Amazon Macie Classic

사용 설명서

Amazon Macie Classic: 사용 설명서

Table of Contents

이 문서는 Amazon Macie Classic에 대한 사용 설명서입니다. 새로운 Amazon Macie에 대한 자세한 내용은 Amazon Macie 사용 설명서를 참조하십시오. Macie Classic 콘솔에 액세스하려면 https://console.aws.amazon.com/macie/에서 Macie 콘솔을 열고 탐색 창에서 Macie Classic을 선택합니다.

문서의 영문과 번역 사이에 충돌이 있는 경우에는 영문 버전을 따릅니다. 번역 버전은 기계 번역을 사용하여 제공합니다.

Amazon Macie Classic란 무엇입니까?

이제 설계가 대폭 향상되고 추가 기능이 포함된 새로운 Amazon Macie를 보다 저렴한 가격으로 대부분의 AWS 리전에서 사용할 수 있습니다. 새롭고 향상된 기능을 살펴보고 사용하여 비용 절감의 이점을 누리는 것이 좋습니다. 새로운 Amazon Macie의 기능 및 요금에 대한 자세한 내용은 Amazon Macie 단원을 참조하십시오. 새로운 Macie로 이전하는 방법에 대한 자세한 내용은 새로운 Amazon Macie로 이전 (p. 3) 단원을 참조하십시오.

Amazon Macie Classic의 기능

Amazon Macie Classic는 기계 학습을 사용하여 AWS에서 민감한 데이터를 자동으로 검색, 분류 및 보호하는 보안 서비스입니다. Macie Classic는 PII(개인 식별 정보) 또는 지적 재산과 같은 민감한 데이터를 인식합니다. 이 데이터에 대한 액세스와 이동이 어떻게 이루어지는지 알 수 있는 대시보드와 알림을 제공합니다.

Macie Classic는 다음 AWS 리전에서 지원됩니다.

- 미국 동부(버지니아 북부) (us-east-1)
- 미국 서부(오레곤) (us-west-2)

데이터 검색 및 분류

Amazon Macie Classic를 사용하여 다음과 같이 비즈니스 운영에 핵심적인 데이터를 식별하고 액세스 패턴과 사용자 행동을 분석할 수 있습니다.

- AWS 환경에서 새로운 데이터를 지속적으로 모니터링
- 인공 지능을 사용하여 기록 데이터의 액세스 패턴 이해
- 사용자 활동, 애플리케이션 및 서비스 계정에 자동으로 액세스
- 자연 언어 처리(NLP) 방법을 사용하여 데이터 이해
- 지능적이고 정확하게 비즈니스 가치를 데이터에 할당하고, 고유 조직에 따라 비즈니스 운영에 핵심적인 데이터의 우선 순위 지정
- 고유한 보안 알림 및 사용자 지정 정책 정의 생성

데이터 보안

Amazon Macie Classic를 사용하면 다음과 같이 보안을 사전에 준수하고 예방적 차원의 보안을 달성할 수 있습니다.

- PII, PHI, 규제 문서, API 키, 보안 키 등 다양한 데이터 유형을 식별 및 보호
- 즉각적인 감사를 가능케 하는 자동화된 로그로 보안 및 규정 준수 확인
- 정책 및 액세스 제어 목록의 변경 사항 확인
- 사용자 행동의 변화를 관찰하고 실행 가능한 알림 수신
- 데이터와 계정 자격 증명이 보호 구역에서 벗어나면 알림 수신
- 비즈니스 운영에 핵심적인 문서가 대량으로 내부 및 외부에서 공유되는 경우 감지

Macie Classic에 액세스

Macie Classic 콘솔은 Macie Classic을 액세스하고 사용하기 위한 브라우저 기반 인터페이스입니다. AWS 계정에 로그인하고 다음 링크 중 하나를 사용하여 Macie Classic 콘솔을 엽니다.

- https://us-east-1.redirection.macie.aws.amazon.com/
- https://us-west-2.redirection.macie.aws.amazon.com/

그런 다음 탐색 창에서 Macie Classic를 선택합니다.

