 초대장을 보내야 합니다. 초대를 보내면 계정에 Macie가 활성화된 경우 수신자 계정에 대한 계정 배지 및 알림이 Amazon Macie 콘솔에 표시됩니다. 또한 Macie는 해당 계정에 대한 AWS Health 이벤트를 생성합니다.

초대장을 보낼 때 Amazon Macie 콘솔을 사용하는지 또는 API를 사용하는지에 따라 Macie는 계정을 추가할 때 수신자 계정에 지정한 이메일 주소로도 초대장을 보냅니다. 이메일 메시지에는 해당 계정의 Macie 관리자가 되고 싶다는 메시지가 표시되며 여기에는 사용자 AWS 계정 와 수신자의 AWS 계정에 대한 계정 ID가 포함되어 있습니다. 또한 초대장에 액세스하는 방법도 설명되어 있습니다. 선택 사항으로 메시지에 사용자 지정 텍스트를 추가할 수 있습니다.

하나 이상의 계정에 멤버십 초대를 보낼 때 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하면 됩니다.

Console

Amazon Macie 콘솔을 사용하여 멤버십 초대장을 보내려면 다음 단계를 따르십시오.

멤버십 초대장을 보내는 방법

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 초대를 보낼 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 현재 계정과 연결된 계정 테이블이 표시됩니다.
4. 계정 표에서 초대장을 보내려는 각 계정의 체크박스를 선택합니다.

> **Tip**
>
> 표를 필터링하여 추가한 계정과 아직 초대를 보내지 않은 계정을 더 쉽게 구분할 수 있습니다. 이렇게 하려면 테이블 위의 필터 상자에 커서를 놓고 상태를 선택합니다. 그런 다음 상태 = 생성됨을 선택합니다.

5. 작업 메뉴에서 초대를 선택합니다.
6. (선택 사항) 메시지 상자에서 초대장이 포함된 이메일 메시지에 기재할 사용자 지정 텍스트를 입력합니다. 텍스트에는 영숫자 80자까지 입력할 수 있습니다.
7. [Invite]를 선택합니다.

추가로 초대장을 보내려면 각 추가 AWS 리전지역에서 이전 단계를 반복하세요.

초대장을 보내면 계정 인벤토리에 수신자 계정 상태가 이메일 확인 진행 중으로 변경됩니다. Macie가 계정의 이메일 주소를 확인하면 이후 계정 상태가 초대됨으로 변경됩니다. Macie가 주소를 확인하지 않으면 계정 상태가 이메일 확인 실패로 변경됩니다. 이 경우 계정 소유자에게 문의하여 올바른 이메일 주소를 확인합니다. 그런 다음 계정 간 연결을 삭제하고 다시 계정을 추가한 다음 다시 초대장을 보냅니다.

수신자가 초대를 수락하면 계정 인벤토리에서 수신자 계정 상태가 활성화됨으로 변경됩니다. 수신자가 초대를 거절하면 수신자의 계정은 내 계정에서 분리되고 계정 인벤토리에서 제거됩니다.

API

프로그래밍 방식으로 초대를 보내려면 Amazon CreateInvitationsMacie API의 작업을 사용하십시오. 요청을 제출할 때 지원되는 매개변수를 사용하여 초대를 AWS 계정 보낼 각 계정의 12자리 계정 ID를 지정하십시오. 계정 ID는 계정 인벤토리에 있는 계정의 계정 ID와 일치해야 합니다. 그렇지

않으면 오류가 발생합니다. 또한 초대장을 보낼 리전을 지정합니다. 추가 지역에 초대장을 보내려면 각 리전에서 이전 단계를 반복합니다.

요청에서 초대를 이메일 메시지로 보낼지 및 해당 메시지에 사용자 지정 텍스트를 기재할지 지정할 수 있습니다. 이메일 메시지를 보내도록 선택하면 Macie는 계정 인벤토리에 계정을 추가할 때 지정한 이메일 주소로 초대장을 보냅니다. 이메일 메시지로 초대장을 보내려면 `disableEmailNotification` 파라미터를 생략하거나 파라미터 값을 `false`로 설정합니다. (기본값은 `false`입니다.) 메시지에 사용자 지정 텍스트를 추가하려면 `message` 파라미터를 사용하여 추가할 텍스트를 지정합니다. 텍스트에는 영숫자 80자까지 입력할 수 있습니다.

를 사용하여 초대를 보내려면 create-invitations 명령을 실행합니다. AWS CLI `region` 파라미터를 사용하여 초대장을 보낼 리전을 지정합니다. `account-ids` 파라미터를 사용하여 초대장을 보낼 각 AWS 계정 의 계정 ID를 지정합니다. 예:

```
C:\> aws macie2 create-invitations --region us-east-1 --account-
ids=[\"111111111111\",\"222222222222\",\"333333333333\"]
```

여기서 *us-east-1*은 초대장을 보낼 리전(미국 동부(버지니아 북부) 리전)이고 `account-ids` 파라미터는 초대장을 보낼 세 계정의 계정 ID를 지정합니다. 이메일 메시지로도 초대장을 보내려면 `no-disable-email-notification` 파라미터를 포함하고 선택적으로 `message` 파라미터를 포함시켜 메시지에 추가할 사용자 지정 텍스트를 지정합니다.

초대장을 보내고 나면 각 수신자 계정의 상태가 `EmailVerificationInProgress`로 변경됩니다. Macie가 계정의 이메일 주소를 확인하면 이후 계정 상태가 `Invited`으로 변경됩니다. Macie가 주소를 확인하지 않으면 계정 상태가 `EmailVerificationFailed`로 변경됩니다. 이 경우 계정 소유자에게 문의하여 올바른 주소를 확인합니다. 그런 다음 계정 간 연결을 삭제하고 다시 계정을 추가한 다음 다시 초대장을 보냅니다.

수신자가 초대를 수락하면 계정 인벤토리에서 수신자 계정 상태가 `Enabled`으로 변경됩니다. 수신자가 초대를 거절하면 수신자의 계정은 내 계정에서 분리되고 계정 인벤토리에서 제거됩니다.

초대 기반 조직의 멤버 계정에 대한 Amazon Macie 일시 중지

조직의 Macie 관리자는 조직의 특정 개별 구성원 계정에서 Macie를 일시 중단할 수 있습니다. AWS 리전 단, 멤버 계정을 일시 중지한 후에는 해당 멤버 계정에 대해 Macie를 다시 활성화할 수 없습니다. 이후에는 해당 계정의 사용자만 계정에 대해 Macie를 다시 활성화할 수 있습니다.

멤버 계정에 대해 Macie를 정지하는 경우:

- Macie는 해당 리전에 있는 계정의 Amazon S3 데이터 액세스 권한을 상실하고, 해당 메타데이터 제공을 중단합니다.
- Macie는 리전에서 계정에 대한 모든 활동을 중지합니다. 여기에는 보안 및 액세스 제어를 위한 S3 버킷 모니터링, 민감한 데이터 자동 검색 수행, 현재 진행 중인 민감한 데이터 검색 작업 실행 등이 포함됩니다.
- Macie는 리전 내 계정에서 생성한 모든 민감한 데이터 검색 작업을 취소합니다. 취소된 작업은 다시 시작하거나 재개할 수 없습니다. 멤버 계정이 소유한 데이터를 분석하기 위해 작업을 생성한 경우 Macie는 해당 작업을 취소하지 않습니다. 대신 작업은 계정에서 소유한 리소스를 건너뜁니다.

계정이 일시 중지되는 동안 Macie는 해당 리전의 계정에 대한 Macie 세션 식별자, 설정 및 리소스를 유지합니다. 예를 들어 계정의 검색 결과는 그대로 유지되며 최대 90일 동안 영향을 받지 않습니다. 해당 리전에서 계정에 대해 Macie가 일시 중지된 동안에는 해당 리전에서 Macie 사용에 대해 계정에 요금이 청구되지 않습니다.

초대 기반 조직의 멤버 계정에 대해 Macie를 일시 중지하는 방법

초대 기반 조직의 멤버 계정에 대해 Macie를 일시 중지하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하면 됩니다.

Console

Amazon Macie 콘솔을 사용하여 멤버 계정의 Macie를 일시 중지하려면 다음 단계를 수행합니다.

멤버 계정에서 Macie를 일시 중지하는 방법

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 회원 계정에 대해 Macie를 일시 중단하려는 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 현재 계정과 연결된 계정 테이블이 표시됩니다.
4. 계정 테이블에서 일시 중지하려는 계정의 확인란을 선택합니다.
5. 작업 메뉴에서 Macie 일시 중지를 선택합니다.
6. 선택한 계정에 대해 Macie 일시 중지를 확인합니다.

일시 중지를 확인하면 계정 인벤토리에서 계정 상태가 중지됨(일시 중지됨)으로 변경됩니다.

Macie 계정을 이용 정지하려는 각 리전마다 앞의 단계를 반복합니다.

API

회원 계정의 Macie를 프로그래밍 방식으로 일시 중지하려면 Amazon Macie UpdateMemberSessionAPI의 작업을 사용하십시오. 요청을 제출할 때 `id` 파라미터를 사용하여 Macie를 일시 AWS 계정 중지하려는 12자리 계정 ID를 지정합니다. `status` 파라미터의 경우 Macie 계정의 새 상태를 `PAUSED`로 지정합니다. 또한 요청이 적용되는 리전을 지정합니다. 추가로 다른 리전에서 Macie를 일시 중지하려면 각 리전에 요청을 제출합니다.

멤버 계정의 계정 ID를 검색하려면 Amazon Macie API의 ListMembers작업을 사용할 수 있습니다. 이렇게 하려면 요청에 `onlyAssociated` 파라미터를 포함하여 결과를 필터링하는 것을 고려해 보십시오. 이 파라미터의 값을 `true`로 설정하면 Macie는 현재 관리자 계정의 멤버 계정인 계정에 대한 세부 정보만 제공하는 `members` 배열을 반환합니다.

를 사용하여 멤버 계정의 Macie를 일시 AWS CLI중지하려면 명령을 실행합니다. update-member-session `region` 파라미터를 사용하여 Macie를 일시 중지할 리전을 지정하고 `id` 파라미터를 사용하여 Macie를 일시 중지할 계정의 계정 ID를 지정합니다. `status` 파라미터에서 `PAUSED`를 지정합니다. 예:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

여기서 *us-east-1*은 Macie를 일시 중지할 리전(미국 동부 (버지니아 북부) 리전)이고, *123456789012*는 Macie를 일시 중지할 계정의 계정 ID이며, `PAUSED`은(는) 해당 계정에서 Macie의 새로운 상태입니다.

요청이 성공하면 Macie는 빈 응답을 반환하고 지정된 계정의 상태는 계정 인벤토리에서 `Paused`로 변경됩니다.

초대 기반 조직에서 Amazon Macie 멤버 계정 제거

멤버 계정의 관리자로서 조직에서 멤버 계정을 제거할 수 있습니다. Macie 관리자 계정에서 계정 연결을 해제하면 됩니다.

멤버 계정을 제거해도 Macie는 해당 계정에서 계속 활성화되어 있으며 계정 인벤토리에 계속 표시됩니다. 이전의 마스터 계정은 독립형 Macie 계정이 됩니다. 계정을 제거해도 Macie는 계정 소유자에게 알림을 보내지 않습니다. 따라서 계정 소유자에게 연락하여 계정의 설정 및 리소스 관리하도록 하는 것이 좋습니다.

멤버 계정을 제거하면 해당 계정의 모든 Macie 설정, 리소스 및 데이터에 액세스할 수 없게 됩니다. 여기에는 계정이 소유한 S3 버킷에 대한 정책 결과 및 메타데이터도 포함됩니다. 또한 더 이상 Macie를

사용하여 계정이 소유하고 있는 S3 버킷의 민감한 데이터를 검색할 수 없습니다. 이를 위해 민감한 데이터 검색 작업을 이미 생성한 경우 해당 작업은 계정이 소유한 버킷을 건너뛰게 됩니다. 계정에 대해 민감한 데이터 자동 검색 기능을 활성화한 경우 계정 및 계정 모두 계정 자동 검색을 수행하는 동안 Macie가 생성하고 직접 제공한 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다.

멤버 계정을 제거한 후에는 해당 계정으로 새 초대장을 보내 조직에 다시 추가할 수 있습니다. 계정이 새 초대를 수락하고 30일 이내에 계정에 대한 민감한 데이터 자동 검색을 활성화하면 계정에 대한 자동 검색을 수행하는 동안 Macie가 이전에 생성하여 직접 제공한 데이터 및 정보에도 다시 액세스할 수 있습니다.

회원 계정을 제거했다가 다시 추가할 계획이 없는 경우 계정 인벤토리에서 완전히 제거할 수 있습니다. 자세한 방법은 다른 계정과 연결 삭제(을)를 참조하세요.

초대 기반 조직에서 멤버 계정을 제거하는 방법

조직에서 멤버 계정을 제거할 때 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하면 됩니다.

Console

Amazon Macie 콘솔을 사용하여 멤버 계정을 제거하려면 다음 단계를 수행합니다.

멤버 계정 제거

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 회원 계정을 제거하려는 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 현재 계정과 연결된 계정 테이블이 표시됩니다.
4. 계정 테이블에서 제거하려는 계정의 확인란을 선택합니다.
5. 작업 메뉴에서 계정 연결 해제를 선택합니다.
6. 선택한 계정을 멤버 계정에서 제거할 것인지 확인합니다.

선택을 확인하면 계정 인벤토리에서 계정 상태가 제거됨(연결 해제됨)으로 변경됩니다.

멤버 계정을 제거할 추가적인 각 리전마다 이전 단계를 반복합니다.

API

프로그래밍 방식으로 멤버 계정을 제거하려면 Amazon Macie DisassociateMemberAPI의 작업을 사용하십시오. 요청을 제출할 때 `id` 파라미터를 사용하여 제거할 회원 계정의 12자리 AWS 계정 ID를 지정합니다. 또한 요청이 적용되는 리전을 지정합니다. 다른 리전에 계정을 삭제하려면 각 리전에서 요청을 제출합니다.

제거할 계정의 계정 ID를 검색하려면 Amazon Macie API의 ListMembers작업을 사용할 수 있습니다. 이렇게 하려면 요청에 `onlyAssociated` 파라미터를 포함하여 결과를 필터링하는 것을 고려해 보십시오. 이 파라미터의 값을 `true`로 설정하면 Macie는 현재 사용자 계정의 멤버 계정인 계정에 대한 세부 정보만 제공하는 `members` 배열을 반환합니다.

를 사용하여 멤버 계정을 제거하려면 disassociate-member 명령을 실행합니다. AWS CLI`region` 파라미터를 사용하여 계정을 제거할 리전을 지정합니다. `id` 파라미터를 사용하여 계정을 제거할 계정 ID를 지정합니다. 예:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

여기서 *us-east-1*은 계정을 제거할 리전(미국 동부 (버지니아 북부) 리전)이고 *123456789012*는 제거할 계정의 계정 ID입니다.

요청이 성공하면 Macie는 빈 응답을 반환하고 지정된 계정의 상태는 계정 인벤토리에서 `Removed`로 변경됩니다.

다른 계정과 연결 삭제

계정 인벤토리에 계정을 추가한 후 내 계정과 다른 계정 간 연결을 삭제할 수 있습니다. 다음을 제외하고 인벤토리의 모든 계정에 대해 이 작업을 수행할 수 있습니다.

- 사용자 조직의 일부인 AWS Organizations계정입니다. 이러한 유형의 연결은 Macie를 통해 제어되지 않습니다. AWS Organizations
- 조직에 가입하라는 Macie 멤버십 초대장을 수락한 멤버 계정입니다. 이러한 경우에는 먼저 멤버 계정을 제거해야 연결을 삭제할 수 있습니다.

연결을 삭제하면 Macie는 계정 인벤토리에서 해당 계정을 제거합니다. 이후에 연결을 복원하려면 완전히 새 계정인 것처럼 계정을 다시 추가해야 합니다.

다른 계정과 연결을 삭제하는 방법

내 계정과 다른 계정 간 연결을 삭제할 때 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하면 됩니다.

Console

Amazon Macie 콘솔을 사용하여 다른 계정과의 연결을 삭제하려면 다음 단계를 수행합니다.

연결을 삭제하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 연결을 삭제하려는 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 현재 계정과 연결된 계정 테이블이 표시됩니다.
4. 계정 표에서 연결을 삭제하려는 계정의 체크박스를 선택합니다.
5. [Actions] 메뉴에서 [Delete]를 선택합니다.
6. 선택한 연결을 삭제할 것인지 확인합니다.

연결을 삭제하려는 각 추가 리전마다 앞의 단계를 반복합니다.

API

프로그래밍 방식으로 다른 계정과의 연결을 삭제하려면 Amazon DeleteMemberMacie API의 작업을 사용하십시오. 요청을 제출할 때 `id` 파라미터를 사용하여 연결을 삭제할 12자리 계정 ID를 지정하십시오. AWS 계정 또한 요청이 적용되는 리전을 지정합니다. 추가로 다른 리전에서 연결을 삭제하려면 각 리전에 요청을 제출합니다.

계정의 계정 ID를 검색하려면 Amazon Macie API의 ListMembers작업을 사용할 수 있습니다. 이 경우 요청에 `onlyAssociated` 파라미터를 포함하고 파라미터 값을 `false`로 설정합니다. 작업이 성공하면 Macie는 현재 멤버 계정이 아닌 계정을 포함하여 내 계정에 연결된 모든 계정에 대한 세부 정보를 제공하는 `members` 배열을 반환합니다.

를 사용하여 다른 계정과의 연결을 삭제하려면 delete-member 명령을 실행합니다. AWS CLI`region` 파라미터를 사용하여 Macie를 삭제할 리전을 지정하고 `id` 파라미터를 사용하여 Macie를 연결을 삭제할 계정의 계정 ID를 지정합니다. 예:

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

여기서 *us-east-1*은 계정을 제거할 리전(미국 동부 (버지니아 북부) 리전)이고 *123456789012*는 계정 ID입니다.

요청이 성공하면 Macie는 빈 응답을 반환하고 내 계정과 다른 계정 간 연결이 삭제됩니다. 이전에 연결된 계정은 계정 인벤토리에서 제거됩니다.

초대 기반 조직의 Amazon Macie 계정 검토

조직의 계정을 관리할 수 있도록 Amazon Macie는 사용자가 Macie를 사용하는 각 AWS 리전 계정에서 Macie 계정과 연결된 계정의 인벤토리를 제공합니다. 조직의 Macie 관리자는 이 인벤토리를 사용하여 조직의 계정 통계 및 세부 정보를 검토할 수 있습니다. 또한 이를 사용하여 구성원 계정에 대한 특정 관리 작업을 수행하고 계정과 다른 계정 간의 관계 상태를 관리할 수 있습니다.

초대 기반 조직의 계정 검토

조직에서 계정을 검토할 때 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하면 됩니다.

Console

Amazon Macie 콘솔을 사용하여 조직의 계정을 검토하려면 다음 단계를 수행합니다.

조직의 계정 검토

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 조직의 계정을 검토할 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다.

계정 페이지가 열리고 집계된 통계와 현재 AWS 리전에 Macie 계정과 연결된 계정 표가 표시됩니다.

계정 페이지 상단에는 다음과 같은 집계된 통계가 표시됩니다.

를 통해 AWS Organizations

에서 AWS Organizations조직의 Macie 관리자인 경우 Active는 현재 조직의 Macie 회원 계정을 통해 사용자 AWS Organizations 계정과 연결되어 있는 총 계정 수를 보고합니다. Macie는 이러한 계정에서 활성화되어 있으며, 해당 계정의 Macie 관리자입니다.

모든 보고서는 현재 Macie 회원 계정이 아닌 계정을 포함하여 사용자 계정과 연결된 총 계정 수를 보고합니다. AWS Organizations

초대장별

활성는 초대 기반 조직에 현재 연결된 총 Macie 멤버 계정 수를 보고합니다. Macie는 이러한 계정에서 활성화되어 있으며, 해당 계정이 멤버십 초대를 수락했으므로 귀하는 해당 계정의 Macie 관리자입니다.

모두은 초대에 응답하지 않은 계정을 포함하여 Macie 초대를 통해 내 계정에 연결된 총 계정 수를 보고합니다.

활성/모두

활성 보고서는 초대를 통해 AWS Organizations 또는 초대를 통해 현재 사용자 계정의 Macie 회원 계정인 총 계정 수를 보고합니다. Macie는 이러한 계정에서 활성화되어 있으며, 해당 계정의 Macie 관리자입니다.

모든 보고서는 초대를 통해 AWS Organizations 또는 초대를 통해 계정에 연결된 총 계정 수를 보고합니다. 여기에는 Macie 멤버십 초대를 수락하지 않은 계정도 포함됩니다. 여기에는 현재 Macie 회원 계정이 아닌 계정을 통해 사용자 AWS Organizations 계정과 연결된 계정도 포함됩니다.

표에서 현재 리전에 있는 각 계정에 대한 세부 정보를 확인할 수 있습니다. 이 표에는 Macie 초대를 통해 또는 Macie 초대를 통해 Macie 계정과 연결된 모든 계정이 포함되어 있습니다. AWS Organizations

계정 ID

AWS 계정의 계정 ID 및 이메일 주소입니다.

이름

AWS 계정의 계정 이름입니다. 초대를 통해 내 계정에 연결된 계정의 경우 이 값은 일반적으로 N/A입니다.

Type

초대 또는 AWS Organizations를 통해 내 계정과 계정을 연결하는 방법입니다.

상태

사용자 계정과 계정 간의 관계 상태입니다. 초대 기반 조직의 계정(유형이 초대)의 경우 가능한 값은 다음과 같습니다.

- 계정이 일시 중지됨 - AWS 계정 는 일시 중지되어 있습니다.

- 생성됨(초대) - 계정을 추가했지만 아직 멤버십 초대장을 보내지 않았습니다.
- 이메일 인증 실패 - 계정으로 멤버십 초대장을 보내려고 했지만 계정에 지정한 이메일 주소가 유효하지 않습니다.
- 이메일 인증 진행 중 - 계정으로 멤버십 초대장을 보냈으며 Macie가 요청을 처리 중입니다.
- 활성화됨 - 계정은 멤버 계정입니다. Macie는 이러한 계정에서 활성화되어 있으며, 해당 계정의 Macie 관리자입니다.
- 초대됨 - 계정으로 멤버십 초대장을 보냈지만 계정에서 초대에 응답하지 않았습니다.
- 멤버 탈퇴 - 계정이 이전 멤버 계정입니다. 하지만 해당 계정은 계정에서 연결을 해제하여 조직에서 탈퇴했습니다.
- 중지됨 (일시 중지) - 멤버 계정이지만 Macie는 현재 해당 계정에서 일시 중지 상태입니다.
- 리전 비활성화됨 - AWS 계정에서 현재 리전이 비활성화되어 있습니다.
- 제거됨 (연결 해제) - 계정이 이전에 멤버 계정이었습니다. 하지만 계정에서 연결을 해제하여 해당 계정을 멤버 계정에서 제거했습니다.

마지막 상태 업데이트

사용자 또는 관련 계정이 가장 최근에 계정 간 관계에 영향을 미치는 작업을 수행한 시점입니다.

민감한 데이터 자동 검색

계정에 대해 민감한 데이터 자동 검색이 현재 활성화되어 있는지 또는 비활성화되어 있는지 여부.

특정 필드를 기준으로 테이블을 정렬하려면 해당 필드의 열 제목을 선택합니다. 정렬 순서를 변경하려면 열 제목을 다시 선택합니다. 표를 필터링하려면 필터 상자에 커서를 놓고 필드에 필터 조건을 추가합니다. 결과를 더 세분화하려면 추가 필드에 필터 조건을 추가합니다.

API

프로그래밍 방식으로 조직의 계정을 검토하려면 Amazon Macie API ListMembers작업을 사용하고 요청이 적용되는 지역을 지정하십시오. 다른 리전에 계정을 추가하려면 각 추가 리전에서 요청을 제출합니다.

요청을 제출할 때 `onlyAssociated` 파라미터를 사용하여 응답에 포함시킬 계정을 지정합니다. 기본적으로 Macie는 초대를 통해 또는 초대를 통해 지정된 지역의 멤버 계정인 계정에 대한 세부 정보만 반환합니다. AWS Organizations멤버 계정이 아닌 계정을 포함하여 모든 관련 계정의 세부 정보를 검색하려면 요청에 `onlyAssociated` 파라미터를 포함시키고 파라미터 값을 `false`로 설정합니다.

AWS Command Line Interface (AWS CLI)를 사용하여 조직의 계정을 검토하려면 list-members 명령을 실행합니다. only-associated 파라미터에 모든 관련 계정을 포함할지 아니면 멤버 계정만 포함시킬지 지정합니다. 멤버 계정만 포함시키려면 이 파라미터를 생략하거나 파라미터 값을 true로 설정합니다. 모든 계정을 포함시키려면 이 값을 false(으)로 설정합니다. 예:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

여기서 *us-east-1*은 요청이 적용되는 리전, 즉 미국 동부 (버지니아 북부) 리전을 나타냅니다.

요청이 성공하면 Macie는 members 배열을 반환합니다. 배열에는 요청에 지정된 기준을 충족하는 각 계정에 대한 member 객체가 포함됩니다. 해당 객체에서 relationshipStatus 필드는 내 계정과 지정된 리전에 있는 다른 계정 간 현재 연결 상태를 나타냅니다. 초대 기반 조직의 계정의 경우 가능한 값은 다음과 같습니다.

- AccountSuspended— 일시 중지되었습니다. AWS 계정
- Created - 계정을 추가했지만 아직 멤버십 초대장을 보내지 않았습니다.
- EmailVerificationFailed - 계정으로 멤버십 초대장을 보내려고 했지만 계정에 지정한 이메일 주소가 유효하지 않습니다.
- EmailVerificationInProgress - 계정으로 멤버십 초대장을 보냈으며 Macie가 요청을 처리 중입니다.
- Enabled - 계정은 멤버 계정입니다. Macie는 이러한 계정에서 활성화되어 있으며, 해당 계정의 Macie 관리자입니다.
- Invited - 계정으로 멤버십 초대장을 보냈지만 계정에서 초대에 응답하지 않았습니다.
- Paused - 멤버 계정이지만 Macie는 현재 해당 계정에서 일시 중지 상태입니다.
- RegionDisabled - AWS 계정에서 현재 리전이 비활성화되어 있습니다.
- Removed - 계정이 이전 멤버 계정입니다. 하지만 계정에서 연결을 해제하여 해당 계정을 멤버 계정에서 제거했습니다.
- Resigned - 계정이 이전 멤버 계정입니다. 하지만 해당 계정은 계정에서 연결을 해제하여 조직에서 탈퇴했습니다.

member 객체의 다른 필드에 대한 자세한 내용은 Amazon Macie API 참조에서 멤버를 참조하십시오.

초대 기반 조직을 위한 다른 Amazon Macie 관리자 계정 지정

초대 기반 조직을 생성하고 설정한 후 조직의 Amazon Macie 관리자 계정을 변경할 수 있습니다. 이를 위해서는 관리자와 조직 멤버가 다음 단계를 수행해야 합니다.

1. 현재 Macie 관리자는 조직의 활성 멤버 계정의 현재 인벤토리를 선택적으로 내보낼 수 있습니다. 이렇게 하면 조직에 계속 남아 있어야 하는 멤버 계정을 쉽게 구분할 수 있어 전환이 간소화됩니다.
2. 현재 Macie 관리자는 현재 조직에서 모든 멤버 계정을 제거합니다. 이렇게 하면 계정이 현재 관리자 계정에서 분리됩니다. Macie는 해당 계정을 계속 사용할 수 있지만 해당 계정은 독립형 Macie 계정이 됩니다.

> **Note**
>
> 현재 Macie 관리자가 구성원 계정을 제거하면 Macie는 해당 계정에 대한 민감한 데이터 자동 검색을 자동으로 비활성화합니다. 또한 이렇게 하면 Macie가 계정에 대한 자동 검색을 수행하는 동안 생성하고 직접 제공한 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다. 새 조직으로의 전환이 완료되면 새 Macie 관리자는 이 데이터에 액세스할 수 없습니다.

3. 새 Macie 관리자는 이전 멤버 계정을 새 조직에 추가합니다. 그러면 계정이 새 관리자 계정과 연결됩니다.
4. 각 멤버 계정은 새 조직에 가입하라는 초대를 수락합니다. 다른 계정으로부터 온 초대를 수락하면 사용자 계정이 새 조직의 멤버 계정이 됩니다. 새 Macie 관리자 계정은 해당 멤버 계정에 대한 Macie 설정, 데이터 및 리소스에 액세스할 수 있습니다. 이전에 계정에 대해 민감한 데이터 자동 검색을 사용하도록 설정한 경우 Macie가 계정에 대한 자동 검색을 수행하는 동안 이전에 생성하여 직접 제공한 데이터는 여기에 포함되지 않습니다. 대신 Macie는 새 Macie 관리자가 계정에 대한 자동 검색을 활성화한 경우 계정에 대한 새 데이터를 생성하고 유지 관리합니다.

조직에서 Macie를 여러 AWS 리전곳에서 사용하는 경우 각 지역에서 이전 단계를 수행하십시오.

활성 멤버 계정의 현재 인벤토리를 내보내려면 현재 Macie 관리자가 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하면 됩니다. 현재 관리자는 콘솔에서 데이터를 쉼표로 구분된 값(CSV) 파일로 내보낼 수 있습니다. 그런 다음 새 관리자는 콘솔을 사용하여 CSV 파일을 업로드하고 모든 계정을 새 조직에 (일괄적으로) 추가할 수 있습니다.

콘솔을 사용하여 멤버 계정 데이터를 내보내는 방법

1. 현재 Macie 관리자 AWS Management Console 계정을 사용하여 로그인합니다.

2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 데이터를 내보낼 지역을 선택합니다.
3. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
4. 탐색 창에서 Accounts(계정)를 선택합니다. 계정 페이지가 열리고 현재 Macie 관리자 계정과 연결된 계정 테이블이 표시됩니다.
5. (선택 사항) 계정 표를 필터링하여 조직에서 현재 활성 Macie 멤버 계정만 표시하려면 표 위에 있는 필터 상자를 사용하여 다음 필터 조건을 추가합니다.
   - 유형 = 초대
   - 상태 = 활성화됨
6. 계정 테이블에서 내보낸 데이터에 포함할 각 구성원 계정의 확인란을 선택합니다.
7. CSV 내보내기를 선택합니다.
8. 출력의 위치 및 파일 이름을 지정합니다.

현재 Macie 관리자는 Amazon Macie API를 사용하여 JSON 형식의 데이터를 검색할 수 있습니다. 그러면 새 Macie 관리자는 이 데이터를 사용하여 새 조직에 추가하고 초대할 계정의 계정 ID 및 이메일 주소 목록을 생성할 수 있습니다. JSON 형식으로 데이터를 검색하려면 Amazon ListMembersMacie API의 작업을 사용하십시오. 작업이 성공하면 Macie는 관리자 계정과 연결된 모든 계정에 대한 세부 정보를 제공하는 `members` 배열을 반환합니다. 계정이 현재 초대 기반 조직의 활성 Macie 멤버 계정인 경우 계정의 `relationshipStatus` 속성 값은 `Enabled`이며 `invitedAt` 속성에는 날짜 및 시간이 지정됩니다.

Amazon Macie에서 초대 기반 조직 관리

Amazon Macie에서 조직에 가입하도록 초대를 받은 경우 선택적으로 초대를 수락하거나 거부할 수 있습니다. Macie에서 조직은 관련 계정의 그룹으로 중앙에서 관리되는 계정 집합입니다. 조직은 지정된 Macie 관리자 계정 하나와 하나 이상의 관련 멤버 계정으로 구성됩니다.

초대를 수락하면 해당 계정은 조직의 멤버 계정이 됩니다. 수락하면 초대를 보낸 계정이 사용자 계정의 Macie 관리자 계정이 됩니다. 계정을 다른 계정과 연결하고 계정 간에 관리자-멤버 관계를 활성화할 수 있습니다. 그러면 Macie 관리자 계정으로 해당 AWS 리전에서 계정에 대한 특정 Macie 설정, 데이터 및 리소스에 액세스할 수 있습니다. 자세한 정보는 Amazon Macie 관리자 및 멤버 계정 간의 관계 이해을 참조하세요.

초대를 거부해도 Macie 계정의 현재 상태 및 설정은 변경되지 않습니다.

주제

조직의 멤버십 초대에 대한 응답

조직 가입 초대를 받으면 Amazon Macie에서 여러 가지 방법으로 알림을 보냅니다. 기본적으로 Macie는 이메일 메시지로 초대장을 보냅니다. Macie는 여러분을 위한 AWS Health 이벤트도 만들어 드립니다. AWS 계정초대장을 보낸 AWS 리전 곳에서 이미 Macie를 사용하고 있는 경우 Macie는 Macie 콘솔에 계정 배지와 알림도 표시합니다.

초대를 받은 후 선택적으로 초대를 수락하거나 거절할 수 있습니다. 응답하기 전에 다음 사항에 유의하세요.

- 사용자는 한 번에 하나의 조직 멤버만 될 수 있습니다. 초대를 여러 번 받은 경우 하나만 수락할 수 있습니다. 또는 이미 조직의 멤버인 경우 다른 조직에 가입하려면 먼저 현재 Macie 관리자 계정에서 계정을 연결 해제해야 합니다.
- 여러 리전에서 Macie를 사용하는 경우, 계정에 모든 리전에서 동일한 Macie 관리자 계정이 있어야 합니다. Macie 관리자는 각 리전마다 별도로 사용자에게 초대를 보내야 하며, 사용자는 각 리전에서 별도로 초대를 수락해야 합니다.
- 초대를 수락하거나 거절하려면 초대를 보낸 리전에서 Macie를 활성화해야 합니다. 초대를 거절하는 것은 선택 사항입니다. Macie가 초대를 거절할 수 있도록 설정한 경우, 초대를 거절하고 나면 해당 리전에서 Macie 비활성화를 할 수 있습니다. 이렇게 하면 해당 리전에서 Macie를 사용할 때 불필요한 요금이 발생하지 않도록 할 수 있습니다.
- 계정에 민감한 데이터 자동 검색 기능이 활성화되어 있고 초대를 수락하면 계정 자동 검색을 수행하는 동안 Macie가 생성하고 직접 제공한 통계 데이터, 인벤토리 데이터 및 기타 정보에 액세스할 수 없게 됩니다. 초대를 수락하면 Macie 관리자가 계정에 대한 자동 검색을 활성화할 수 있습니다. 하지만 이렇게 해도 기존 데이터에 대한 액세스는 복원되지 않습니다. 대신 Macie는 계정에 대한 자동 검색을 수행하는 동안 새 데이터를 생성하고 유지합니다.

추가 고려 사항은 멤버십 초대 응답 및 관리 단원을 참조하세요.

조직의 멤버십 초대에 응답하려면

멤버십 초대에 응답하기 위해 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 멤버십 초대에 응답하려면 다음 단계를 따르세요.

멤버십 초대에 응답하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 초대를 받은 지역을 선택합니다.
3. 해당 리전에서 Macie를 활성화하지 않은 경우 시작하기를 선택한 다음 Macie 활성화를 선택합니다. Macie를 활성화해야 초대를 수락하거나 거절할 수 있습니다.
4. 탐색 창에서 Accounts(계정)를 선택합니다.
5. 관리자 계정에서 다음 중 하나를 수행합니다.

   - 초대를 수락하려면 초대 옆의 수락( ) 을 켜세요. 그런 다음 이전에 다른 초대를 수락했는지 여부에 따라 초대 수락 또는 업데이트를 선택합니다.
   - 초대를 거부하려면 초대 옆의 초대 거절을 선택한 다음 초대를 거부할지 확인합니다.

추가 리전에서 초대를 받았는데 이에 응답하려면 각 추가 리전에서 이전 단계를 반복하세요.

API

프로그래밍 방식으로 초대에 응답하려면 초대를 수락할지 거절할지에 따라 Amazon Macie API의 또는 DeclineInvitations연산을 사용하십시오. AcceptInvitation 요청을 제출할 때는 초대장을 보낸 리전을 지정해야 합니다. 추가 리전의 초대에 응답하려면 각 추가 리전에서 요청을 제출하세요.

`AcceptInvitation`요청 시 `administratorAccountId` 파라미터를 사용하여 초대를 보낸 사람의 12자리 계정 ID를 지정합니다. AWS 계정 `invitationId` 파라미터를 사용하여 수락할 초대의 고유 ID를 지정합니다.

`DeclineInvitations`요청 시 `accountIds` 파라미터를 사용하여 거절 초대를 보낸 사람의 12자리 계정 ID를 지정합니다. AWS 계정

ID를 검색하려면 Amazon Macie API의 ListInvitations작업을 사용할 수 있습니다. 작업이 성공하면 Macie는 각 초대를 보낸 계정의 계정 ID 및 각 초대장의 고유 ID를 포함하여 수신한 초대에 대한 세부 정보를 제공하는 `invitations` 배열을 반환합니다. 초대장의 `relationshipStatus` 속성 값이 `Invited`인 경우 아직 초대에 응답하지 않은 것입니다.

AWS Command Line Interface (AWS CLI)를 사용하여 초대에 응답하려면 초대를 수락할지 거절할지에 따라 초대 수락 또는 초대 거부 명령을 실행합니다. `region` 파라미터를 사용하여 초대를 보낸 리전을 지정할 수 있습니다. 예:

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-
id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

여기서 *us-east-1*은 초대를 보낸 리전(미국 동부(버지니아 북부) 리전)이고, *123456789012*는 초대를 보낸 계정의 계정 ID이며, *d8bdad0e203fd1242e0a4721bexample*은 초대를 수락할 수 있는 고유 ID입니다.

초대 수락 요청이 성공하면 Macie는 빈 응답을 반환합니다. 초대 거부 요청이 성공하면 Macie는 빈 `unprocessedAccounts` 배열을 반환합니다.

초대를 거절한 후에도 초대는 Macie 계정의 리소스로 계속 유지됩니다. 선택적으로 DeleteInvitations작업을 사용하거나 삭제 초대 명령 (의 경우) 을 사용하여 삭제할 수 있습니다. AWS CLI

Amazon Macie 관리자 계정에서 연결 해제

Amazon Macie에서 조직에 가입하라는 초대를 수락하면 나중에 계정을 현재 Macie 관리자 계정에서 분리하여 조직에서 사임할 수 있습니다. 사용자의 계정이 조직의 멤버 계정인 경우에는 AWS Organizations 작업을 수행할 수 없습니다. AWS Organizations 조직에서 탈퇴하려면 Macie 관리자에게 문의하여 Macie 회원 계정으로 등록된 계정을 제거하세요.