새로운 Amazon Macie로 이전

이제 설계가 대폭 향상되고 추가 기능이 포함된 새로운 Amazon Macie를 보다 저렴한 가격으로 대부분의 AWS 리전에서 사용할 수 있습니다. 이러한 개선 사항을 활용하는 동시에 비용을 절감할 수 있도록 새로운 Macie로 이전하는 것이 좋습니다. 새로운 Macie를 사용하면 기본 AWS 콘솔 또는 포괄적인 API를 통해 다음과 같은 작업을 수행할 수 있습니다.

- 개수 제한 없이 Amazon Simple Storage Service(Amazon S3) 버킷 모니터링 및 분석.
- S3 객체에 포함된 민감한 데이터를 심층적으로 검색. 새로운 Macie를 사용하면 S3 객체에서 처음 20MB 이상의 데이터를 분석할 수 있습니다.
- 사용자 지정 데이터 식별자를 작성하고 사용하여 특정 시나리오의 민감한 데이터 검색.
- Macie 리소스에 태그 지정.
- Macie 리소스용 AWS CloudFormation 템플릿 개발 및 배포.
- 여러 계정에 대해 중앙 집중식으로 Macie 관리. 새로운 Macie는 AWS Organizations와 통합되므로 단일 AWS 조직에 대해 최대 5,000개의 Macie 계정을 관리할 수 있습니다. 또한 여러 계정을 관리하는 데 기본 Macie 기능을 계속 사용하여 단일 Macie 마스터 계정으로 최대 1,000개의 멤버 계정을 관리할 수 있습니다.
- 단지 두 개의 리전이 아니라 대부분의 AWS 리전에서 민감한 데이터 검색 및 모니터링.

새로운 Macie의 모든 기능 및 요금에 대한 자세한 내용은 Amazon Macie 단원을 참조하십시오.

현재 Amazon Macie Classic 계정이 있는 경우 해당 계정이 계속 지원됩니다. 새 계정을 활성화하면 새 Amazon Macie를 사용하도록 해당 계정이 구성됩니다. 새 Macie의 계정을 활성화하고 관리하는 방법에 대한 자세한 내용은 Amazon Macie 사용 설명서를 참조하십시오.

이 항목에서는 Amazon Macie Classic에서 새로운 Amazon Macie로 이전하는 프로세스의 각 단계를 안내합니다.

주제

Overview

새로운 Amazon Macie로 손쉽게 이전할 수 있도록 Macie Classic에 내보내기 기능을 추가했습니다. 이 기능을 사용하면 선택적으로 현재 AWS 리전의 계정에 대한 모든 데이터 분류 결과의 복사본을 생성하고 내보낼 수 있습니다. Macie Classic은 이러한 복사본을 S3 버킷에 추가하고 사용자가 지정한 AWS Key Management Service(AWS KMS) 키를 사용하여 데이터를 암호화합니다. 멤버 계정이 있는 마스터 계정의 경우 연결된 모든 멤버 계정에 대한 분류 결과가 내보내기에 포함됩니다.

내보내기가 시작되면 Macie Classic 계정과 해당 멤버 계정이 읽기 전용 모드로 전환됩니다. 즉, 모니터링할 S3 버킷을 추가하고 분류 작업을 생성하는 등의 작업을 수행할 수 없습니다. 또한 Macie Classic에서는 계

정 및 해당 멤버 계정에 대한 대부분의 작업을 중지합니다. 여기에는 데이터 모니터링, 분류 생성 및 Amazon CloudWatch Events에 기반한 알림 전송이 포함됩니다. Macie Classic는 내보내기가 진행되는 동안 이 모드로 유지됩니다. 데이터 양에 따라 내보내기를 완료하는 데 최대 2주가 걸릴 수 있습니다. 언제든지 내보내기 상태를 확인할 수 있습니다.

> **Important**
>
> 계정과 해당 멤버 계정에 대해 지속적으로 데이터를 검색하고 모니터링하려면 새로운 Amazon Macie에서 이러한 계정을 활성화하고 구성한 후에 내보내기 프로세스를 시작하십시오. 새로운 Macie로 이 작업을 수행하는 방법은 Amazon Macie User Guide 단원을 참조하십시오.
> 내보내기가 진행되는 동안 새로운 계정과 기존 계정 모두에 비용이 발생합니다. 각 Macie Classic 계정에는 CloudTrail 이벤트 처리 및 데이터 보존 기간 연장에 대한 요금이 계속 부과되며, 활성화하는 새로운 각 Macie 계정에도 요금이 부과됩니다. Macie 요금에 대한 자세한 내용은 Amazon Macie 요금을 참조하십시오.