계정을 Macie 관리자 계정에서 분리하면 Macie 관리자는 Macie 계정의 모든 설정, 데이터 및 리소스에 액세스할 수 없게 됩니다. 여기에는 소유하고 있는 Amazon S3 데이터에 대한 메타데이터 및 정책 조사 결과가 포함됩니다. 즉, 관리자는 더 이상 민감한 데이터 자동 검색을 수행하거나 민감한 데이터 검색 작업을 실행하여 Amazon S3 데이터를 분석할 수 없습니다.

계정 연결을 해제해도 해당 리전의 Macie는 해당 리전에서 해당 계정을 계속 사용할 수 있습니다. 그러나 사용자 계정은 해당 리전에서 독립 실행형 Macie 계정이 됩니다. 관리자 계정 인벤토리에서 계정 상태가 멤버 탈퇴로 변경됩니다.

Macie 관리자 계정에서 연결 해제

현재 Macie 관리자 계정과의 연결을 끊으려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다.

Console

Amazon Macie 콘솔을 사용하여 다음 단계에 따라 Macie 관리자 계정과 계정의 연결을 해제하세요.

관리자 계정에서 연결 해제

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 관리자 계정과 계정 연결을 해제하려는 지역을 선택합니다.
3. 탐색 창에서 Accounts(계정)를 선택합니다.
4. 관리자 계정에서 초대 옆의 수락()을 끄고 업데이트를 선택합니다.

해당 계정은 계정 페이지에 계속 표시됩니다. 조직에 다시 가입하기로 결정한 경우 이 페이지를 사용하여 원래 초대를 다시 수락할 수 있습니다. 초대를 거부하고 삭제할 수도 있습니다. 이렇게 하면 사용자 계정과 다른 계정 간의 연결도 삭제됩니다. 이렇게 하려면 초대 거부를 선택합니다.

추가 리전의 Macie 관리자 계정과 계정 연결을 끊으려면 각 추가 리전에서 이전 단계를 반복하세요.

API

프로그래밍 방식으로 Macie 관리자 계정과 계정을 분리하려면 Amazon Macie API의 DisassociateFromAdministratorAccount작업을 사용하십시오. 요청을 제출할 때는 요청이 적용되는 리전을 지정해야 합니다. 추가 리전의 계정과의 연결을 끊으려면 각 추가 리전에서 요청을 제출하세요.

를 사용하여 Macie 관리자 계정과 계정의 연결을 끊으려면 명령을 실행합니다. AWS CLIdisassociate-from-administrator-account `region` 파라미터를 사용하여 계정에서 연결을 해제할 리전을 지정합니다.

요청이 성공하면 Macie는 빈 응답을 반환합니다.

계정에서 연결을 끊은 후에도 원래 초대는 삭제하지 않는 한 Macie 계정의 리소스로 유지됩니다. 조직에 다시 가입하기로 결정한 경우 이 리소스를 사용하여 원래 초대를 다시 수락할 수 있습니다. 또는 DeleteInvitations작업을 사용하거나 delete-invitations 명령 () 을 사용하여 초대를 삭제할 수도 있습니다. AWS CLI초대를 삭제하면 사용자 계정과 다른 계정 간의 연결도 삭제됩니다.

Amazon Macie의 보안

AWS에서 클라우드 보안을 가장 중요하게 생각합니다. AWS 고객은 보안에 가장 보안에 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 귀하의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램의 일환으로 보안 효과를 정기적으로 테스트하고 검증합니다. Amazon Macie에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램의 범위에 속하는 AWS 서비스를 참조하세요.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스로 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Macie 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Macie를 구성하는 방법을 보여줍니다. 또한 Macie 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스을(를) 사용하는 방법을 배우게 됩니다.

주제

- Amazon Macie에서의 데이터 보호
- Amazon Macie용 Identity and Access Management
- Amazon Macie에서 로깅 및 모니터링
- Amazon Macie에 대한 규정 준수 확인
- Amazon Macie의 복원성
- Amazon Macie의 인프라 보안
- Amazon Macie 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

Amazon Macie에서의 데이터 보호

AWS 공동 책임 모델은 Amazon Macie의 데이터 보호에 적용됩니다. 이 모델이 설명하는 것처럼 AWS는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 Data Privacy FAQ(데이터 프라이버

시 FAQ)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS Shared Responsibility Model and GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정보안 인증 정보를 보호하고 AWS IAM Identity Center또는 AWS Identity and Access Management(IAM)를 통해 개별 사용자 계정을 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 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신하세요. TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- AWS CloudTrail로 API 및 사용자 활동 로깅을 설정하세요.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용합니다.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API, AWS 서비스 또는 AWS SDK를 사용하여 Macie 또는 기타 AWS CLI와(과) 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 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

저장된 데이터 암호화

Amazon Macie는 AWS 암호화 솔루션을 사용하여 저장 데이터를 안전하게 저장합니다. Macie는 AWS Key Management Service(AWS KMS)의 AWS 관리형 키을(를) 사용하여 조사 결과 등의 데이터를 암호화합니다.

Macie를 비활성화하면 민감한 데이터 검색 작업, 사용자 지정 데이터 식별자, 조사 결과 등 사용자를 위해 저장하거나 유지 관리하는 모든 리소스가 영구적으로 삭제됩니다.

전송 중 암호화

Macie는 AWS 서비스 간에 전송되는 모든 데이터를 암호화합니다.

Amazon Macie는 Amazon S3의 데이터를 분석하고 민감한 데이터 검색 결과를 S3 버킷으로 내보냅니다. Macie가 S3 객체에서 필요한 정보를 가져온 후에는 해당 정보를 폐기합니다.

Macie는 AWS PrivateLink으(로) 구동되는 VPC 엔드포인트를 사용하여 Amazon S3에 액세스합니다. 따라서 Macie와 Amazon S3 간의 트래픽은 Amazon 네트워크에 머무르며 퍼블릭 인터넷을 거치지 않습니다. 자세한 내용은 AWS PrivateLink 섹션을 참조하세요.

Amazon Macie용 Identity and Access Management

AWS Identity and Access Management (IAM) 은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM 관리자는 누가 Macie 리소스를 사용할 수 있도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- Amazon Macie와 호환되는 방식 AWS Identity and Access Management
- Amazon Macie의 ID 기반 정책 예제
- Amazon Macie의 서비스 연결 역할
- Amazon Macie에 대한 AWS 관리형 정책
- Amazon Macie 자격 증명 및 액세스 문제 해결

고객

Macie에서 수행하는 작업에 따라 사용 방법 AWS Identity and Access Management (IAM) 이 다릅니다.

서비스 사용자 - Macie 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Macie 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Macie의 기능에 액세스할 수 없는 경우 Amazon Macie 자격 증명 및 액세스 문제 해결 단원을 참조하세요.

서비스 관리자 - 회사에서 Macie 리소스를 책임지고 있는 경우 Macie에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Macie 기능과 리소스를 결정합

니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Macie에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Amazon Macie와 호환되는 방식 AWS Identity and Access Management 단원을 참조하세요.

IAM 관리자 - IAM 관리자라면 Macie에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Macie 자격 증명 기반 정책 예제를 보려면 Amazon Macie의 ID 기반 정책 예제 단원을 참조하세요.

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있

는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하십시오.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역

할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 생성 단원을 참조하십시오. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접적 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은

사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

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.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.

- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

Amazon Macie와 호환되는 방식 AWS Identity and Access Management

AWS Identity and Access Management (IAM) 을 사용하여 Amazon Macie에 대한 액세스를 관리하기 전에 Macie와 함께 사용할 수 있는 IAM 기능에 대해 알아보십시오.

Amazon Macie에서 사용할 수 있는 IAM 기능

IAM 특성	Macie 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
액세스 제어 목록(ACL)	아니요

IAM 특성	Macie 지원
ABAC(속성 기반 액세스 제어) - 정책 태그	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	아니요
서비스 링크 역할	예

Macie를 비롯한 다른 사람들이 대부분의 IAM 기능을 어떻게 AWS 서비스 사용하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과AWS 서비스 호환되는 기능을 참조하십시오.

Amazon Macie의 자격 증명 기반 정책

보안 인증 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

Macie는 자격 증명 기반 정책을 지원합니다. 예를 보려면 Amazon Macie의 ID 기반 정책 예제을 참조하세요.

Amazon Macie 내의 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

Macie에서는 리소스 기반 정책을 지원하지 않습니다. 즉, 정책을 Macie 리소스에 직접 연결할 수는 없습니다.

Amazon Macie의 정책 작업

정책 작업 지원	예

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 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

Macie의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
macie2
```

예를 들어, Macie가 제공하는 모든 관리형 데이터 식별자에 대한 정보에 액세스할 수 있는 권한을 다른 사람에게 부여하려면(Amazon Macie API의 `ListManagedDataIdentifiers` 작업에 해당하는 작업임) 정책에 `macie2:ListManagedDataIdentifiers` 작업을 포함시킵니다.

```
"Action": "macie2:ListManagedDataIdentifiers"
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다. 예:

```
"Action": [
      "macie2:ListManagedDataIdentifiers",
      "macie2:ListCustomDataIdentifiers"
]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수도 있습니다. 예를 들어, `List`라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "macie2:List*"
```

하지만 가장 좋은 방법은 최소 권한의 원칙을 따르는 정책을 만드는 것입니다. 즉, 특정 작업을 수행하는 데 필요한 권한만 포함하는 정책을 만들어야 합니다.

Macie 작업 목록을 보려면 서비스 권한 부여 참조에서 Amazon Macie에서 정의한 작업을 참조하세요. Macie 작업을 지정하는 정책의 예는 Amazon Macie의 ID 기반 정책 예제 섹션을 참조하세요.

Amazon Macie의 정책 리소스

정책 리소스 지원	예

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 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Macie는 다음과 같은 리소스 유형을 정의합니다.

- 허용 목록
- 사용자 지정 데이터 식별자
- 필터 또는 제외 규칙(결과 필터라고도 함)
- 멤버 계정
- 민감한 데이터 검색 작업(분류 작업이라고도 함)

ARN을 사용하여 정책에서 다음과 같은 리소스 유형을 지정할 수 있습니다.

예를 들어, 작업 ID가 3ce05dbb7ec5505def334104bexample인 민감한 데이터 검색 작업에 대한 정책을 생성하려면 다음 ARN을 사용할 수 있습니다.

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample"
```

또는 특정 계정에 민감한 데이터 검색 작업을 모두 지정하려면 와일드카드(*)를 사용합니다.

```
"Resource": "arn:aws:macie2:*:123456789012:classification-job/*"
```

여기서 *123456789012*는 작업을 생성한 AWS 계정 의 계정 ID입니다. 하지만, 가장 좋은 방법은 최소 권한의 원칙을 따르는 정책을 만드는 것입니다. 즉, 특정 작업을 수행하는 데 필요한 권한만 포함하는 정책을 만들어야 합니다.

일부 Macie 작업은 여러 리소스에 적용할 수 있습니다. 예를 들어 `macie2:BatchGetCustomDataIdentifiers` 작업은 여러 사용자 지정 데이터 식별자의 세부 정보를 검색할 수 있습니다. 이러한 경우 주체는 작업이 적용되는 모든 리소스에 액세스할 수 있는 권한을 가지고 있어야 합니다. 단일 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
 "arn:aws:macie2:*:*:custom-data-identifier/12g4aff9-8e22-4f2b-b3fd-3063eexample",
 "arn:aws:macie2:*:*:custom-data-identifier/2d12c96a-8e78-4ca6-b1dc-8fd65example",
 "arn:aws:macie2:*:*:custom-data-identifier/4383a69d-4a1e-4a07-8715-208ddexample"
]
```

Macie 리소스 유형 및 해당 ARN 신택스 목록을 보려면 서비스 승인 참조의 Amazon Macie에서 정의한 리소스 유형을 참조하세요. 각 리소스 유형으로 지정할 수 있는 작업을 알아보려면 서비스 인증 참조의 Amazon Macie에서 정의한 작업 섹션을 참조하세요. 리소스를 지정하는 정책의 예는 Amazon Macie의 ID 기반 정책 예제 섹션을 참조하세요.

Amazon Macie의 정책 조건 키

서비스별 정책 조건 키 지원	예

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` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예컨대, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

Macie 조건 키 목록을 보려면 서비스 승인 참조의 Amazon Macie에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon Macie에서 정의한 작업을 참조하세요. 조건 키를 사용하는 정책의 예는 Amazon Macie의 ID 기반 정책 예제 섹션을 참조하세요.

Amazon Macie의 액세스 제어 목록(ACL)

ACL 지원	아니요

ACL(액세스 통제 목록)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

아마존 심플 스토리지 서비스 (Amazon S3) 는 ACL을 지원하는 서비스의 AWS 서비스 한 예입니다. 자세히 알아보려면 Amazon Simple Storage Service 사용 설명서의 액세스 제어 목록(ACL) 개요를 참조하세요.

Macie는 ACL을 지원하지 않습니다. 즉, Macie 리소스에 ACL을 연결할 수 없습니다.

Amazon Macie를 사용한 ABAC(속성 기반 액세스 제어)

ABAC 지원(정책의 태그)	예

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇입니까?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

Macie 리소스에 허용 목록, 사용자 지정 데이터 식별자, 필터 규칙 및 금지 규칙, 멤버 계정, 민감한 데이터 검색 작업 등의 태그를 첨부할 수 있습니다. 또한 정책의 `Condition` 요소에 태그 정보를 제공하여 이러한 유형의 리소스에 대한 액세스를 제어할 수 있습니다. Macie 리소스 태그 지정에 대한 자세한 내용은 Amazon Macie에 리소스 태그 지정 섹션을 참조하세요. 태그를 기반으로 리소스에 대한 액세스를 제한하는 자격 증명 기반 정책의 예는 Amazon Macie의 ID 기반 정책 예제 단원을 참조하십시오.

Amazon Macie에서 임시 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하십시오.

Macie에서 임시 자격 증명 사용을 지원합니다.

Amazon Macie를 위한 전달 액세스 세션

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Macie는 다음 작업을 수행할 AWS 서비스 때 FAS 요청을 다운스트림으로 전송합니다.

- S3 버킷에 저장된 허용 목록에 대한 Macie 설정을 생성하거나 업데이트합니다.
- S3 버킷에 저장된 허용 목록의 상태를 확인합니다.
- IAM 사용자 보안 인증을 사용하여 영향을 받는 S3 객체에서 민감한 데이터 샘플을 검색합니다.
- IAM 사용자 보안 인증 또는 IAM 역할을 사용하여 검색된 민감한 데이터 샘플을 암호화합니다.
- Macie와 통합할 수 있도록 하세요. AWS Organizations
- AWS Organizations에서 조직에 대한 위임된 Macie 관리자 계정을 지정합니다.

다른 작업의 경우 Macie는 사용자를 대신하여 작업을 수행하기 위해 서비스 연결 역할을 사용합니다. 이 역할에 대한 자세한 내용은 Amazon Macie의 서비스 연결 역할 단원을 참조하세요.

Amazon Macie의 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

Macie는 서비스 역할을 맡거나 사용하지 않습니다. Macie는 사용자를 대신하여 작업을 수행하기 위해 주로 서비스 연결 역할을 사용합니다. 이 역할에 대한 자세한 내용은 Amazon Macie의 서비스 연결 역할 단원을 참조하세요.

Amazon Macie의 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Macie는 사용자를 대신하여 작업을 수행하기 위해 서비스 연결 역할을 사용합니다. 이 역할에 대한 자세한 내용은 Amazon Macie의 서비스 연결 역할 단원을 참조하세요.

Amazon Macie의 ID 기반 정책 예제

기본적으로 사용자 및 역할에는 Macie 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface(AWS CLI) 또는 AWS API를 사용해 태스크를 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 Macie에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조에서 Amazon Macie에 대한 작업, 리소스 및 조건 키를 참조하세요.

정책을 생성할 때는 AWS Identity and Access Management Access Analyzer(IAM Access Analyzer)의 보안 경고, 오류, 일반 경고 및 제안 사항을 해결한 후 정책을 저장해야 합니다. IAM Access Analyzer는 정책 확인을 실행하여 IAM 정책 문법 및 모범 사례에 대해 정책을 검증합니다. 이러한 확인은 조사 결과를 생성하고 보안 모범 사례를 준수하고 작동하는 정책을 작성하는 데 도움이 되는 실행 가능한 권장 사항을 제공합니다. IAM Access Analyzer를 사용한 정책 검증에 대해 알아보려면 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요. IAM Access Analyzer에서 반환할 수 있는 경고, 오류 및 제안 사항 목록을 검토하려면 IAM 사용 설명서에서 IAM Access Analyzer 정책 확인 참조를 참조하세요.

주제

- 정책 모범 사례
- Amazon Macie 콘솔 사용
- 예: 사용자가 자신의 고유한 권한을 검토할 수 있도록 허용함
- 예: 사용자가 민감한 데이터 검색 작업을 만들 수 있도록 허용함
- 예: 사용자가 민감한 데이터 검색 작업을 관리할 수 있도록 허용함
- 예: 사용자가 조사 결과를 검토할 수 있도록 허용함
- 예: 사용자가 태그를 기반으로 사용자 지정 데이터 식별자를 검토할 수 있도록 허용함

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Macie 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 정책으로 시작하고 최소 권한을 향해 나아가기 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 관리형 정책은 AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 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. 특정 AWS 서비스(예: AWS CloudFormation)를 통해 사용되는 경우에만 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer policy validation(IAM Access Analyzer 정책 검증)을 참조하세요.
- 다중 인증(MFA) 필요 – AWS 계정 계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 설정합니다. API 작업을 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Amazon Macie 콘솔 사용

Amazon Macie 콘솔에 액세스하려면 최소한의 권한 세트가 있어야 합니다. 이러한 권한은 AWS 계정에서 Macie 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요가 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 Amazon Macie 콘솔을 사용할 수 있도록 하려면, 사용자와 역할에 콘솔 액세스를 제공하는 IAM 정책을 생성합니다. 자세한 내용은 IAM 사용 설명서에서 IAM의 정책 및 권한을 참조하세요.

사용자 또는 역할이 Amazon Macie 콘솔을 사용할 수 있도록 허용하는 정책을 생성하는 경우, 정책이 `macie2:GetMacieSession` 작업을 허용하는지 확인합니다. 그렇지 않으면, 해당 사용자 또는 역할이 콘솔에 있는 Macie 리소스 또는 데이터에 액세스할 수 없습니다.

또한 해당 사용자 또는 역할이 콘솔에서 액세스해야 하는 리소스에 대해 적절한 `macie2:List` 작업을 정책이 허용하는지 확인합니다. 그렇지 않으면, 해당 사용자 또는 역할이 콘솔에서 해당 리소스로 이동하거나 해당 리소스에 대한 세부 정보를 표시할 수 없습니다. 예를 들어, 콘솔

을 사용하여 민감한 데이터 검색 작업의 세부 정보를 검토하려면, 사용자가 해당 작업에 대한 `macie2:DescribeClassificationJob` 작업 및 `macie2:ListClassificationJobs` 작업을 수행할 수 있어야 합니다. 사용자가 `macie2:ListClassificationJobs` 작업을 수행할 수 없는 경우, 사용자는 콘솔의 작업 페이지에 작업 목록을 표시할 수 없으므로 세부 정보를 표시할 작업을 선택할 수 없습니다. 작업이 사용하는 사용자 지정 데이터 식별자에 대한 정보를 포함하는 세부 정보의 경우, 사용자가 사용자 지정 데이터 식별자에 대한 `macie2:BatchGetCustomDataIdentifiers` 작업도 수행할 수 있어야 합니다.