내보내기가 완료되면 Macie Classic이 계정 및 해당 멤버 계정에 대한 CloudTrail 이벤트 처리도 중지합니다. 이는 Macie Classic에서 이러한 계정에 대한 모든 작업을 중지했음을 의미합니다. 그러나 계정은 여전히 활성화되어 있습니다.

내보내기가 완료된 후에는 계속 Macie Classic 콘솔을 사용하여 기존 데이터 분류 결과를 볼 수 있습니다. (새로운 기능을 사용하여 이러한 결과를 보거나 액세스할 수 없습니다. Macie.) 또한 S3 버킷에서 로그 관리 또는 시각화 도구로 결과를 가져올 수 있습니다. 또한 계속 AWS Security Hub에서 기존 알림 데이터를, AWS CloudTrail에서 기존 이벤트 데이터를 보고 분석할 수 있습니다.

Macie Classic 계정 및 해당 멤버 계정에 대해 이 프로세스를 완료한 후에는 계정을 비활성화할 수 있습니다. 여러 AWS 리전에서 Macie Classic를 사용하는 경우 각 추가 리전에 대해 이 프로세스를 반복합니다.

시작하기 전

내보내기 프로세스를 시작하고 새로운 Amazon Macie로 이전하기 전에 필요한 리소스가 있는지 확인하고 다음 사항을 고려하십시오.

계정

멤버 계정이 있는 마스터 계정의 경우 첫 번째 단계는 새로운 Macie로 이전할 계정을 결정하는 것입니다. 마스터 계정만 내보내기 프로세스를 시작하고 이후에 멤버 계정을 비활성화할 수 있습니다. 또한 내보내기 프로세스를 시작하면 Macie Classic에서 마스터 계정과 모든 멤버 계정을 읽기 전용 모드로 자동 전환하고 마스터 계정 및 모든 멤버 계정의 데이터를 내보냅니다.

여러 단계를 통해 새로운 Macie로 이전하려면 조직의 현재 마스터-멤버 계정 연결을 조정하는 것이 좋습니다. 특정 단계에서 특정 멤버 계정을 제외하려면 마스터 계정에서 해당 계정을 연결 해제합니다. 그런 다음 선택적으로 해당 멤버 계정에 대한 새 마스터 계정을 생성할 수 있습니다. 이렇게 하면 별도의 단계로 새 마스터 계정 및 해당 멤버 계정에 대한 내보내기 프로세스를 시작할 수 있습니다.

지속적인 모니터링의 필요 여부

내보내기 프로세스가 시작되면 Macie Classic이 계정 및 해당 멤버 계정에 대한 대부분의 작업을 중지합니다. 여기에는 데이터 모니터링, 분류 생성 및 Amazon CloudWatch Events에 기반한 알림 전송이 포함됩니다. Macie Classic는 내보내기가 진행되는 동안 이 모드로 유지됩니다. 데이터 양에 따라 내보내기를 완료하는 데 최대 2주가 걸릴 수 있습니다.

계정과 해당 멤버 계정에 대해 지속적으로 데이터를 검색하고 모니터링하려면 내보내기 프로세스를 시작하기 전에 새로운 Amazon Macie에서 이러한 계정을 활성화하고 구성합니다. 이 작업을 수행하는 방법은 Amazon Macie User Guide 단원을 참조하십시오. 이 경우 새로운 계정과 기존 계정에 모두 비용이 발생합니다. Macie Classic 계정에 대한 내보내기가 진행 중인 동안에는 CloudTrail 이벤트 처리 및 데이터 보존 기간 연장에 대한 요금이 계속 부과되며, 내보내기가 완료된 후에는 계정을 비활성화할 때까지 데이터 보존 기간 연장에 대한 요금이 계속 부과됩니다. 또한 활성화하는 새로운 각 Macie 계정에도 요금이 부과됩니다. Macie 요금에 대한 자세한 내용은 Amazon Macie 요금을 참조하십시오.

S3 버킷

내보내기 프로세스를 시작할 때 분류 결과를 내보낼 위치를 지정할 수 있습니다. 여기에는 두 가지 옵션이 있습니다.