예: 사용자가 자신의 고유한 권한을 검토할 수 있도록 허용함

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI나 AWS API를 사용하여 프로그래밍 방식으로 이 태스크를 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": "*"
        }
    ]
}
```

예: 사용자가 민감한 데이터 검색 작업을 만들 수 있도록 허용함

이 예제는 사용자가 민감한 데이터 검색 작업을 생성하도록 허용하는 정책을 생성하는 방법을 보여줍니다.

이 예제에서, 첫 번째 명령문은 사용자에게 `macie2:CreateClassificationJob` 권한을 부여합니다. 이러한 권한을 통해 사용자는 작업을 생성할 수 있습니다. 이 명령문은 `macie2:DescribeClassificationJob` 권한도 부여합니다. 이러한 권한을 통해 사용자는 기존 작업의 세부 정보에 액세스할 수 있습니다. 작업을 생성하는 데 이러한 권한이 필요하지는 않지만, 이러한 세부 정보에 액세스하면 사용자가 고유한 구성 설정을 보유한 작업을 생성하는 데 도움이 될 수 있습니다.

예제의 두 번째 명령문은 사용자가 Amazon Macie 콘솔을 사용하여 작업을 생성, 구성 및 검토할 수 있도록 허용합니다. `macie2:ListClassificationJobs` 권한을 통해 사용자는 콘솔의 작업 페이지에 기존 작업을 표시할 수 있습니다. 명령문의 다른 모든 권한은 사용자가 콘솔의 작업 생성 페이지를 사용하여 작업을 구성하고 생성할 수 있도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndReviewJobs",
            "Effect": "Allow",
            "Action": [
                "macie2:CreateClassificationJob",
                "macie2:DescribeClassificationJob"
            ],
            "Resource": "arn:aws:macie2:*:*:classification-job/*"
        },
        {
            "Sid": "CreateAndReviewJobsOnConsole",
            "Effect": "Allow",
            "Action": [
                "macie2:ListClassificationJobs",
                "macie2:ListAllowLists",
                "macie2:ListCustomDataIdentifiers",
                "macie2:ListManagedDataIdentifiers",
```

```
                "macie2:SearchResources",
                "macie2:DescribeBuckets"
            ],
            "Resource": "*"
        }
    ]
}
```

예: 사용자가 민감한 데이터 검색 작업을 관리할 수 있도록 허용함

이 예제에서는 사용자가 특정 민감한 데이터 검색 작업, 즉 3ce05dbb7ec5505def334104bexample의 ID를 가진 작업의 세부 정보에 액세스하도록 허용하는 정책을 생성하는 방법을 보여줍니다. 또한 이 예제를 통해 사용자는 필요에 따라 작업 상태를 변경할 수 있습니다.

예제의 첫 번째 명령문은 사용자에게 macie2:DescribeClassificationJob 및 macie2:UpdateClassificationJob 권한을 부여합니다. 이러한 권한을 통해 사용자는 각각 작업 세부 정보를 검색하고 작업 상태를 변경할 수 있습니다. 두 번째 명령문은 사용자에게 macie2:ListClassificationJobs 권한을 부여하여 사용자가 Amazon Macie 콘솔의 작업 페이지를 사용하여 작업에 액세스할 수 있도록 합니다.

```
{
   "Version": "2012-10-17",
   "Statement": [
 {
         "Sid": "ManageOneJob",
         "Effect": "Allow",
         "Action": [
            "macie2:DescribeClassificationJob",
            "macie2:UpdateClassificationJob"
         ],
         "Resource": "arn:aws:macie2:*:*:classification-
job/3ce05dbb7ec5505def334104bexample"
 },
 {
         "Sid": "ListJobsOnConsole",
         "Effect": "Allow",
         "Action": "macie2:ListClassificationJobs",
         "Resource": "*"
 }
   ]
}
```

또한 Macie가 작업을 위해 Amazon CloudWatch Logs에 게시하는 로깅 데이터(로그 이벤트)에 사용자가 액세스하도록 허용할 수도 있습니다. 이를 위해 해당 작업에 대한 로그 그룹 및 스트림에서 CloudWatch Logs(`logs`) 작업을 수행할 권한을 부여하는 명령문을 추가할 수 있습니다. 예:

```
"Statement": [
    {
        "Sid": "AccessLogGroupForMacieJobs",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs"
    },
    {
        "Sid": "AccessLogEventsForOneMacieJob",
        "Effect": "Allow",
        "Action": "logs:GetLogEvents",
        "Resource": [
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs/*",
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs:log-
stream:3ce05dbb7ec5505def334104bexample"
        ]
    }
]
```

CloudWatch Logs에 대한 액세스 관리에 대한 자세한 내용은 Amazon CloudWatch Logs 사용 설명서의 CloudWatch Logs 리소스에 대한 액세스 권한 관리 개요를 참조하세요.

예: 사용자가 조사 결과를 검토할 수 있도록 허용함

이 예제에서는 사용자의 조사 결과 데이터 액세스를 허용하는 정책을 생성하는 방법을 보여줍니다.

이 예제에서는 `macie2:GetFindings` 및 `macie2:GetFindingStatistics` 권한을 통해 사용자가 Amazon Macie API 또는 Amazon Macie 콘솔을 사용하여 데이터를 검색할 수 있습니다. `macie2:ListFindings` 권한을 통해 사용자는 Amazon Macie 콘솔의 요약 대시보드 및 조사 결과 페이지를 사용하여 데이터를 검색하고 검토할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

또한 사용자가 조사 결과에 대한 필터 규칙 및 금지 규칙을 생성하고 관리하도록 허용할 수 있습니다. 이렇게 하기 위해, `macie2:CreateFindingsFilter`, `macie2:GetFindingsFilter`, `macie2:UpdateFindingsFilter`, 및 `macie2:DeleteFindingsFilter` 권한을 부여하는 명령문을 포함할 수 있습니다. 사용자가 Amazon Macie 콘솔을 사용하여 규칙을 관리할 수 있게 하려면 정책에 `macie2:ListFindingsFilters` 권한도 포함합니다. 예:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageRules",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindingsFilter",
                "macie2:UpdateFindingsFilter",
                "macie2:CreateFindingsFilter",
                "macie2:DeleteFindingsFilter"
            ],
            "Resource": "arn:aws:macie2:*:*:findings-filter/*"
        },
```

```
        {
            "Sid": "ListRulesOnConsole",
            "Effect": "Allow",
            "Action": "macie2:ListFindingsFilters",
            "Resource": "*"
        }
    ]
}
```

예: 사용자가 태그를 기반으로 사용자 지정 데이터 식별자를 검토할 수 있도록 허용함

ID 기반 정책에서, 조건을 사용하여 태그를 기반으로 Amazon Macie 리소스에 대한 액세스를 제어할 수 있습니다. 이 예제에서는 Amazon Macie Console 또는 Amazon Macie API를 사용하여 사용자가 사용자 지정 데이터 식별자를 검토할 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 하지만 `Owner` 태그가 해당 사용자의 사용자 이름 값을 가지고 있는 경우에만 권한이 부여됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewCustomDataIdentifiersIfOwner",
            "Effect": "Allow",
            "Action": "macie2:GetCustomDataIdentifier",
            "Resource": "arn:aws:macie2:*:*:custom-data-identifier/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListCustomDataIdentifiersOnConsoleIfOwner",
            "Effect": "Allow",
            "Action": "macie2:ListCustomDataIdentifiers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

이 예제에서는 사용자 이름 `richard-roe`를 가진 사용자가 사용자 지정 데이터 식별자의 세부 정보를 검토하려는 경우 사용자 지정 데이터 식별자에 `Owner=richard-roe` 또는 `owner=richard-roe` 태

그를 지정해야 합니다. 그렇지 않으면 사용자는 액세스가 거부됩니다. 조건 키 이름은 대/소문자를 구분하지 않기 때문에 태그 키 `Owner`는 `Owner` 및 `owner` 모두와 일치합니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

Amazon Macie의 서비스 연결 역할

Amazon Macie는 이름이 지정된 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. `AWSServiceRoleForAmazonMacie` 서비스 연결 역할은 Macie에 직접 연결된 고유한 IAM 역할입니다. Macie가 미리 정의한 것으로, Macie가 사용자를 대신하여 다른 AWS 서비스 사람에게 전화를 걸고 리소스를 모니터링하는 데 필요한 모든 권한이 포함되어 있습니다. AWS Macie는 AWS 리전 Macie를 사용할 수 있는 모든 리전에서 이 서비스 연결 역할을 사용합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Macie를 더 쉽게 설정할 수 있습니다. Macie에서 이 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한, Macie만이 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

사용자는 권한을 구성하여 IAM 엔터티(사용자나 역할과 같은)가 서비스 연결 역할을 작성하고 편집하거나 삭제해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하십시오. 사용자가 관련 리소스를 삭제한 후해야 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스을(를) 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾아보세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크에 예를 선택합니다.

주제

- Amazon Macie에 대한 서비스 연결 역할 권한
- Amazon Macie에 대한 서비스 연결 역할 생성
- Amazon Macie에 대한 서비스 연결 역할 편집
- Amazon Macie에 대한 서비스 연결 역할 삭제
- Amazon Macie 서비스 연결 역할 AWS 리전 지원

Amazon Macie에 대한 서비스 연결 역할 권한

Amazon Macie는 `AWSServiceRoleForAmazonMacie`라는 이름의 서비스 연결 역할을 사용합니다. 이 서비스 연결 역할은 `macie.amazonaws.com` 서비스를 그 역할을 맡도록 맡깁니다.

그 역할에 대한 권한 정책은 AmazonMacieServiceRolePolicy라는 이름이며, Macier로 하여금 지정된 리소스에서 다음과 같은 작업 수행을 허용합니다.

- Amazon S3 작업을 사용하여 S3 버킷 및 객체에 대한 정보를 검색할 수 있습니다.
- Amazon S3 작업을 사용하여 S3 객체를 검색합니다.
- AWS Organizations 작업을 사용하여 관련 계정에 대한 정보를 검색할 수 있습니다.
- Amazon CloudWatch Logs 작업을 사용하여 민감한 데이터 검색 작업에 대한 이벤트를 기록할 수 있습니다.

역할은 다음과 같은 권한 정책으로 구성됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "*"
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

AmazonMacieServiceRolePolicy 정책의 업데이트에 대한 자세한 정보는 AWS 관리형 정책에 대한 Amazon Macie 업데이트 섹션을 참조하세요. 이 정책의 변경 사항에 대한 자동 알림을 받으려면 Macie 문서 기록 페이지에서 RSS 피드를 구독하십시오.

사용자는 권한을 구성하여 IAM 엔터티(사용자나 역할과 같은)가 서비스 연결 역할을 작성하고 편집하거나 삭제해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하십시오.

Amazon Macie에 대한 서비스 연결 역할 생성

Amazon Macie를 위해 AWSServiceRoleForAmazonMacie 서비스 연결 역할을 수동으로 생성할 필요가 없습니다. 사용자를 위해 Macie를 활성화하면 Macie가 자동으로 서비스 연결 역할을 생성합니다. AWS 계정

Macie 서비스 연결 역할을 삭제 후에 다시 생성해야 하는 경우, 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. Macie를 다시 활성화하면 Macie가 서비스 연결 역할을 다시 생성합니다.

Amazon Macie에 대한 서비스 연결 역할 편집

Amazon Macie는 사용자가 AWSServiceRoleForAmazonMacie 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할이 생성된 후, 여러 엔터티가 역할을 참조할 수 있으므로, 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하십시오.

Amazon Macie에 대한 서비스 연결 역할 삭제

Amazon Macie를 더 이상 사용하지 않을 경우에는 수동으로 AWSServiceRoleForAmazonMacie 서비스 연결 역할을 삭제하는 것이 좋습니다. Macie를 비활성화해도 Macie는 사용자를 위한 역할을 삭제하지 않습니다.

역할을 삭제하기 전에 역할을 활성화한 각 AWS 리전 위치에서 Macie를 비활성화해야 합니다. 또한 역할의 리소스를 수동으로 정리해야 합니다. 역할을 삭제하려면 IAM 콘솔 AWS CLI, 또는 API를 사용할 수 있습니다. AWS 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 삭제를 참조하세요.

> **Note**
>
> 사용자가 리소스를 삭제할 때 Macie가 AWSServiceRoleForAmazonMacie 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

사용자가 AWSServiceRoleForAmazonMacie서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우, 계정에서 Macie 기능을 활성화하여 다시 생성할 수 있습니다. Macie를 다시 활성화하면 Macie가 서비스 연결 역할을 다시 생성합니다.

Amazon Macie 서비스 연결 역할 AWS 리전 지원

Amazon Macie는 AWSServiceRoleForAmazonMacie Macie를 사용할 수 AWS 리전 있는 모든 지역에서 서비스 연결 역할을 사용할 수 있도록 지원합니다. 현재 Macie를 사용할 수 있는 모든 리전 목록은 AWS 일반 참조의 Amazon Macie 및 엔드포인트 및 할당량을 참조하세요.

Amazon Macie에 대한 AWS 관리형 정책

AWS 관리형 정책은 AWS에 의해 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있기 때문에 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. AWS에서 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새로운 AWS 서비스를 시작하거나 새로운 API 작업을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

Amazon Macie는 `AmazonMacieFullAccess` 정책, `AmazonMacieReadOnlyAccess` 정책 및 `AmazonMacieServiceRolePolicy` 정책 등 여러 AWS 관리형 정책을 제공합니다.

주제

- AWS 관리형 정책: AmazonMacieFullAccess
- AWS 관리형 정책: AmazonMacieReadOnlyAccess
- AWS 관리형 정책: AmazonMacieServiceRolePolicy
- AWS 관리형 정책에 대한 Amazon Macie 업데이트

AWS 관리형 정책: AmazonMacieFullAccess

`AmazonMacieFullAccess` 정책을 IAM 엔터티에 연결할 수 있습니다.

이 정책은 IAM 자격 증명(보안 주체)이 Amazon Macie 서비스 연결 역할을 생성하고 Amazon Macie에 대한 모든 읽기 및 쓰기 작업을 수행할 수 있도록 허용하는 전체 관리 권한을 부여합니다. 권한에는 생성, 업데이트 및 삭제와 같은 변경 기능이 포함됩니다. 이 정책을 보안 주체와 연결하면 보안 주체는 자신의 계정에 대한 모든 Macie 리소스, 데이터 및 설정을 만들고 검색하며 액세스할 수 있습니다.

보안 주체가 자신의 계정에 대해 Macie를 활성화하려면 먼저 이 정책을 보안 주체에 연결해야 합니다. 즉, 보안 주체가 Macie를 계정에 사용하도록 설정하려면 Macie 서비스 연결 역할을 만들 수 있어야 합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `macie2` – 보안 주체가 Amazon Macie에 대한 모든 읽기 및 쓰기 작업을 수행할 수 있도록 허용합니다.
- `iam` – 보안 주체가 서비스 연결 역할을 생성할 수 있도록 허용합니다. `Resource` 요소는 Macie의 서비스 연결 역할을 지정합니다. `Condition` 요소는 `iam:AWSServiceName` 조건 키와 `StringLike` 조건 연산자를 사용하여 Macie의 서비스 연결 역할에 대한 권한을 제한합니다.
- `pricing` – 보안 주체가 AWS Billing and Cost Management에서 AWS 계정의 가격 데이터를 검색할 수 있습니다. Macie는 이 데이터를 사용하여 보안 주체가 민감한 데이터 검색 작업을 생성하고 구성할 때 예상 비용을 계산하고 표시합니다.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:*"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "macie.amazonaws.com"
            }
         }
      },
      {
         "Effect": "Allow",
         "Action": "pricing:GetProducts",
         "Resource": "*"
      }
```

```
   ]
}
```

AWS 관리형 정책: AmazonMacieReadOnlyAccess

`AmazonMacieReadOnlyAccess` 정책을 IAM 엔터티에 연결할 수 있습니다.

이 정책은 IAM 자격 증명(보안 주체)이 Amazon Macie에 대한 모든 읽기 작업을 수행할 수 있도록 하는 읽기 전용 권한을 부여합니다. 권한에는 생성, 업데이트 또는 삭제와 같은 변경 기능이 포함되지 않습니다. 이 정책을 보안 주체와 연결하면 보안 주체는 자신의 계정에 대한 모든 Macie 리소스, 데이터 및 설정을 검색할 수 있지만 그렇지 않은 경우에는 액세스할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

`macie2` – 보안 주체가 Amazon Macie에 대한 모든 읽기 작업을 수행하도록 허용합니다.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:Describe*",
            "macie2:Get*",
            "macie2:List*",
            "macie2:BatchGetCustomDataIdentifiers",
            "macie2:SearchResources"
         ],
         "Resource": "*"
      }
   ]
}
```

AWS 관리형 정책: AmazonMacieServiceRolePolicy

AmazonMacieServiceRolePolicy 정책을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Macie에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 내용은 Amazon Macie의 서비스 연결 역할 섹션을 참조하세요.

AWS 관리형 정책에 대한 Amazon Macie 업데이트

이 서비스가 이러한 변경 내용을 추적하기 시작한 이후부터 Amazon Macie의 AWS 관리형 정책 업데이트에 대한 세부 정보를 검토합니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Macie 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AmazonMacieReadOnlyAccess – 새 정책 추가됨	Macie 가 새 정책인 AmazonMacieReadOnlyAccess 정책을 추가했습니다. 이 정책은 보안 주체가 자신의 계정에 대한 모든 Macie 리소스, 데이터 및 설정을 검색할 수 있는 읽기 전용 권한을 부여합니다.	2023년 6월 15일
AmazonMacieFullAccess – 기존 정책 업데이트됨	AmazonMacieFullAccess 정책에서 Macie 서비스 연결 역할(aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie)의 Amazon 리소스 이름(ARN) 을 업데이트했습니다.	2022년 6월 30일
AmazonMacieServiceRolePolicy – 기존 정책 업데이트됨	Macie는 AmazonMacieServiceRolePolicy 정책에서 Amazon Macie Classic에 대한 작업 및 리소스를 삭제했습니다. Amazon	2022년 5월 20일

변경 사항	설명	날짜
	Macie Classic은 단종되어 더 이상 사용할 수 없습니다. 더 구체적으로 말하자면, Macie는 모든 AWS CloudTrail 작업을 제거했습니다. 또한 Macie는 다음 리소스에 대한 모든 Amazon S3 작업을 제거했습니다: `arn:aws:s3:::awsmaciecie-*` , `arn:aws:s3:::awsmacietrail-*` 및 `arn:aws:s3:::*-awsmacietrail-*` .	
AmazonMacieFullAccess – 기존 정책 업데이트됨	Macie는 `AmazonMacieFullAccess` 정책에 AWS Billing and Cost Management(`pricing`) 작업을 추가했습니다. 이 작업을 통해 보안 주체가 자신의 계정에 대한 가격 데이터를 검색할 수 있습니다. Macie는 이 데이터를 사용하여 보안 주체가 민감한 데이터 검색 작업을 생성하고 구성할 때 예상 비용을 계산하고 표시합니다. 또한 Macie는 `AmazonMacieFullAccess` 정책에서 Amazon Macie Classic(`macie`)을 삭제했습니다.	2022년 3월 7일

변경 사항	설명	날짜
AmazonMacieService RolePolicy – 기존 정책 업데이트됨	Macie는 Amazon CloudWatch Logs 작업을 AmazonMacieServiceRolePolicy 정책에 추가했습니다. 이러한 작업을 통해 Macie는 민감한 데이터 검색 작업에 대한 로그 이벤트를 CloudWatch Logs에 게시할 수 있습니다.	2021년 4월 13일
Macie가 변경 사항 추적을 시작함	Macie가 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 4월 13일

Amazon Macie 자격 증명 및 액세스 문제 해결

다음 정보는 Amazon Macie and AWS Identity and Access Management (IAM) 를 사용할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 될 수 있습니다.

주제

- Amazon Macie에서 작업을 수행할 권한이 없음
- 외부 사용자가 내 Amazon Macie AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

Amazon Macie에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojacksonIAM 사용자가 콘솔을 사용하여 가상 *my-example-widget*리소스에 대한 세부 정보를 보려고 하지만 가상 macie2:*GetWidget*권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 macie2:GetWidget on resource: my-example-widget
```

이 경우 macie2:*GetWidget*작업을 사용하여 *my-example-widget*리소스에 액세스할 수 있도록 mateojackson사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 관리자에게 문의하십시오. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 Amazon Macie AWS 계정 리소스에 액세스할 수 있도록 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.

자세히 알아보려면 다음을 참조하십시오.

- Macie에서 이러한 기능을 지원하는지 여부를 알아보려면 Amazon Macie와 호환되는 방식 AWS Identity and Access Management 단원을 참조하세요.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 페더레이션)을 참조하십시오.
- 교차 계정 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

Amazon Macie에서 로깅 및 모니터링

Amazon Macie는 사용자, 역할 또는 다른 AWS 서비스에 의해 Macie에서 수행된 작업의 레코코드를 제공하는 서비스인 AWS CloudTrail와 통합됩니다. 여기에는 Amazon Macie 콘솔에서의 작업과 Amazon Macie API 작업에 대한 프로그래밍 방식의 호출이 포함됩니다. CloudTrail에서 수집한 정보를 사용하여 Macie에 어떤 요청이 수행되었는지 확인할 수 있습니다. 각 요청에 대해 요청이 이루어진 시기, 요청이 이루어진 IP 주소, 요청한 사람 및 추가 세부 정보를 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail을 사용하여 Amazon Macie API 호출 로깅 섹션을 참조하세요.

Amazon Macie에 대한 규정 준수 확인

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- 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— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Amazon Macie의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 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.

Amazon Macie의 인프라 보안

관리형 서비스인 Amazon Macie는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스와 AWS의 인프라 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안에 대한 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS에서 게시한 API 호출을 사용하여 네트워크를 통해 Macie에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(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.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 보안 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

Amazon Macie 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

Amazon Virtual Private Cloud(VPC)를 사용하여 AWS 리소스를 호스트하는 경우, VPC와 Amazon Macie 간에 프라이빗 연결을 설정할 수 있습니다. Amazon VPC란 사용자가 정의한 가상 네트워크에서 AWS 리소스를 시작할 때 사용할 수 있는 AWS 서비스입니다. VPC를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다.

VPC를 Macie에 연결하려면 Macie에 대해 인터페이스 VPC 엔드포인트를 정의하십시오. 인터페이스 엔드포인트는 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 비공

개로 Amazon Macie에 액세스할 수 있도록 지원하는 AWS PrivateLink 기술로 구동됩니다. VPC의 인스턴스는 Amazon Macie API와 통신하는 데 퍼블릭 IP 주소를 필요로 하지 않습니다. VPC와 Macie 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 탄력적 네트워크 인터페이스로 표현됩니다. 자세한 정보는 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트를 사용하여 AWS 서비스에 액세스를 참조하세요.

주제

- Amazon Macie VPC 엔드포인트에 대한 고려 사항
- Amazon Macie에 대한 인터페이스 VPC 엔드포인트 생성

Amazon Macie VPC 엔드포인트에 대한 고려 사항

Amazon Macie는 아시아 태평양(오사카)과 이스라엘(텔아비브) 리전을 제외하고 현재 사용 가능한 모든 AWS 리전에서 VPC 엔드포인트를 지원합니다. 현재 Macie를 사용할 수 있는 모든 리전 목록은 AWS 일반 참조의 Amazon Macie 및 엔드포인트 및 할당량을 참조하세요. 또한 Macie는 VPC에서 모든 API 작업에 대한 호출 수행을 지원합니다.

Macie용 인터페이스 VPC 엔드포인트를 생성하는 경우, VPC 지원을 제공하고 Macie와 통합하는 Amazon EventBridge와 AWS 서비스 같은 다른 AWS Security Hub에도 동일한 작업을 수행하는 것을 고려해 보세요. 그러면 Macie와 해당 서비스가 통합을 위해 VPC 엔드포인트를 사용할 수 있습니다. 예를 들어 Macie용 VPC 엔드포인트와 Security Hub용 VPC 엔드포인트를 생성하는 경우, Macie는 Security Hub에 조사 결과를 게시할 때 VPC 엔드포인트를 사용할 수 있으며, Security Hub는 조사 결과를 수신할 때 VPC 엔드포인트를 사용할 수 있습니다. VPC 엔드포인트를 지원하는 서비스에 대한 자세한 내용은 Amazon VPC 사용 설명서의 AWS PrivateLink와 통합된 AWS 서비스 섹션을 참조하세요.

추가 고려 사항은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트를 사용하여 AWS 서비스에 액세스 섹션을 참조하세요.

Macie에 대한 VPC 엔드포인트 정책이 지원됩니다. 기본적으로 엔드포인트를 통해 Macie에 대한 전체 액세스가 허용됩니다. 자세한 내용은 Amazon VPC 사용 설명서의VPC 엔드포인트 및 VPC 엔드포인트 서비스에 대한 ID 및 액세스 관리 섹션을 참조하세요.

Amazon Macie에 대한 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔이나 AWS Command Line Interface(AWS CLI)을(를) 사용하여 Amazon Macie 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다. 자세한 정보는 Amazon VPC 사용 설명서의 VPC 엔드포인트 생성을 참조하세요.

Macie용 VPC 엔드포인트를 생성하려면 다음 서비스 이름을 사용합니다.

- com.amazonaws.*region*.macie2

여기서 *region*은 해당 AWS 리전의 리전 코드입니다.

엔드포인트에 프라이빗 DNS를 사용하도록 설정하는 경우, 리전에 대한 기본 DNS 이름(예: `macie2.us-east-1.amazonaws.com` 미국 동부(버지니아 북부) 리전)을 사용하여 Macie에 API 요청을 할 수 있습니다.

자세한 정보는 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트를 사용하여 AWS 서비스에 액세스를 참조하세요.

AWS CloudTrail을 사용하여 Amazon Macie API 호출 로깅

Amazon Macie는 사용자, 역할 또는 다른 AWS 서비스에 의해 Macie에서 수행된 작업의 레코코드를 제공하는 서비스인 AWS CloudTrail와 통합됩니다. CloudTrail은 Macie에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Amazon Macie 콘솔에서의 직접 호출과 Amazon Macie API 작업에 대한 프로그래밍 방식의 직접 호출이 포함되어 있습니다.

추적을 생성하면, Macie에 대한 이벤트를 포함한 CloudTrail 이벤트를 Amazon Simple Storage Service(S3) 버킷에 지속적으로 전송할 수 있습니다. 추적을 구성하지 않은 경우에도 AWS CloudTrail 콘솔에서 이벤트 기록을 사용하여 가장 최근의 이벤트를 검토할 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Macie에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

주제

- AWS CloudTrail의 Amazon Macie 정보
- Amazon Macie 로그 파일 항목 이해

AWS CloudTrail의 Amazon Macie 정보

AWS CloudTrail은 계정 생성 시 AWS 계정에 대해 활성화됩니다. Amazon Macie에서 활동이 발생하면, 해당 활동이 이벤트 기록의 다른 AWS 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 검토, 검색 및 다운로드할 수 있습니다. 자세한 설명은 AWS CloudTrail 사용 설명서의 CloudTrail 이벤트 기록 작업을 참조하세요.

Macie에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면, 추적을 생성합니다. CloudTrail은 추적(trail)을 사용하여 Amazon Simple Storage Service(Amazon S3) 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로, AWS CloudTrail 콘솔을 사용하여 추적을 생성할 때 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서에서 다음 주제를 참조하십시오.

- AWS 계정에 대한 추적 생성
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성

- 여러 리전에서 CloudTrail 로그 파일 수신
- 여러 계정에서 CloudTrail 로그 파일 수신

모든 Macie 작업은 CloudTrail에서 로깅되며 Amazon Macie API 참조에 설명되어 있습니다. 예를 들어 `CreateClassificationJob`, `DescribeBuckets`, `ListFindings` 작업을 직접적으로 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 보안 인증 정보로 했는지
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail userIdentity 요소를 참조하세요.

Amazon Macie 로그 파일 항목 이해

추적은 이벤트를 지정한 Amazon Simple Storage Service(Amazon S3) 버킷에 로그 파일로 전송할 수 있도록 하는 구성입니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 포함되어 있습니다. AWS CloudTrail 로그 파일에는 이벤트에 대한 하나 이상의 로그 항목이 포함되어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제에서는 Amazon Macie 작업에 대한 이벤트를 보여주는 CloudTrail 로그 항목을 보여줍니다. 로그 항목에 포함될 수 있는 정보에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 로그 이벤트 참조를 참조하세요.

예: 리스팅 조사 결과

다음 예는 Macie ListFindings 작업에 대한 이벤트를 보여주는 CloudTrail 로그 항목을 보여줍니다. 이 예에서는 AWS Identity and Access Management(IAM) 사용자(`Mary_Major`)가 Amazon Macie 콘솔을 사용하여 계정에 대한 현재 정책 조사 결과에 대한 일부 정보를 검색했습니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext":{
            "attributes": {
                "creationdate": "2023-11-14T15:49:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-14T16:09:56Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "ListFindings",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "sortCriteria": {
            "attributeName": "updatedAt",
            "orderBy": "DESC"
        },
        "findingCriteria": {
            "criterion": {
                "archived": {
                    "eq": [
                        "false"
                    ]
                },
                "category": {
                    "eq": [
                        "POLICY"
                    ]
                }
            }
        },
        "maxResults": 25,
        "nextToken": ""
    },
    "responseElements": null,
    "requestID": "d58af6be-1115-4a41-91f8-ace03example",
```

```
    "eventID": "ad97fac5-f7cf-4ff9-9cf2-d0676example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

예: 조사 결과의 민감한 데이터 샘플 검색

이 예는 Macie가 발견하여 보고한 민감한 데이터의 샘플을 검색하고 공개하는 이벤트를 보여주는 CloudTrail 로그 항목을 보여줍니다. 이 예제에서는 IAM 사용자(JohnDoe)가 Amazon Macie 콘솔을 사용하여 민감한 데이터 샘플을 검색하고 공개했습니다. 사용자의 Macie 계정은 민감한 데이터 샘플을 검색하고 공개하기 위해 IAM 역할(MacieReveal)을 수임하도록 구성됩니다.

다음 로그 이벤트는 Macie GetSensitiveDataOccurrences 작업을 수행하여 민감한 데이터 샘플을 검색하고 공개하려는 사용자의 요청에 대한 세부 정보를 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "UU4MH7OYK5ZCOAEXAMPLE:JohnDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/JohnDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "UU4MH7OYK5ZCOAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-12-12T14:40:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "macie2.amazonaws.com",
```

```
    "eventName": "GetSensitiveDataOccurrences",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.252",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "findingId": "3ad9d8cd61c5c390bede45cd2example"
    },
    "responseElements": null,
    "requestID": "c30cb760-5102-47e7-88d8-ff2e8example",
    "eventID": "baf52d92-f9c3-431a-bfe8-71c81example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

다음 로그 이벤트는 Macie가 AWS Security Token Service(AWS STS) AssumeRole 작업을 수행하여 지정된 IAM 역할(`MacieReveal`)을 수임하는 것에 대한 세부 정보를 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "reveal-samples.macie.amazonaws.com"
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "reveal-samples.macie.amazonaws.com",
    "userAgent": "reveal-samples.macie.amazonaws.com",
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/MacieReveal",
        "roleSessionName": "RevealCrossAccount"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionToken": "XXYYaz...
EXAMPLE_SESSION_TOKEN
XXyYaZAz",
```

```
            "expiration": "Dec 12, 2023, 6:04:47 PM"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROAXOTKAROCSNEXAMPLE:RevealCrossAccount",
            "arn": "arn:aws:sts::111122223333:assumed-role/MacieReveal/
RevealCrossAccount"
        }
    },
    "requestID": "d905cea8-2dcb-44c1-948e-19419example",
    "eventID": "74ee4d0c-932d-3332-87aa-8bcf3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::IAM::Role",
            "ARN": "arn:aws:iam::111122223333:role/MacieReveal"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Amazon Macie에 리소스 태그 지정

태그는 특정 유형의 Amazon Macie 리소스를 포함한 AWS 리소스를 선택적으로 정의하고 연결하는 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

허용 목록, 사용자 지정 데이터 식별자, 조사 결과에 대한 필터 규칙 및 억제 규칙, 민감한 데이터 검색 작업 등의 Macie 리소스 유형에 태그를 할당할 수 있습니다. 조직의 Macie 관리자인 경우, 조직의 멤버 계정에도 태그를 할당할 수 있습니다.

주제

태그 지정 기본 사항

리소스는 최대 50개의 태그를 가질 수 있습니다. 각 태그는 사용자가 정의하는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그 키는 더 구체적인 태그 값에 대해 카테고리와 같은 역할을 하는 일반적인 레이블입니다. 태그 값은 태그 키에 대한 설명자 역할을 합니다.

예를 들어, 사용자 지정 데이터 식별자와 민감한 데이터 검색 작업을 만들어 워크플로의 여러 지점(한 세트는 스테이징된 데이터용, 다른 하나는 프로덕션 데이터용)에서 데이터를 분석하는 경우, 해당 리소스에 `Stack` 태그 키를 할당할 수 있습니다. 이 태그 키의 태그 값은 사용자 지정 데이터 식별자와 스테이징된 데이터를 분석하도록 설계된 작업의 경우, `Staging`, 다른 경우에는 `Production`일 수 있습니다.

태그를 정의하고 리소스에 할당할 때 다음 사항에 유의하세요.

- 각 리소스는 최대 50개의 태그를 보유할 수 있습니다.

- 각 리소스에 대해 각 태그 키는 고유하며 하나의 값만 가질 수 있습니다.
- 태그 키와 값은 대/소문자를 구분합니다. 모범적으로는 태그를 대문자로 사용하는 전략을 세우고 이러한 전략을 모든 리소스 유형에 대해 일관되게 구현하는 것이 좋습니다.
- 태그 키는 최대 128개의 UTF-8 문자를 포함할 수 있습니다. 태그 값은 최대 256 UTF-8 문자를 포함할 수 있습니다. 문자는 문자, 숫자, 공백 또는 _ . : / = + - @ 기호일 수 있습니다.
- `aws:` 접두사는 AWS용으로 예약되어 있습니다. 정의한 태그 키나 값에는 이를 사용할 수 없습니다. 또는 이 접두사를 사용하는 태그 키 또는 값을 변경하거나 제거할 수 없습니다. 이 접두사를 사용하는 태그는 리소스당 50개의 할당량에 포함되지 않습니다.
- 할당한 모든 태그는 사용자의 AWS 계정에서와 태그를 할당하는 AWS 리전에서만 사용할 수 있습니다.
- 리소스를 삭제하면, 리소스에 할당된 태그 또한 삭제됩니다.

추가 제한 사항, 팁, 모범 사례는 AWS 리소스 태깅 사용 설명서를 참조하세요.

> **Important**
>
> 기밀 또는 기타 유형의 민감한 데이터를 태그에 저장하지 마세요. AWS Billing and Cost Management을(를) 비롯한 여러 AWS 서비스에서 태그에 액세스할 수 있습니다. 태그는 민감한 데이터에 사용하기 위한 것이 아닙니다.

Macie 리소스에 태그를 추가하고 관리하려면 Amazon Macie 콘솔, Amazon Macie API, AWS Resource Groups 콘솔의 태그 편집기 또는 AWS Resource Groups 태그 지정 API를 사용할 수 있습니다. Macie와 함께라면 리소스를 만들 때 태그를 리소스에 추가할 수 있습니다. 개별 기존 리소스의 태그를 추가하고 관리할 수도 있습니다. 리소스 그룹을 사용하면 Macie를 포함하여 여러 AWS 서비스에 걸쳐 있는 여러 기존 리소스에 대해 대량으로 태그를 추가하고 관리할 수 있습니다. 자세한 내용을 알아보려면 AWS 리소스 태깅 사용 설명서를 참조하세요.

IAM 정책에서 태그 사용

리소스에 태그를 지정한 후 AWS Identity and Access Management(IAM)정책에서 태그 기반의 리소스 수준 권한을 정의할 수 있습니다. 이런 식으로 태그를 사용하면 리소스 생성 및 태그 지정할 권한을 가질 AWS 계정 사용자와 역할은 물론, 보다 일반적으로 태그를 생성, 편집 및 제거할 권한을 가질 사용자와 역할을 세부적으로 제어할 수 있습니다. 태그를 기반으로 액세스를 제어하려면 IAM 정책의 조건 요소에서 태그 관련 조건 키를 사용할 수 있습니다.

예를 들어, 사용자가 이름이 리소스의 Owner 태그 값인 모든 Amazon Macie 리소스에 대한 전체 액세스 권한을 갖도록 허용하는 정책을 생성할 수 있습니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "macie2:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

태그 기반의 리소스 수준 권한을 정의하면 권한이 즉시 적용됩니다. 즉 리소스를 생성하자마자 더 안전하게 보호할 수 있으며 새 리소스에 태그 사용 적용을 빠르게 시작할 수 있습니다. 리소스 수준 권한을 사용하여 새 리소스 및 기존 리소스와 연결할 수 있는 태그 키와 값을 제어할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 태그를 사용하여 AWS 리소스에 대한 액세스 제어를 참조하세요.

Amazon Macie 리소스에 태그 추가

개별 Amazon Macie 리소스에 태그를 추가하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용하면 됩니다. 여러 Macie 리소스에 동시에 태그를 추가하려면 AWS Resource Groups 콘솔의 태그 편집기를 사용하거나 AWS Resource Groups API 태그 지정의 태그 지정 작업을 사용합니다.

> **Important**
>
> 리소스에 태그를 추가하면 리소스에 대한 액세스에 영향을 줄 수 있습니다. 리소스에 태그를 추가하기 전에 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 모든 AWS Identity and Access Management(IAM)정책을 검토하세요.

Console

허용 목록, 사용자 지정 데이터 식별자 또는 민감한 데이터 검색 작업을 생성할 때 Amazon Macie 콘솔은 리소스에 태그를 추가하는 옵션을 제공합니다. 리소스를 생성할 때 콘솔의 지침에 따라 이

러한 유형의 리소스에 태그를 추가합니다. 필터 또는 억제 규칙 또는 조직의 멤버 계정에 태그를 추가하려면 먼저 리소스를 만들어야 태그를 추가할 수 있습니다.

Amazon Macie 콘솔을 사용하여 기존 리소스에 하나 이상의 태그를 추가하려면 다음 단계를 따르세요.

리소스에 태그를 추가합니다.

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 태그를 추가하고 싶은 리소스 유형에 따라 다음 중 하나를 수행합니다.

   - 허용 목록을 보려면 탐색 창에서 허용 목록을 선택합니다.

     그런 다음, 테이블에서 목록의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
   - 사용자 지정 데이터 식별자의 경우, 탐색 창에서 사용자 지정 데이터 식별자를 선택합니다.