- 만든 새로운 S3 버킷을 사용합니다. – 만든 특정 S3 버킷으로 결과를 내보내고 버킷의 이름이 시작되어 버킷의 이름이 `awsmacie-*`. (이를 통해 Macie Classic 기존의 서비스 연결 역할 (p. 16) for your Macie Classic 계정) 또한, Macie Classic 버킷에서 개체를 만듭니다. 사용할 버킷 정책의 예는 이 항목의 뒷부분에 나오는 내보내는 데이터 분류 결과에 대한 S3 버킷 정책 (p. 8)을 참조하십시오.
- Macie Classic이 생성하는 새 S3 버킷 사용 – S3 버킷을 지정하지 않으면 Macie Classic에서 자동으로 새 버킷을 생성합니다. (이렇게 하려면, 서비스 연결 역할 (p. 16) for your Macie Classic 계정) 버킷을 찾으려면 `awsmacie-classification-export` 버킷 이름. 또한 Macie Classic은 버킷을 생성할 때 버킷에 데이터를 쓸 수 있도록 허용하는(버킷 소유자가 버킷의 객체를 완전히 제어할 수 있는 경우에 한 함) 버킷 정책도 적용합니다. 정책을 보려면 이 항목의 뒷부분에 나오는 내보내는 데이터 분류 결과에 대한 S3 버킷 정책 (p. 8)을 참조하십시오.

새로운 Amazon Macie에서도 분류 결과를 S3 버킷에 저장하는 옵션을 제공합니다. 그러나 두 Macie 버전의 분류 결과를 저장하는 데 동일한 버킷을 사용하지 않는 것이 좋습니다. Macie Classic과 새로운 Macie는 데이터 분류 결과에 서로 다른 스키마를 사용합니다.

암호화 키

내보내기 프로세스를 시작할 때 Macie Classic이 내보내는 데이터를 암호화하는 데 사용할 AWS Key Management Service(AWS KMS) 키를 지정해야 합니다. 따라서 내보내기를 시작하기 전에 사용할 키를 결정하고 키의 ARN을 기록해 두는 것이 좋습니다. 내보내기 프로세스를 시작할 때 ARN을 입력해야 합니다. 또한 Macie Classic이 `Encrypt` 및 `GenerateDataKey*` 작업을 수행할 수 있도록 키 정책에서 허용하는지 확인합니다. 예: .

```
{
    "Version":"2012-10-17",
    "Id":"key-policy-id",
    "Statement":[
        {
            "Sid":"Allow Macie Classic to use the key",
            "Effect":"Allow",
            "Principal":{
                "Service":"macie.amazonaws.com"
            },
            "Action":[
                "kms:Encrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource":"*"
        }
    ]
}
```

단계 1. 데이터 분류 결과 내보내기

새 Amazon Macie로 이전하는 첫 번째 단계는 선택적으로 계정에 대한 기존 데이터 분류 결과를 내보내는 것입니다. 계정이 마스터 계정인 경우 연결된 모든 멤버 계정에 대한 결과가 포함됩니다.

데이터 분류 결과를 내보낼 때 Macie Classic는 S3 버킷에 있는 하나 이상의 객체에 결과 데이터를 복사하며, 사용자가 지정한 AWS KMS 키를 사용하여 데이터를 암호화합니다. 객체 수는 보유한 데이터의 양에 따라 달라집니다.

각 객체에는 분류 결과 배치에 대한 JSON 형식의 데이터가 포함되어 있습니다. 데이터는 날짜별로 그룹화되며 데이터 분류 결과에 Macie Classic 스키마가 사용됩니다. 즉, 데이터가 Macie Classic 대시보드의 그룹 및

필드에 밀접하게 매핑됩니다. 이러한 그룹 및 필드의 팔레트는 Amazon Macie Classic가 모니터링하는 데이터 및 활동 보기 (p. 41). 각 개체는 조각이며 gzip 파일로 저장됩니다.

Macie Classic는 이러한 객체 외에도 빈 `JOB_START_TOKEN` 객체를 버킷에 생성합니다. 이 객체는 내보내기가 시작되었음을 나타냅니다. 또한 빈 `JOB_END_TOKEN` 객체를 생성하는데, 이 객체는 내보내기가 완료되었음을 나타냅니다. 모든 쿼리 또는 후속 데이터 분석에서 이러한 객체를 무시할 수 있습니다.