     그런 다음, 테이블에서 사용자 지정 데이터 식별자의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
   - 필터 또는 억제 규칙의 경우, 탐색 창에서 조사 결과를 선택합니다.

     그런 다음, 저장된 규칙 목록에서 규칙 옆에 있는 편집 아이콘
     (
)
     을 선택합니다. 태그 관리를 선택합니다.
   - 조직의 멤버 계정인 경우, 탐색 창에서 계정을 선택합니다.

     그런 다음, 테이블에서 계정의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
   - 민감한 데이터 검색 작업의 경우, 탐색 창에서 작업을 선택합니다.

     그런 다음, 테이블에서 작업의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.

   태그 관리 창에는 현재 리소스에 할당된 모든 태그가 나열됩니다.
3. 태그 관리 창에서 태그 편집을 선택합니다.
4. 태그 추가를 선택합니다.
5. 키 상자에 리소스에 추가할 태그의 태그 키를 입력합니다. 그런 다음, 값 상자에서 키에 대한 태그 값을 입력합니다(선택 사항).

태그 키에는 최대 128자를 사용할 수 있습니다. 태그 값에는 최대 256자를 사용할 수 있습니다. 문자는 문자, 숫자, 공백 또는 _ . : / = + - @ 기호일 수 있습니다.

6. (선택 사항) 다른 리소스를 추가하려면 태그 추가를 선택한 다음 이전 단계를 반복합니다. 리소스에 최대 50개의 태그를 할당할 수 있습니다.
7. 태그 추가가 완료되면 저장을 선택합니다.

API

리소스를 만들고 프로그래밍 방식으로 하나 이상의 태그를 추가하려면 만들려는 리소스 유형에 맞는 `Create` 작업을 사용합니다.

- 허용 목록 - CreateAllowList 작업을 사용하거나 AWS Command Line Interface(AWS CLI)를 사용하는 경우, create-allow-list 명령을 실행합니다.
- 사용자 지정 데이터 식별자 - CreateCustomDataIdentifier 작업을 사용하거나, AWS CLI를 사용하는 경우, create-custom-data-identifier 명령을 실행합니다.
- 필터 또는 억제 규칙 - CreateFindingsFilter 작업을 사용하거나, AWS CLI를 사용하는 경우, create-findings-filter 명령을 실행합니다.
- 멤버 계정 - CreateMember 작업을 사용하거나, AWS CLI를 사용하는 경우, create-member 명령을 실행합니다.
- 민감한 데이터 검색 작업 - CreateClassificationJob 작업을 사용하거나, AWS CLI을(를) 사용하는 경우, create-classification-job 명령을 실행합니다.

요청에서 `tags` 파라미터를 사용하여 리소스에 추가할 각 태그의 태그 키(`key`)와 선택적 태그 값(`value`)을 지정합니다. `tags` 파라미터는 태그 키와 연결된 태그 값의 문자열 간 맵을 지정합니다.

기존 리소스에 하나 이상의 태그를 추가하려면 Amazon Macie API의 TagResource 작업을 사용하거나, AWS CLI을(를) 사용하는 경우, tag-resource 명령을 실행합니다. 요청에서 태그를 추가하려는 리소스의 Amazon 리소스 이름(ARN)을 지정합니다. `tags` 파라미터를 사용하여 리소스에 추가할 각 태그의 태그 키(`key`)와 선택적 태그 값(`value`)을 지정합니다. `Create` 작업 및 명령의 경우와 마찬가지로 `tags` 파라미터는 태그 키와 관련 태그 값의 문자열 간 맵을 지정합니다.

예를 들어, 다음 AWS CLI 명령은 지정된 작업에 `Production` 태그 값을 가진 `Stack` 태그 키를 추가합니다. 이 예제는 Microsoft Windows용으로 포맷되었으며 가독성을 높이기 위해 캐럿(^) 줄 연속 문자를 사용합니다.

```
C:\> aws macie2 tag-resource ^
```

```
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\"}
```

위치:

- `resource-arn`은(는) 태그를 추가할 작업의 ARN을 지정합니다.
- *Stack*은(는) 작업에 추가할 태그의 태그 키입니다.
- *Production*은(는) 지정된 태그 키(*Stack*)의 태그 값입니다.

다음 예제에서 명령은 작업에 여러 태그를 추가합니다.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\",\"CostCenter\":\"12345\",\"Owner\":\"jane-doe\"}
```

`tags` 맵의 각 태그에는 `key` 및 `value` 인수가 모두 필요합니다. 그러나 `value` 인수 값은 빈 문자열일 수도 있습니다. 태그 값을 태그 키와 연결하지 않으려면 `value` 인수 값을 지정하지 마세요. 예를 들어 다음 AWS CLI 명령은 관련 태그 값이 없는 `Owner` 태그 키를 추가합니다.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Owner\":\"\"}
```

태그 지정 작업이 성공하면 Macie는 빈 HTTP 204 응답을 반환합니다. 그렇지 않으면 Macie는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

Amazon Macie 리소스의 태그 검토

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여 Amazon Macie 리소스의 태그(태그 키와 태그 값 모두)를 검토할 수 있습니다. 여러 Macie 리소스에 대해 동시에 이 작업을 수행하려는 경우, AWS Resource Groups 콘솔의 태그 편집기를 사용하거나 AWS Resource Groups API 태그 지정의 태그 지정 작업을 사용할 수 있습니다.

Console

다음 단계에 따라 Amazon Macie 콘솔을 사용하여 리소스 태그를 검토합니다.

리소스의 태그를 검토하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 태그를 검토할 리소스의 유형에 따라 다음 중 하나를 수행합니다.

   - 허용 목록을 보려면 탐색 창에서 허용 목록을 선택합니다.

     그런 다음, 테이블에서 목록의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
   - 사용자 지정 데이터 식별자의 경우, 탐색 창에서 사용자 지정 데이터 식별자를 선택합니다.

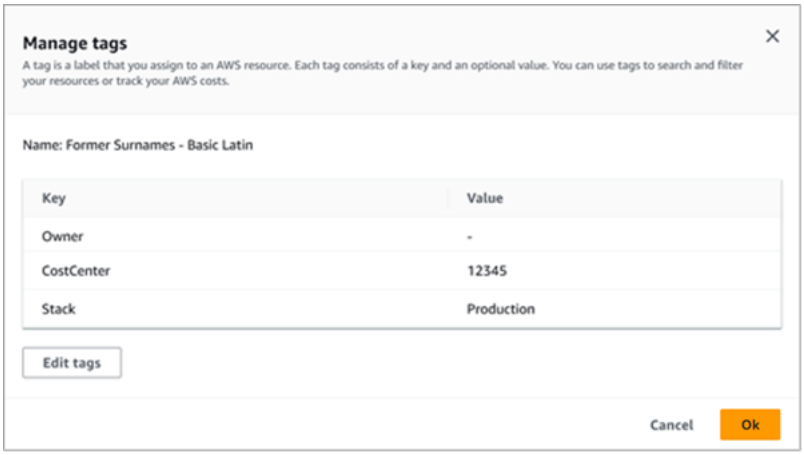
     그런 다음, 테이블에서 사용자 지정 데이터 식별자의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
   - 필터 또는 억제 규칙의 경우, 탐색 창에서 조사 결과를 선택합니다.

     그런 다음, 저장된 규칙 목록에서 규칙 옆에 있는 편집 아이콘 ()을 선택합니다. 태그 관리를 선택합니다.
   - 조직의 멤버 계정인 경우, 탐색 창에서 계정을 선택합니다.

     그런 다음, 테이블에서 계정의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
   - 민감한 데이터 검색 작업의 경우, 탐색 창에서 작업을 선택합니다.

     그런 다음, 테이블에서 작업의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.

태그 관리 창에는 현재 리소스에 할당된 모든 태그가 나열됩니다. 예를 들어 다음 이미지는 사용자 지정 데이터 식별자에 할당된 태그를 보여줍니다.



이 예제에서는 사용자 지정 데이터 식별자에 다음 세 가지 태그가 할당되어 있습니다. 연결된 태그 값이 없는 소유자 태그 키, 연결된 태그 값이 12345인 CostCenter 태그 키, 연결된 태그 값이 프로덕션인 Stack 태그 키.

3. 태그 검토를 마치면 취소를 선택하여 창을 닫습니다.

API

프로그래밍 방식으로 기존 리소스의 태그를 검색하고 검토하려면 태그를 검토하려는 리소스 유형에 적합한 `Get` 또는 `Describe` 작업을 사용할 수 있습니다. 예를 들어 GetCustomDataIdentifier 작업을 사용하거나 AWS Command Line Interface(AWS CLI)에서 get-custom-data-identifier 명령을 실행하면 응답에 `tags` 객체가 포함됩니다. 객체에는 현재 리소스에 할당된 모든 태그(태그 키와 태그 값 모두)가 나열됩니다.

Amazon Macie API의 ListTagsForResource 작업을 사용할 수도 있습니다. 요청에서 `resourceArn` 파라미터를 사용하여 리소스의 Amazon 리소스 이름(ARN)을 지정합니다. AWS CLI을(를) 사용하는 경우, list-tags-for-resource 명령을 실행하고 `resource-arn` 파라미터를 사용하여 리소스의 ARN을 지정합니다. 예:

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

위 예제에서 *arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample*은 기존의 민감한 데이터 검색 작업의 ARN입니다.

작업이 성공하면 Macie는 현재 리소스에 할당된 모든 태그(태그 키와 태그 값 모두)를 나열하는 `tags` 객체를 반환합니다. 예:

```
{
    "tags": {
        "Stack": "Production",
        "CostCenter": "12345",
        "Owner": ""
    }
}
```

여기서 Stack, CostCenter, Owner은(는) 리소스에 할당된 태그 키입니다. Production은(는) Stack 태그 키에 연결된 태그 값입니다. 12345은(는) CostCenter 태그 키에 연결된 태그 값입니다. Owner 태그 키에는 연결된 태그 값이 없습니다.

태그가 있는 모든 Macie 리소스의 목록과 이러한 각 리소스와 연결된 모든 태그를 검색하려면, AWS Resource Groups 태그 지정 API의 GetResources 작업을 사용하십시오. 요청에서 ResourceTypeFilters 파라미터 값을 macie2로 설정합니다. AWS CLI을(를) 사용하여 이 작업을 수행하려면 get-resources 명령을 실행하고 resource-type-filters 파라미터 값을 macie2로 설정합니다. 예:

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

작업이 성공하면 리소스 그룹은 태그가 있는 모든 Macie 리소스의 ARN과 해당 리소스 각각에 할당된 태그 키 및 값이 포함된 ResourceTagMappingList 배열을 반환합니다.

Amazon Macie 리소스의 태그 편집

Amazon Macie 리소스의 태그(태그 키 또는 태그 값)를 편집하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 여러 Macie 리소스에서 동시에 이 작업을 수행하려면 AWS Resource Groups 콘솔의 태그 편집기를 사용하거나 AWS Resource Groups API 태그 지정의 태그 지정 작업을 사용합니다.

> **Important**
>
> 리소스의 태그를 편집하면 리소스 액세스에 영향을 줄 수 있습니다. 리소스의 태그 키 또는 값을 편집하기 전에 해당 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 모든 AWS Identity and Access Management(IAM)정책을 검토하세요.

Console

Amazon Macie 콘솔을 사용하여 리소스의 태그를 편집하려면 다음 단계를 따르세요.

리소스에 대한 태그를 편집하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 태그를 편집할 리소스의 유형에 따라 다음 중 하나를 수행합니다.
   - 허용 목록을 보려면 탐색 창에서 허용 목록을 선택합니다.

     그런 다음, 테이블에서 목록의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
   - 사용자 지정 데이터 식별자의 경우, 탐색 창에서 사용자 지정 데이터 식별자를 선택합니다.

     그런 다음, 테이블에서 사용자 지정 데이터 식별자의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
   - 필터 또는 억제 규칙의 경우, 탐색 창에서 조사 결과를 선택합니다.

     그런 다음, 저장된 규칙 목록에서 규칙 옆에 있는 편집 아이콘 () 을 선택합니다. 태그 관리를 선택합니다.
   - 조직의 멤버 계정인 경우, 탐색 창에서 계정을 선택합니다.

     그런 다음, 테이블에서 계정의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
   - 민감한 데이터 검색 작업의 경우, 탐색 창에서 작업을 선택합니다.

     그런 다음, 테이블에서 작업의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.

   태그 관리 창에는 현재 리소스에 할당된 모든 태그가 나열됩니다.
3. 태그 관리 창에서 태그 편집을 선택합니다.
4. 다음을 수행하세요.
   - 태그 키에 태그 값을 추가하려면 태그 키 옆의 값 상자에 값을 입력합니다.

- 기존 태그 키를 변경하려면 태그 옆에 있는 제거를 선택합니다. 그런 다음, 태그 추가를 선택합니다. 나타나는 키 상자에 새로운 태그 키를 입력합니다. 값 상자에 연결된 태그 값을 입력합니다(선택 사항).
- 기존 태그 값을 변경하려면 값이 포함된 값 상자에서 X를 선택합니다. 그런 다음, 값 상자에 새 태그 값을 입력합니다.
- 기존 태그 값을 제거하려면 값이 포함된 값 상자에서 X를 선택합니다.
- 기존 태그(태그 키 및 태그 값 모두)를 제거하려면 태그 옆의 제거를 선택합니다.

리소스는 최대 50개의 태그를 가질 수 있습니다. 태그 키에는 최대 128자를 사용할 수 있습니다. 태그 값에는 최대 256자를 사용할 수 있습니다. 문자는 문자, 숫자, 공백 또는 _ . : / = + - @ 기호일 수 있습니다.

5. 태그 편집을 완료하면 저장을 선택합니다.

API

프로그래밍 방식으로 리소스의 태그를 편집하면 기존 태그를 새 값으로 덮어쓰게 됩니다. 따라서 태그를 편집하는 가장 좋은 방법은 태그 키를 편집할지, 태그 값을 편집할지 또는 둘 다를 편집할지에 따라 다릅니다. 태그 키를 편집하려면 현재 태그를 제거하고 새 태그를 추가합니다.

태그 키와 연결된 태그 값만 편집하거나 제거하려면 Amazon Macie API의 TagResource 작업을 사용하거나 AWS Command Line Interface(AWS CLI)를 사용하는 경우, tag-resource 명령을 실행하여 기존 값을 덮어씁니다. 요청에서 태그 값을 편집 또는 제거하려는 리소스의 Amazon 리소스 이름(ARN)을 지정합니다.

태그 키의 태그 값을 편집하려면 `tags` 파라미터를 사용하여 태그 값을 변경하려는 태그 키를 지정하고 키에 새 태그 값을 지정합니다. 예를 들어, 다음 명령은 지정된 민감한 데이터 검색 작업과 연결된 `Stack` 태크 키의 태그 값을 `Production`에서 `Staging`으로 바꿉니다. 이 예제는 Microsoft Windows용으로 포맷되었으며 가독성을 높이기 위해 캐럿(^) 줄 연속 문자를 사용합니다.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Staging\"}
```

위치:

- `resource-arn`은(는) 작업의 ARN을 지정합니다.

- *Stack*은(는) 변경할 태그 값과 연결된 태그 키입니다.
- *Staging*은(는) 지정된 태그 키*Stack*()에 사용할 새 태그 값입니다.

태그 키에서 태그 값을 제거하려면 `tags` 파라미터에 `value` 인수 값을 지정하지 마세요. 예:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"\"}
```

작업이 성공하면 Macie는 빈 HTTP 204 응답을 반환합니다. 그렇지 않으면 Macie는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

Amazon Macie 리소스에서 태그 제거

Amazon Macie 리소스에서 태그를 제거하려면 Amazon Macie 콘솔 또는 Amazon Macie API를 사용할 수 있습니다. 여러 Macie 리소스에서 동시에 이 작업을 수행하려면 AWS Resource Groups 콘솔의 태그 편집기를 사용하거나 AWS Resource Groups API 태그 지정의 태그 지정 작업을 사용합니다.

> **Important**
>
> 리소스에서 태그를 제거하면 리소스에 대한 액세스에 영향을 줄 수 있습니다. 태그를 제거하기 전에 해당 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 모든 AWS Identity and Access Management(IAM)정책을 검토하세요.

Console

Amazon Macie를 사용하여 리소스에서 하나 이상의 태그를 삭제하려면 다음 단계를 따르세요.

리소스에서 태그를 제거합니다.

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 태그를 제거하고 싶은 리소스 유형에 따라 다음 중 하나를 수행합니다.

   - 허용 목록을 보려면 탐색 창에서 허용 목록을 선택합니다.

     그런 다음, 테이블에서 목록의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.

- 사용자 지정 데이터 식별자의 경우, 탐색 창에서 사용자 지정 데이터 식별자를 선택합니다.

  그런 다음, 테이블에서 사용자 지정 데이터 식별자의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
- 필터 또는 억제 규칙의 경우, 탐색 창에서 조사 결과를 선택합니다.

  그런 다음, 저장된 규칙 목록에서 규칙 옆에 있는 편집 아이콘 ()을 선택합니다. 태그 관리를 선택합니다.
- 조직의 멤버 계정인 경우, 탐색 창에서 계정을 선택합니다.

  그런 다음, 테이블에서 계정의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.
- 민감한 데이터 검색 작업의 경우, 탐색 창에서 작업을 선택합니다.

  그런 다음, 테이블에서 작업의 확인란을 선택합니다. 작업 메뉴에서 태그 관리를 선택합니다.

  태그 관리 창에는 현재 리소스에 할당된 모든 태그가 나열됩니다.
3. 태그 관리 창에서 태그 편집을 선택합니다.
4. 다음을 수행하세요.
   - 태그의 태그 값만 제거하려면 제거할 값이 포함된 값 상자에서 X를 선택합니다.
   - 태그의 태그 키와 태그 값(한 쌍)을 모두 제거하려면 제거할 태그 옆의 제거를 선택합니다.
5. (선택 사항) 리소스에서 더 많은 태그를 제거하려면 제거할 각 추가 태그에 대해 이전 단계를 반복합니다.
6. 태그 제거를 마치면 저장을 선택합니다.

API

리소스에서 하나 이상의 태그를 프로그래밍 방식으로 삭제하려면 Amazon Macie API의 UntagResource 작업을 사용합니다. 요청에서 `resourceArn` 파라미터를 사용하여 태그를 제거할 리소스의 Amazon 리소스 이름(ARN)을 지정합니다. `tagKeys` 파라미터를 사용하여 제거할 태그의 태그 키를 지정합니다. 리소스에서 특정 태그 값(태그 키 아님)만 제거하려면 태그를 제거하는 대신 태그를 편집합니다.

AWS Command Line Interface(AWS CLI)를 사용하는 경우, untag-resource 명령을 실행하고 `resource-arn` 파라미터를 사용하여 태그를 제거할 리소스의 ARN을 지정합니다. `tag-keys` 파라미터를 사용하여 제거할 태그의 태그 키를 지정합니다. 예를 들어 다음 명령은 지정된 민감한 데이터 검색 작업에서 `Stack` 태그(태그 키와 태그 값 모두)를 제거합니다.

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack
```

여기서 `resource-arn`은(는) 태그를 제거할 작업의 ARN을 지정하고, *`Stack`*은(는) 제거할 태그의 태그 키입니다.

리소스에서 여러 태그를 제거하려면, 각 추가 키를 `tag-keys` 파라미터의 인수로 추가합니다. 예:

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack Owner
```

여기서 `resource-arn`은(는) 태그를 제거할 작업의 ARN을 지정하고, *`Stack`* 및 *`Owner`*은(는) 제거할 태그의 태그 키입니다.

작업이 성공하면 Macie는 빈 HTTP 204 응답을 반환합니다. 그렇지 않으면 Macie는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

AWS CloudFormation를 사용하여 Amazon Macie 리소스 생성

Amazon Macie는 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있도록 AWS 리소스를 모델링하고 설정하는 데 도움이 되는 서비스인 AWS CloudFormation과 통합됩니다. 사용자 지정 데이터 식별자와 같이 필요한 모든 AWS 리소스를 설명하는 템플릿을 생성하면 AWS CloudFormation에서 이러한 리소스를 프로비저닝하고 구성합니다.

AWS CloudFormation을 사용할 때 템플릿을 재사용하여 Macie 리소스를 일관되고 반복적으로 설정할 수 있습니다. 리소스를 한 번 설명한 후 여러 AWS 계정 및 AWS 리전에서 동일한 리소스를 반복적으로 프로비저닝할 수 있습니다.

주제

Amazon Macie 및 AWS CloudFormation 템플릿

Amazon Macie 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML 형식의 텍스트 파일입니다. 이 템플릿은 AWS CloudFormation 스택에서 프로비저닝할 리소스에 대해 설명합니다.

JSON 또는 YAML에 익숙하지 않은 경우 AWS CloudFormation 템플릿을 생성하고 수정하기 위한 그래픽 도구인 AWS CloudFormation Designer를 사용할 수 있습니다. Designer를 사용하면 끌어 놓기 인터페이스를 사용해 템플릿 리소스 다이어그램을 생성한 다음 통합 JSON 및 YAML 편집기를 사용하여 세부 정보를 편집할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇입니까?를 참조하세요.

다음 유형의 Macie 리소스에 대한 AWS CloudFormation 템플릿을 생성할 수 있습니다:

- 허용 목록
- 사용자 지정 데이터 식별자
- 결과 필터라고도 하는 검색 결과에 대한 필터 규칙 및 억제 규칙

이러한 리소스에 대한 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서에서 Amazon Macie 리소스 유형 참조를 참조하세요.

AWS CloudFormation에 대해 자세히 알아보기

AWS CloudFormation에 대한 자세한 내용은 다음 리소스를 참조하세요.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation API 참조
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

Amazon Macie 일시 중지 또는 비활성화

Amazon Macie 콘솔 또는 Amazon Macie API를 사용하여AWS 리전 특정 영역에서 Amazon Macie를 일시 중지하거나 비활성화할 수 있습니다. 그러면 Macie는 해당 리전에서 사용자 계정에 대한 모든 활동의 수행을 중지합니다. Macie가 일시 중지되거나 비활성화된 동안에는 해당 리전에서 Macie를 사용해도 요금이 부과되지 않습니다.

Macie를 일시 중지하거나 비활성화한 경우 나중에 다시 활성화할 수 있습니다.

주제

Amazon Macie 일시 중지

Amazon Macie를 일시 중단하면, Macie는 적용 가능한 AWS 리전에서 사용자 계정에 대한 세션 식별자, 설정 및 리소스를 유지합니다. 예를 들어, 기존 조사 결과는 그대로 유지되며 최대 90일 동안 유지됩니다. 그러나 Macie를 을 일시 중지하면, 그것은 적용가능한 리전에서 사용자 계정에 대한 모든 활동의 수행을 중지합니다. 여기에는 Amazon Simple Storage Service(S3) 모니터링, 민감한 데이터 자동 검색, 그리고 현재 진행 중인 모든 민감한 데이터 검색 작업의 실행이 포함됩니다. 또한 Macie는 해당 리전의 모든 민감한 데이터 검색 작업을 취소합니다.

Macie를 일시 중지한 후, 다시 활성화할 수 있습니다. 그러면 적용가능한 리전에서 설정 및 리소스에 액세스 권한을 다시 획득하고 해당 리전에서 사용자 계정에 대한 모든 활동을 재개합니다. 여기에는 계정에 대한 S3 버킷 인벤토리 업데이트와 보안 및 액세스 제어를 위한 버킷의 모니터링이 포함됩니다. 여기에는 민감한 데이터 검색 작업의 재개 또는 재시작이 포함되지 않습니다. 민감한 데이터 검색 작업은 취소한 후에는 재개하거나 다시 시작할 수 없습니다.

이 주제에서는 Amazon Macie 콘솔을 사용하여 Macie를 일시 중단하는 방법을 설명합니다. 이것을 프로그래밍 방식으로 수행하려면, Amazon Macie API의 UpdateMacieSession 작업을 사용할 수 있습니다.

> **Note**
>
> 사용자가 조직의 Macie 관리자인 경우, 사용자 계정에 대한 Macie를 일시 중지하기 전에 모든 구성원 계정을 제거해야 합니다. 자세한 내용은 여러 계정 관리 섹션을 참조하세요.

Macie를 일시 중지하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여, Macie를 일시 주지하고하 하는 리전을 선택합니다.
3. 탐색 창에서 설정을 선택합니다.
4. Macie 일시 중지를 선택합니다.
5. 확인 메시지가 나타나면, **Suspend**을 입력한 다음 일시중지를 선택합니다.

추가적인 리전에서 Macie를 일시 중지하려면 각각의 추가적인 리전에서 앞의 단계를 반복합니다.

Amazon Macie 비활성화

Amazon Macie를 비활성화할 때, 적용 가능한 AWS 리전에서 Macie는 해당 계정에 대한 모든 활동의 수행을 중지합니다. 여기에는 Amazon Simple Storage Service(S3) 모니터링, 민감한 데이터 자동 검색, 그리고 현재 진행 중인 모든 민감한 데이터 검색 작업의 실행이 포함됩니다. 또한 Macie는 조사 결과 및 민감한 데이터 검색 작업을 포함하여 해당 리전의 사용자 계정에 대해 저장하거나 유지 관리하는 기존 설정 및 리소스를 모두 삭제합니다. 저장하거나 다른 사람에게 게시한 데이터는 그대로 AWS 서비스 유지되며 영향을 받지 않습니다. 예를 들어 Amazon S3에서의 민감한 데이터 검색 결과 및 Amazon EventBridge에서의 이벤트 조사 결과가 이에 해당합니다.

> **Warning**
>
> Macie를 비활성화하면, Macie가 해당 리전의 사용자 계정에 대해 저장하거나 유지 관리하는 기존 검색 결과, 민감한 데이터 검색 작업, 사용자 지정 데이터 식별자 및 기타 리소스도 모두 영구적으로 삭제됩니다. 이러한 리소스는 삭제된 후에는 복구할 수 없습니다. 리소스를 유지하고 Macie의 사용만 일시 중지하려면 Macie를 비활성화하는 대신 일시 중지하세요.

이 주제에서는 Amazon Macie 콘솔을 사용하여 Macie를 비활성화하는 방법을 설명합니다. 이것을 프로그래밍 방식으로 수행을 선호하면, Amazon Macie API의 DisableMacie 작업을 사용할 수 있습니다.

> **Note**
>
> 계정이 여러 Macie 계정을 중앙에서 관리하는 조직의 일부인 경우, Macie를 비활성하기 전에 사용자는 다음을 해야 합니다.

- 사용자 계정이 Macie 회원 계정인 경우, Macie 관리자와 협력하여 회원 계정에서 사용자의 계정을 제거하세요.
- 사용자 계정이 Macie 관리자 계정인 경우, 계정과 연결된 모든 회원 계정을 제거하고 사용자 계정과 해당 계정 간의 연결을 삭제하세요.

이전 작업을 완료하는 방법은 Macie 계정이 초대를 통해 다른 계정과 연결되었는지 AWS Organizations를 통해 또는 초대를 의해 연결되었는지에 따라 달라집니다. 자세한 내용은 여러 계정 관리 섹션을 참조하세요.

Macie 비활성화하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여, Macie를 비활성하고하 하는 리전을 선택합니다.
3. 탐색 창에서 설정을 선택합니다.
4. Macie 비활성화를 선택합니다.
5. 확인 메시지가 나타나면, **`Disable`**을 입력한 다음 비활성화를 선택합니다.

추가 리전에서 Macie를 비활성화하려면, 각 추가 리전에서 이전 단계를 반복합니다.

Amazon Macie 할당량

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량(이전에는 제한이라고 함)이 있습니다. 이러한 할당량은 한도라 함은 계정의 최대 서비스 리소스 또는 작업 수입니다. 이 주제에서는 사용자의 계정에 대한 Amazon Macie 리소스 및 작업에 적용되는 할당량을 나열합니다. 다르게 표시되지 않는 한, AWS 리전의 계정에 각 할당량이 적용됩니다.

일부 할당량만 늘릴 수 있습니다. 할당량 증가를 요청하려면 Service Quotas 콘솔을 사용합니다. 할당량 증가을 요청에 관한 정보는 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요. Service Quotas 콘솔에서 할당량을 사용할 수 없는 경우, AWS Support Center Console에서 서비스 한도 증가 양식을 사용하여 할당량 증가를 요청하세요.

계정

- 초대장을 이용한 멤버 계정: 1,000개
- AWS Organizations을 통한 멤버 계정: 10,000개

결과

- 계정당 필터 규칙 및 억제 규칙: 1,000개
- 민감한 데이터 검색 작업의 실행당 결과: 100,000개 + 100,000개 임계값 충족 이후 남은 조사 결과의 5% 이상

  이 할당량은 Amazon Macie 콘솔과 Amazon Macie API에만 적용됩니다. Macie가 Amazon EventBridge에 게시하는 검색 이벤트 수 또는 Macie가 각 작업 실행에 대해 생성하는 민감한 데이터 검색 결과의 수에는 할당량이 없습니다.
- 민감한 데이터 조사 결과당 탐지 위치: 15개
- Amazon S3 객체에서 민감한 데이터 샘플 검색 및 공개 요청: 하루에 100건

  이 할당량은 24시간마다 00:00:01 UTC+0에 재설정됩니다.
- 다음으로부터 민감한 데이터 샘플 검색 및 공개하기 위한 Amazon S3 객체의 크기:
  - Apache Avro 객체 컨테이너(.avro) 파일: 70MB
  - Apache Parquet(.parquet) 파일: 100MB
  - CSV(.csv) 파일: 255MB
  - GNU Zip 압축 아카이브(.gz 또는 .gzip)파일: 90MB
  - JSON 또는 JSON 라인(.json 또는 .jsonl)파일: 25MB

- Microsoft Excel 통합문서(.xlsx) 파일: 20MB
- 바이너리가 아닌 텍스트(text/plain)파일: 100MB
- TSV(.tsv)파일: 75MB
- ZIP 압축 아카이브(.zip) 파일: 355MB

해당하는 민감한 데이터 조사 결과로 여러 .gz 파일을 생성하는 아카이브 파일에 조사 결과가 적용되는 경우 아카이브 파일에서 민감한 데이터 샘플을 검색하고 공개할 수 없습니다.

민감한 데이터 검색

- 민감한 데이터 검색 작업별 계정당 월별 분석: 5TB

  이 할당량은 민감한 데이터 검색 작업에만 적용됩니다. 할당량을 1,000TB(1PB)까지 늘리려면 Service Quotas 콘솔을 사용하세요. 1PB 이상 증가를 요청하려면 의AWS Support Center Console 서비스 한도 증가 양식을 사용합니다.
- 계정당 사용자 지정 데이터 식별자: 10,000개
- 계정당 허용 목록: 10개, 사전 정의된 텍스트를 지정하는 허용 목록 1~5개, 정규식을 지정하는 허용 목록 1~5개

  사전 정의된 텍스트를 지정하는 허용 목록에 추가 할당량이 적용됩니다. 목록에는 100,000개 이상의 항목이 포함될 수 없으며 목록의 스토리지 크기는 35MB를 초과할 수 없습니다.
- 민감한 데이터 자동 검색에서 제외할 S3 버킷: 1,000개

  계정이 조직의 Macie 관리자 계정인 경우, 이 할당량은 조직 전체에 적용됩니다.
- 민감한 데이터 검색 작업당 S3 버킷: 1,000개

  런타임 버킷 기준을 사용하여 분석할 버킷을 결정하는 작업에는 이 할당량이 적용되지 않습니다. 선택한 특정 버킷을 분석하도록 작업을 구성한 경우에만 작업에 적용됩니다. 계정이 조직의 Macie 관리자 계정인 경우 조직에서 최대 1,000개 계정에 걸쳐 1,000개의 버킷을 선택할 수 있습니다.
- 민감한 데이터 검색 작업당 사용자 지정 데이터 식별자: 30개
- 민감한 데이터 검색 작업당 허용 목록: 10개, 사전 정의된 텍스트를 지정하는 허용 목록 1~5개, 정규식을 지정하는 허용 목록 1~5개
- CreateClassificationJob 작업: 초당 요청 0.1건
- 개별 파일 분석 시간: 10시간
- 분석할 개별 파일의 크기:

  - Adobe Portable Document Format(.pdf) 파일: 1,024MB
  - Apache Avro 객체 컨테이너(.avro)파일: 8GB
  - Apache Parquet(.parquet)파일: 8GB
  - 이메일 메시지(.eml)파일: 20GB
  - GNU Zip 압축 아카이브(.gz 또는 .gzip) 파일: 8GB
  - Microsoft Excel 통합문서(.xls 또는 .xlsx) 파일: 512MB
  - Microsoft Word 문서(.doc 또는 .docx) 파일: 512MB
  - 바이너리가 아닌 텍스트 파일: 20GB
  - TAR 아카이브(.tar) 파일: 20GB
  - ZIP 압축 아카이브(.zip) 파일: 8GB

  파일이 해당 할당량보다 큰 경우 Macie는 파일의 데이터를 분석하지 않습니다.
- 압축 또는 아카이브 파일의 데이터 추출 및 분석:
  - 스토리지 크기(압축): GNU Zip 압축 아카이브(.gz 또는 .gzip)파일 또는 ZIP 압축 아카이브(.zip)파일의 경우 8GB, TAR 아카이브(.tar) 파일의 경우 20GB
  - 중첩 아카이브 깊이: 10개의 레벨
  - 추출된 파일: 1,000,000개
  - 추출된 바이트: 전체 10GB의 비압축 데이터. 지원되는 파일 유형 또는 스토리지 형식을 사용하는 추출된 각 파일에 대해 3GB의 압축되지 않은 데이터.

  압축 파일 또는 아카이브 파일의 메타데이터에서 파일에 10개 이상의 중첩 레벨이 포함되어 있거나 스토리지 크기 또는 추출된 바이트에 해당하는 할당량을 초과하는 것으로 나타나는 경우, Macie는 파일에 있는 데이터를 추출하거나 분석하지 않습니다. Macie가 압축 파일 또는 아카이브 파일의 데이터를 추출 및 분석하기 시작한 후 파일에 1,000,000개 이상의 파일이 포함되어 있거나 추출된 바이트 할당량을 초과하는 것으로 확인되면 Macie는 파일의 데이터 분석을 중단하고 처리된 데이터에 대해서만 민감한 데이터 조사 결과 및 검사 결과를 생성합니다.
- 구조화된 데이터의 중첩 요소 분석: 파일당 256개의 레벨

  이 할당량은 JSON(.json)및 JSON 라인(.jsonl)파일에만 적용됩니다. 두 파일 유형 중 하나의 중첩 깊이가 이 할당량을 초과하는 경우 Macie는 파일 내 데이터를 분석하지 않습니다.
- 민감한 데이터 검색 결과당 탐지 위치: 민감한 데이터 탐지 유형당 1,000개
- 전체 이름 탐지: 아카이브 파일을 포함하여 파일당 1,000개

Macie가 파일에서 처음 1,000개의 전체 이름 항목을 감지하면 Macie는 전체 이름의 수를 늘리고 위치 데이터를 보고하는 작업을 중단합니다

- 우편 주소 감지: 파일당 1,000개(아카이브 파일 포함)

  Macie가 파일에서 처음 1,000개의 우편 주소 항목을 감지하면 Macie는 우편 주소의 수를 늘리고 위치 데이터를 보고하는 작업을 중단합니다.

Amazon Macie 사용 설명서에 대한 문서 기록

다음 표에서는 Amazon Macie의 최신 릴리스 이후에 이 설명서에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

최신 설명서 업데이트: 2024년 6월 14일

변경 사항	설명	날짜
새 기능	조직의 Macie 위임 관리자인 경우 이제 조직의 개별 계정에 대해 민감한 데이터 자동 검색을 활성화하거나 비활성화할 수 있습니다. 이제 이 추가 옵션을 사용하여 모든 계정에 대한 자동 검색을 활성화하고, 특정 계정에 대한 자동 검색을 선택적으로 활성화하고, 특정 S3 버킷을 제외하는 등 여러 가지 방법으로 분석 범위를 정의할 수 있습니다.	2024년 6월 14일
새로운 기능	AWS Security Hub 이제 Macie의 상태를 확인하는 보안 제어 기능과 계정에 대한 자동화된 민감한 데이터 검색 기능을 제공합니다. 이러한 컨트롤을 사용하도록 설정하면 Security Hub는 정기적으로 보안 검사를 실행하여 Macie가 AWS 계정 (Macie.1 컨트롤) 에 대해 활성화되었는지 여부와 Macie 계정에 민감한 데이터 자동 검색이 활성화되어 있는지 (Macie.2 컨트롤) 확인합니다.	2024년 2월 20일

새로운 기능	Macie는 이제 (DSSE-KMS) 로 이중 계층 서버 측 암호화를 사용하여 암호화된 Amazon S3 객체를 분석할 수 있습니다. AWS KMS keys 이제 Macie가 민감한 데이터 자동 검색을 수행하거나 민감한 데이터 검색 작업을 실행할 때 이러한 객체를 분석할 수 있습니다. 또한 DSSE-KMS 암호화를 사용하는 S3 버킷과 객체는 이제 Macie가 Amazon S3 데이터에 대해 제공하는 통계 및 메타데이터에 포함됩니다.	2024년 1월 17일
새 기능	이제 Macie가 조사 결과를 보고한 민감한 데이터의 샘플을 검색하고 공개하도록 선택할 때 AWS Identity and Access Management (IAM) 역할을 맡도록 Macie를 구성할 수 있습니다. 샘플은 Macie가 발견한 민감한 데이터의 특성을 확인하고 영향을 받는 Amazon S3 객체 및 버킷에 대한 조사를 맞춤 설정하는 데 도움이 될 수 있습니다.	2023년 11월 16일
새로운 기능	Macie는 이제 47개 추가 국가 및 지역의 국제 은행 계좌 번호 (IBAN)를 탐지하도록 설계된 관리형 데이터 식별자를 제공합니다. 이제 Macie를 사용하여 50개가 넘는 국가 및 지역에서 IBAN 발생을 탐지하고 보고할 수 있습니다.	2023년 11월 1일

새로운 기능	Macie는 이제 Google Cloud API 키, Stripe API 키, Aadhaar 번호, PAN(영구 계정 번호), 인도의 운전면허증 식별 번호 등 민감한 데이터 유형을 탐지하도록 설계된 관리형 데이터 식별자를 제공합니다.	2023년 9월 25일
새로운 할당량	조사 결과에 의해 보고된 민감한 데이터의 특성을 확인할 수 있도록 Amazon S3 객체에서 민감한 데이터 샘플을 검색하고 공개하기 위한 크기 할당량을 늘렸습니다. 이제 스토리지 크기가 10MB를 초과하는 S3 객체에서 샘플을 검색하고 확인할 수 있습니다. 새 할당량에 대한 목록은 Amazon Macie 할당량을 참조하세요.	2023년 9월 7일
지역별 가용성	이제 이스라엘(텔아비브) 지역에서 Macie를 사용할 수 있습니다. Macie를 현재 사용할 수 있는 AWS 리전 목록은 AWS 일반 참조의 Amazon Macie 엔드포인트 및 할당량을 참조하세요.	2023년 8월 28일