데이터 분류 결과를 내보내려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 Macie Classic을 선택합니다.
3. 멤버 계정이 있는 마스터 계정의 경우 내보내기 프로세스에 포함하지 않을 멤버 계정을 연결 해제합니다.
4. Macie Classic과 통합한 모든 S3 리소스를 제거합니다. 이렇게 하려면 탐색 창에서 통합을 선택한 다음 모니터링할 데이터 원본에 대한 현재 선택 사항을 모두 지웁니다.
5. 콘솔 상단의 배너에서 분류 데이터 내보내기를 선택합니다. 배너가 숨겨져 있으면 브라우저에서 페이지를 다시 로드합니다.
6. KMS 키에, 내보낸 데이터를 암호화하는 데 사용할 AWS KMS 키의 Amazon 리소스 이름(ARN)을 입력합니다.
7. (선택 사항) 버킷 이름에, 내보낸 데이터를 저장할 S3 버킷의 이름을 입력합니다. 버킷 이름을 입력하지 않으면 Macie Classic에서 자동으로 버킷을 생성하고 버킷에 대한 버킷 정책 (p. 8)을 정의합니다.
8. 내보내기 설정 입력을 마치면 데이터 내보내기를 선택하여 내보내기를 시작합니다. Macie Classic는 내보내는 데이터를 위한 S3 버킷을 생성하거나 액세스할 수 있는지 확인합니다. 또한 사용자가 지정한 AWS KMS 키를 사용할 수 있는지 확인합니다. 이러한 작업을 수행할 수 있는 경우 분류 결과를 버킷에 복사하기 시작합니다.
9. 언제든지 내보내기 상태를 확인하려면 1단계와 2단계를 반복하여 Macie Classic 콘솔로 돌아갑니다. 콘솔 상단의 배너에 내보내기 상태가 표시됩니다. 내보내기가 완료되면 배너에 내보내기가 완료되었습니다가 표시됩니다.

   문제가 발생하여 Macie Classic이 내보내기를 완료할 수 없는 경우 배너에 내보내기에 실패했습니다가 표시됩니다. 문제에 대한 세부 정보를 표시하려면 내보내기에 실패했습니다를 선택합니다. 문제의 특성에 따라 데이터를 다시 내보내거나 AWS Support에 문의하여 지원을 받으십시오.
10. 내보내기가 완료되면 내보낸 데이터가 포함된 S3 버킷으로 이동하여 결과를 확인합니다. 결과의 수와 특성은 Macie Classic 대시보드에 나타나는 데이터와 일치해야 합니다.

각 추가 Macie Classic 마스터 계정(및 해당 멤버 계정) 및 AWS 리전에 대해 이전 단계를 반복합니다.

단계 2. 비활성화 Macie Classic 계정

내보내기가 완료되고 결과를 확인한 후 Macie Classic 계정을 비활성화할 수 있습니다.

> Warning
>
> Macie Classic 계정을 비활성화하면 다음과 같은 결과가 발생합니다.
>
> - Macie Classic이 마스터 계정 및 모든 멤버 계정의 리소스에 대한 액세스 권한을 잃게 됩니다.
> - 사용자와 마스터 계정 및 해당 멤버 계정의 다른 모든 사용자가 Macie Classic 콘솔에 액세스할 수 없습니다.
> - Macie Classic이 마스터 계정 및 모든 해당 멤버 계정에 대한 데이터를 모니터링하는 동안 수집한 모든 메타데이터를 삭제합니다. Macie Classic을 비활성화한 후 90일 이내에 이 메타데이터가 모두 Macie Classic 시스템 백업에서 만료되고 제거됩니다.

Macie Classic은 사용자를 위해 다른 AWS 서비스에 생성 및 저장한 데이터는 삭제하지 않습니다. 여기에는 AWS Security Hub의 기존 알림 데이터, AWS CloudTrail의 이벤트 데이터 및 Amazon S3의 로그 및 내보낸 분류 결과가 포함됩니다.

Macie Classic 계정을 비활성화하려면

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 Macie Classic을 선택합니다.
3. 콘솔 상단의 배너에서 Macie Classic 비활성화를 선택합니다.
4. 나타나는 창에서 Macie Classic 계정을 비활성화한 결과에 대한 정보를 검토합니다. 계정 및 멤버 계정을 비활성화하려면 해당 확인란을 선택한 다음 Macie Classic 비활성화를 선택합니다.