업데이트된 기능	민감한 데이터 자동 검색을 위해 새롭고 동적인 기본 관리형 데이터 식별자 세트를 구현했습니다. 기본 세트에는 민감한 데이터 자동 검색에 권장되는 관리형 데이터 식별자가 포함됩니다. 이 항목은 민감한 데이터의 일반적인 범주와 유형을 탐지하는 동시에 민감한 데이터 자동 검색 결과를 최적화하도록 설계되었습니다.	2023년 8월 2일
업데이트된 기능	Macie가 민감한 데이터 조사 결과 및 민감한 데이터 검색 결과에서 보고하는 민감한 데이터의 발생 위치를 쉽게 찾을 수 있도록 `Record` 객체의 JSON 경로 요소 이름에 대한 문자 제한을 20자에서 240자로 변경했습니다. 이 변경은 Apache Avro 객체 컨테이너, Apache Parquet 파일, JSON 파일 및 JSON 라인 파일에 대한 새로운 민감한 데이터 조사 결과 및 검색 결과에 영향을 줍니다.	2023년 7월 24일
업데이트된 기능	에 있는 조직의 위임 Macie 관리자인 경우 이제 조직 내 최대 AWS Organizations 10,000개의 계정에 대해 Macie를 관리할 수 있습니다.	2023년 6월 30일

새로운 특성	이제 민감한 데이터 검색 작업의 결과를 생성 및 구성하여 작업에 권장되는 관리형 데이터 식별자 세트를 자동으로 사용하도록 개별 작업을 구성할 수 있습니다. 이러한 권장되는 관리형 데이터 식별자 세트는 작업 결과를 최적화하면서도 민감한 데이터의 일반적인 범주 및 유형을 탐지하도록 설계되었습니다.	2023년 6월 28일
새 정책	새 AWS 관리형 정책인 `AmazonMacieReadOnlyAccess` 정책을 추가했습니다. 이 정책은 IAM ID(보안 주체)가 자신의 계정에 대한 모든 Macie 리소스, 데이터 및 설정을 검색할 수 있도록 하는 읽기 전용 권한을 부여합니다.	2023년 6월 15일
새 기능	Amazon S3 데이터의 민감한 데이터 자동 검색 범위를 평가하고 모니터링할 수 있도록 이제 Macie 콘솔에 리소스 범위 페이지가 포함됩니다. 이 페이지를 통해 각 버킷에서 최근에 발생한 분석 문제의 롤업(해당하는 경우)을 포함하여 모든 S3 버킷의 범위 통계 및 데이터를 통합적으로 볼 수 있습니다. 문제가 발생한 경우 이 페이지에서는 수정 지침도 제공합니다.	2023년 5월 15일

새 기능	Macie는 알림의 중앙 위치 역할을 AWS 서비스 하는 새로운 기능인 과 AWS 사용자 알림통합됩니다. AWS AWS Management Console를 사용하면 Macie가 정책 및 민감한 데이터 조사 결과를 위해 게시하는 Amazon EventBridge 이벤트에 대한 알림을 생성하고 전송하기 위한 사용자 지정 규칙 및 전송 채널을 구성할 수 있습니다. 사용자 알림	2023년 5월 5일
업데이트 내용	Macie가 S3 버킷의 기본 암호화 설정에 대해 제공하는 통계 및 메타데이터에 대한 설명이 업데이트되었습니다. Policy:IAMUser/S3BucketEncryptionDisabled 정책 조사 결과에 대한 설명도 업데이트되었습니다. 이제 Amazon S3가 Amazon S3 관리형 키를 사용한 서버 측 암호화(SSE-S3)를 신규 및 기존 버킷에 추가되는 객체의 암호화의 기본 수준으로 자동 적용합니다. Amazon S3의 이러한 변경 사항에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 S3 버킷에 대한 기본 서버 측 암호화 동작 설정을 참조하세요.	2023년 2월 27일

새로운 기능	이제 Macie는 S3 버킷: `Policy:IAMUser/S3BucketSharedWithCloudFront` 에 대한 추가 유형의 정책 조사 결과를 생성할 수 있습니다. 이러한 유형의 검색은 Amazon CloudFront 원본 액세스 ID (OAI), CloudFront 원본 액세스 제어 (OAC) 또는 둘 다와 버킷을 공유할 수 있도록 버킷 정책이 변경되었음을 나타냅니다. 또한 CloudFront OAI 또는 OAC와 공유되는 버킷은 이제 Macie가 Amazon S3 데이터에 대해 제공하는 통계 및 메타데이터에서 외부적으로 공유된 것으로 간주됩니다.	2023년 2월 24일
새로운 기능	Macie는 이제 민감한 데이터 검색을 위한 Amazon S3 Glacier Instant Retrieval 스토리지 클래스를 지원합니다. 이제 Macie가 민감한 데이터 자동 검색을 수행하거나 민감한 데이터 검색 작업을 실행할 때 이 스토리지 클래스를 사용하는 S3 객체를 분석할 수 있습니다. 또한 해당 내용은 Macie가 Amazon S3 데이터에 대해 제공하는 통계 및 메타데이터에서도 분류 가능한 객체로 간주됩니다.	2022년 12월 21일

새 기능	이제 계정 또는 조직에 대해 민감한 데이터 자동 검색을 수행하도록 Macie를 구성할 수 있습니다. Macie는 민감한 데이터 자동 검색을 통해 Amazon S3 데이터를 지속적으로 평가하고, 샘플링 기법을 사용하여 S3 버킷의 대표적인 S3 객체를 식별, 선택, 분석하며 민감한 데이터에 대한 객체를 조사합니다. Macie가 Amazon S3 데이터에 대해 제공하는 통계, 조사 결과 및 기타 정보로 분석 결과를 평가할 수 있습니다.	2022년 11월 28일
새 기능	이제 허용 목록을 만들고 사용하여 Macie가 Amazon S3 객체에서 민감한 데이터를 검사할 때 무시하도록 하려는 텍스트 및 텍스트 패턴을 지정할 수 있습니다. 허용 목록을 사용하면 특정 시나리오나 환경에 대한 민감한 데이터 예외사항을 정의할 수 있습니다. 예를 들어, 조직의 공공 담당자 이름, 특정 전화번호 또는 조직에서 테스트에 사용하는 샘플 데이터 등이 이에 해당합니다.	2022년 8월 30일
새 기능	Macie가 S3 객체에서 찾은 민감한 데이터의 특성을 확인하기 위해, 이제 Macie를 구성하고 사용하여 조사 결과에 의해 보고된 민감한 데이터의 샘플을 검색할 수 있습니다.	2022년 7월 26일

업데이트된 기능	AmazonMacieFullAccess 정책에서 Macie 서비스 연결 역할(`aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`)의 Amazon 리소스 이름(ARN)을 업데이트했습니다.	2022년 6월 30일
업데이트된 기능	Macie 서비스 연결 역할(`AWSServiceRoleForAmazonMacie`)에 연결된 정책인 AmazonMacieServiceRolePolicy 정책을 업데이트했습니다. 이 정책에서는 더 이상 Amazon Macie Classic에 대한 작업 및 리소스를 지정하지 않습니다. Amazon Macie Classic은 단종되어 더 이상 사용할 수 없습니다.	2022년 5월 20일
새로운 기능	이제 Macie는 해당 `OriginType` 필드를 게시하는 민감한 데이터 결과에 포함시킵니다. AWS Security Hub 이 `OriginType` 필드는 Macie가 조사 결과를 생성한 민감한 데이터를 발견한 방법을 지정합니다.	2022년 5월 11일
업데이트 내용	사용자 정의 데이터 식별자에 대한 키워드 및 최대 일치 거리 설정이 작동하는 방식을 명확히 했습니다.	2022년 4월 22일

새로운 기능	Macie는 이제 HTTP 기본 인증 헤더, HTTP 쿠키 및 JSON 웹 토큰을 탐지하도록 설계된 관리형 데이터 식별자를 제공합니다.	2022년 4월 21일
새 콘텐츠	Macie의 주요 개념 및 용어에 대한 설명과 정의가 추가되었습니다.	2022년 3월 16일
새로운 기능	이제 Macie는 민감한 데이터 검색 작업을 생성하고 구성할 때 예상 비용을 계산하고 표시하기 위해 양식의 가격 데이터를 검색합니다. AWS 계정 AWS Billing and Cost Management이 기능을 지원하기 위해 AmazonMacieFullAccess 정책에 Billing and Cost Management 작업을 추가했습니다.	2022년 3월 7일
새로운 기능	이제 Macie는 해당 `Sample` 필드를 게시할 조사 결과에 포함시킵니다. AWS Security Hub이 `Sample` 필드는 조사 결과가 샘플 조사 결과인지 여부를 지정합니다.	2022년 2월 24일
새 콘텐츠	Amazon Virtual Private Cloud를 사용하여 VPC 및 Macie 사이의 프라이빗 연결을 구축하는 방법에 대한 정보가 추가되었습니다.	2022년 1월 19일

새로운 기능	이제 Amazon Macie 콘솔을 사용하여 사용자 정의 데이터 식별자, 조사 결과에 대한 필터 및 금지 규칙, 민감한 데이터 검색 작업, 그리고 조직의 Macie 관리자인 경우 조직의 멤버 계정에 대해 태그를 할당하고 관리할 수 있습니다. 태그는 선택적으로 정의하고 특정 유형의 AWS 리소스에 할당하는 레이블입니다.	2022년 1월 12일
새 콘텐츠	Macie에 대한 액세스를 관리하기 위한 AWS Identity and Access Management사용에 대한 정보가 추가되었습니다.	2021년 12월 20일
새 기능	이제 사용자 정의 데이터 식별자를 만들 때 해당 식별자가 생성하는 민감한 데이터 조사 결과에 대한 심각도 설정을 정의할 수 있습니다. 이러한 설정을 사용하면 사용자 정의 데이터 식별자의 탐지 기준과 일치하는 텍스트 발생 횟수를 기반으로 조사 결과에 할당할 심각도를 지정할 수 있습니다.	2021년 11월 4일
새로운 기능	Amazon Macie가 생성할 수 있는 다양한 유형의 조사 결과에 대해 알아보려면, 샘플 조사 결과를 생성할 수 있습니다. 샘플 조사 결과는 예제 데이터와 자리 표시자 값을 사용하여 Macie가 각 조사 결과 유형에 포함할 수 있는 정보의 종류를 보여줍니다.	2021년 10월 28일

새로운 기능	Macie는 이제 출판하는 연구 결과에 해당 `OwnerAccountId` 분야를 포함시킵니다. AWS Security Hub이 필드는 영향을 받는 S3 버킷을 AWS 계정 소유한 사용자의 계정 ID를 지정합니다.	2021년 10월 27일
새 콘텐츠	여러 Macie 계정을 중앙에서 관리하는 방법에 대한 정보가 추가되었습니다. Macie를 Macie와 AWS Organizations 통합하거나 Macie로부터 멤버십 초대를 보내는 등 두 가지 방법으로 이 작업을 수행할 수 있습니다.	2021년 10월 13일
새로운 기능	이제 S3 버킷 인벤토리에는 버킷의 권한 설정으로 인해 Macie가 버킷 또는 버킷 객체에 대한 정보를 검색하고 버킷 데이터의 보안 및 개인 정보 보호를 평가 및 모니터링하지 못하는지가 표시됩니다. 또한 최신 용어를 반영하여 참조 AWS KMS keys 및 고객 관리 키를 업데이트했습니다.	2021년 10월 5일

새로운 기능	Macie는 이제 정책 및 민감한 데이터 조사 결과를 30일이 아닌 90일 동안 저장합니다. Macie가 2021년 8월 31일 또는 그 이후에 조사 결과를 만들거나 업데이트한 경우 Macie 콘솔 또는 Macie API를 사용하여 최대 90일 동안 조사 결과에 액세스할 수 있습니다. 확실히 AWS 리전 Macie는 2021년 9월 27일부터 90일 동안 연구 결과를 보관하기 시작했습니다.	2021년 10월 1일
새 기능	민감한 데이터 검색 작업을 만들 때, S3 객체를 분석할 때 어떤 관리형 데이터 식별자를 작업에서 사용할 것인지를 지정할 수 있습니다. 이 기능을 사용하면 특정 유형의 민감한 데이터에 초점을 맞추도록 작업 분석을 조정할 수 있습니다.	2021년 9월 17일
새로운 기능	이제 민감한 데이터 조사 결과는 JSON 및 JSON 라인 파일에서 민감한 데이터의 위치를 찾는 데 도움이 되는 추가 정보를 제공합니다.	2021년 7월 6일

업데이트된 기능	Macie는 이제 게시하는 조사 결과에 `AwsS3Bucket` 리소스 유형을 사용합니다. AWS Security Hub(Macie는 이전에 이 값을 로 설정했습니다.) `AWS::S3::Bucket` `AwsS3Bucket` ASFF (AWS 보안 검색 결과 형식) 에서 S3 버킷에 사용되는 리소스 유형 값입니다.	2021년 6월 28일
새 기능	민감한 데이터 검색 작업을 생성할 때 이제 작업에서 분석하는 S3 버킷을 결정하는 런타임 기준을 정의할 수 있습니다. 이 기능을 사용하면 작업 분석 범위가 버킷 인벤토리 변경에 따라 동적으로 조정될 수 있습니다.	2021년 5월 15일
새로운 기능	이제 S3 버킷 인벤토리와 요약 대시보드는 버킷 정책에 새 객체의 서버 측 암호화가 필요한지를 나타내는 암호화 메타데이터 및 통계를 제공합니다. 또한 이제 버킷 인벤토리의 개별 버킷에 대한 객체 메타데이터의 온디맨드 새로 고침을 수행할 수 있습니다.	2021년 4월 30일

새 기능	이제 Amazon CloudWatch Logs를 사용하여 민감한 데이터 검색 작업을 실행할 때 발생하는 이벤트를 모니터링하고 분석할 수 있습니다. 이 기능을 지원하기 위해 Macie 서비스 연결 역할의 AWS 관리형 정책에 CloudWatch 로그 작업을 추가했습니다.	2021년 4월 14일
지역별 가용성	이제 Macie를 AWS 아시아 태평양 (오사카) 지역에서 사용할 수 있습니다.	2021년 4월 5일
새 기능	이제 사용자는 AWS Security Hub에 민감한 데이터 조사 결과를 게시하도록 Macie를 구성할 수 있습니다.	2021년 3월 22일
새 콘텐츠	Macie 비용 모니터링 및 예측과 무료 평가판 참여에 대한 정보가 추가되었습니다.	2021년 2월 26일
업데이트 내용	마스터 계정이라는 용어를 관리자 계정이라는 용어로 대체했습니다. 관리자 계정은 여러 계정을 중앙에서 관리하는 데 사용됩니다.	2021년 2월 12일
새로운 기능	이제 사용자 정의 포함 및 제외 기준에서 S3 객체 접두사를 사용하여 민감한 데이터 검색 작업의 범위를 좁힐 수 있습니다.	2021년 2월 2일

업데이트 내용	Macie는 이제 정책 결과를 발표할 때 AWS 보안 조사 결과 형식 (ASFF) 의 검색 유형 분류법을 고수하고 있습니다. AWS Security Hub	2021년 1월 28일
새 콘텐츠	Amazon S3 데이터 모니터링 및 해당 데이터의 보안 및 개인 정보 보호 평가에 대한 정보가 추가되었습니다.	2021년 1월 8일
지역별 가용성	Macie는 이제 AWS 아프리카 (케이프타운) 지역, AWS 유럽 (밀라노) 지역 및 중동 (바레인) 지역에서 사용할 수 있습니다. AWS	2020년 12월 21일
새로운 기능	사용자의 계정이 Macie 관리자 계정인 경우, 이제 조직 내 1,000개 계정에 걸쳐 있는 최대 1,000개의 버킷에 대한 데이터를 분석하는 민감한 데이터 검색 작업을 만들고 실행할 수 있습니다.	2020년 11월 25일
새로운 기능	이제 S3 버킷 인벤토리에 버킷의 데이터를 분석하기 위한 일회성 또는 주기적 민감한 데이터 검색 작업을 구성했는지가 표시됩니다. 구성한 경우, 가장 최근에 실행된 작업에 대한 세부 정보도 제공됩니다.	2020년 11월 23일
새 콘텐츠	조사 결과 필터링에 대한 정보가 추가되었습니다.	2020년 11월 12일

새로운 기능	이제 민감한 데이터 조사 결과는 Apache Avro 객체 컨테이너, Apache Parquet 파일 및 Microsoft Excel 통합 문서에서 민감한 데이터의 위치를 찾는 데 도움이 되는 추가 정보를 제공합니다.	2020년 11월 9일
새 기능	이제 민감한 데이터 조사 결과를 사용하여 S3 객체에서 발생한 민감한 데이터의 위치를 개별적으로 찾을 수 있습니다.	2020년 10월 22일
새 기능	이제 민감한 데이터 검색 작업을 일시 중지했다가 재개할 수 있습니다.	2020년 10월 16일
새 콘텐츠	정책 조사 결과 및 민감한 데이터 조사 결과에 대한 심각도 점수 산정 시스템에 대한 세부 정보가 추가되었습니다.	2020년 10월 6일
새로운 기능	이제 민감한 데이터 검색 작업을 실행할 때 Macie가 개별 S3 버킷에서 분석할 수 있는 데이터의 양을 나타내는 통계를 볼 수 있습니다. 또한 이제 작업을 생성할 때 작업의 예상 비용을 볼 수 있습니다.	2020년 9월 3일
새 콘텐츠	민감한 데이터 검색 작업의 구성, 실행 및 관리에 대한 정보가 추가되었습니다.	2020년 8월 31일
새로운 기능	이제 관리형 데이터 식별자는 브라질의 특정 유형의 개인 식별 정보를 탐지할 수 있습니다.	2020년 7월 31일

업데이트 내용	사용자 정의 데이터 식별자의 정규 표현식에 지원되는 구문에 대한 정보가 추가되었습니다.	2020년 7월 30일
업데이트 내용	관리형 데이터 식별자에 대한 키워드 요구 사항을 추가하고 각 민감한 데이터 검색 작업에서 생성할 수 있는 조사 결과 수에 대한 할당량을 늘렸습니다.	2020년 7월 17일
새 콘텐츠	Amazon 사용 및 결과 모니터링 EventBridge 및 AWS Security Hub 처리에 대한 정보가 추가되었습니다. 여기에는 결과에 대한 EventBridge 이벤트 스키마와 정책 및 민감한 데이터 발견에 대한 이벤트 예제가 포함됩니다.	2020년 6월 22일
새 콘텐츠	조사 결과 분석 및 숨기기에 대한 정보가 추가되었습니다.	2020년 6월 17일
새 콘텐츠	세부 검색 결과를 S3 버킷에 저장하도록 Macie를 구성하기에 대한 지침을 추가했습니다.	2020년 6월 2일
새 콘텐츠	Macie가 탐지할 수 있는 민감한 데이터 유형과 Amazon S3 객체의 민감한 데이터를 탐지하기 위한 암호화 요구 사항에 대한 정보가 추가되었습니다.	2020년 5월 28일
정식 출시	이는 Amazon Macie 사용 설명서의 최초 공개 릴리스입니다.	2020년 5월 13일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.