단계 3. 리소스 삭제 및 메타데이터 수집

Macie Classic 계정을 비활성화하면 계정의 다른 AWS 서비스에 생성, 사용 또는 저장된 데이터나 리소스는 삭제되지 않고, 계정에 대해 직접 수집 및 저장된 데이터만 삭제됩니다.

불필요한 비용을 피하기 위해, Macie Classic 계정을 비활성화한 후 다음 리소스와 데이터를 평가하는 것이 좋습니다.

- AWS CloudTrail 데이터 이벤트 – Macie Classic은 모니터링한 버킷에 대한 Amazon S3 데이터 이벤트를 활성화하는 추적을 생성했습니다. 새로운 Amazon Macie는 다른 아키텍처를 사용하며 Amazon S3 데이터 이벤트를 활성화할 필요가 없습니다. 이 로깅이 더 이상 필요하지 않으면 Macie Classic에서 생성된 추적을 삭제해야 합니다. 이를 통해 추적에 대한 추가 AWS CloudTrail 요금 청구를 방지할 수 있습니다. 또한 S3 버킷에 저장된 로그 데이터를 보관하거나 제거할 수도 있습니다.
- Amazon CloudWatch Events – Macie Classic은 계정에 대해 생성된 CloudWatch 이벤트를 삭제하지 않습니다. 새로운 Macie도 이벤트를 CloudWatch에 게시하지만 이벤트 데이터가 새 Macie 계정에만 해당됩니다. 따라서 비활성화한 Macie Classic 계정에 대한 이벤트를 삭제하도록 결정할 수 있습니다.
- 레거시 IAM 역할 – 서비스 연결 역할을 지원하기 시작한 June 21, 2018 이전에 Macie Classic을 사용한 경우 AWS 계정에 더 이상 필요하지 않은 두 개의 레거시 AWS Identity and Access Management(IAM) 역할이 있습니다. 이러한 역할은 AmazonMacieServiceRole 및 AmazonMacieSetupRole입니다. 이러한 역할은 Macie Classic이 사용자를 대신하여 다른 AWS 서비스를 호출 할 수 있도록 허용했습니다. 새로운 Macie는 이러한 역할을 사용하지 않습니다. 따라서 삭제하는 것을 고려할 수 있습니다.

June 21, 2018 이후에 Macie Classic을 사용하기 시작한 경우 사용자를 대신하여 AWSServiceRoleForAmazonMacie 서비스 수준 역할이 생성되었습니다. 이 역할을 통해 Macie Classic이 사용자를 대신하여 민감한 데이터를 검색하고 모니터링할 수 있었습니다. 새로운 Amazon Macie에서도 이 서비스 수준 역할을 사용하여 유사한 작업을 수행합니다. 따라서 새 Macie 계정에서 사용할 수 있도록 이 역할을 유지하는 것이 좋습니다.

단계 4. 새로운 기능 Amazon Macie 계정

새로운 Amazon Macie를 사용할 준비가 되면 AWS 계정에 로그인하고 Amazon Macie 콘솔로 이동하여 새 Macie 계정을 활성화합니다. 새로운 Macie의 기능 및 요금에 대한 자세한 내용은 Amazon Macie 단원을 참조하십시오.

새 Macie 계정을 활성화하려면

1. AWS Management 콘솔에 로그인한 후 https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 시작하기를 선택합니다.
3. Macie 활성화를 선택합니다.

몇 분 내에 Macie 은 계정에 대한 S3 버킷의 인벤토리를 생성하고 보안 및 액세스 제어를 위해 버킷 모니터링을 시작합니다.

다음 단계

새로운 데이터로 지속적인 데이터 분류 보장 Macie 계정에서 다음 단계는 다음과 같습니다.

검색 결과의 저장소 구성

새로운 Macie민감한 데이터 검색 작업을 생성하고 실행하여 S3 버킷에서 민감한 데이터를 분석하고 보고합니다. 언제 Macie 작업을 실행하며, 이는 민감한 데이터 검색. Macie 찾았습니다. Macie는 또한 민감한 데이터 검색 결과작업이 분석하거나 분석하려고 시도하는 S3 객체에 대한 세부 분석 기록입니다. 여기에는 민감한 데이터가 포함되지 않은 개체가 포함되어 있으므로 소견을 생성하지 마십시오.

검색 결과를 저장하도록 저장소를 구성할 때 계정에 대한 이러한 결과의 장기 액세스 및 저장을 보장합니다. 자세한 내용은 발견 결과 저장 및 유지 in the Amazon Macie 사용자 안내서.

정기 데이터 검색 작업 생성

검색 결과에 저장소를 구성한 후 매일, 매주 또는 매월 주기적으로 실행되는 작업을 생성합니다. 불필요한 비용 및 중복된 분류 데이터를 피하기 위해, 내보내기 프로세스를 시작했을 때와 같이 특정 시점 이후에 생성되거나 수정되었던 개체만 분석하도록 작업을 구성할 수 있습니다. Macie Classic. 작업 범위를 구성할 때 이 작업을 두 가지 방법으로 수행할 수 있습니다.

- 작업 전에 생성된 개체 건너뛰기 – 이 구성을 사용하면 작업의 첫 번째 실행은 작업 생성을 마친 후 생성되는 객체만 분석합니다. 각 후속 실행은 이전 실행 후 생성된 개체만 분석합니다. 이 구성을 사용하려면 기존 개체 포함 아래의 확인란 예약된 작업.
- 특정 시간 전에 생성되었거나 마지막으로 수정된 개체를 건너뜁니다. – 이 구성에서는 작업 실행이 지정한 날짜 및 시간 전에 생성되거나 수정되었던 개체를 건너뜁니다. 이 구성을 사용하려면 추가 설정 섹션. 대상 개체 기준, 선택 마지막 수정. 에서 대상 확인란을 선택하고 개체의 최신 생성 또는 수정 날짜와 시간을 입력한 다음 제외.

자세한 내용은 민감한 데이터 검색 작업 실행 in the Amazon Macie 사용자 안내서.

계정 구성 및 관리에 대한 다음 단계 및 정보를 보려면 Amazon Macie 사용자 안내서. 이 가이드에서는 AWS Organizations 또는 전송 Macie 회원 초대.

참조 수출 데이터 분류 결과에 대한 S3 버킷 정책

이 항목의 앞부분 (p. 4)에서 설명한 대로, Macie Classic은 자동으로 S3 버킷을 생성하여 내보내는 데이터 분류 결과를 저장할 수 있습니다. 이 옵션을 선택하면 Macie Classic에서 생성하는 버킷에 대해 다음 버킷 정책 (p. 8)을 정의합니다.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"MacieClassificationExportS3WriteBucketPolicy",
            "Effect":"Allow",
            "Principal":{
                "Service":"macie.amazonaws.com"
            },
            "Action":"s3:PutObject",
            "Resource":"arn:aws:s3:::{bucket_name}/*",
            "Condition":{
                "StringEquals":{
                    "s3:x-amz-acl":"bucket-owner-full-control"
                }
            }
```

```
        },
        {
            "Sid":"Deny non-HTTPS access",
            "Action":"s3:*",
            "Effect":"Deny",
            "Principal":"*",
            "Resource":[
                "arn:aws:s3:::{bucket_name}/*",
                "arn:aws:s3:::{bucket_name}"
            ],
            "Condition":{
                "Bool":{
                    "aws:SecureTransport":false
                }
            }
        },
        {
            "Sid":"Deny incorrect encryption header",
            "Action":"s3:PutObject",
            "Effect":"Deny",
            "Principal":"*",
            "Resource":"arn:aws:s3:::{bucket_name}/*",
            "Condition":{
                "StringNotEquals":{
                    "s3:x-amz-server-side-encryption-aws-kms-key-id":"{kms_key_arn}"
                }
            }
        },
        {
            "Sid":"Deny unencrypted object uploads",
            "Action":"s3:PutObject",
            "Effect":"Deny",
            "Principal":"*",
            "Resource":"arn:aws:s3:::{bucket_name}/*",
            "Condition":{
                "StringNotEquals":{
                    "s3:x-amz-server-side-encryption":"aws:kms"
                }
            }
        }
    ]
}
```

개념 및 용어

Amazon Macie Classic를 시작할 때 핵심 개념을 알아두면 유익합니다.

Account

AWS 리소스를 포함하는 표준 AWS 계정입니다. Amazon Web Services(AWS)에 가입할 때 계정은 AWS의 모든 서비스에 자동으로 등록되며, 로그인하기 위해 사용한 계정 AWS 활성화한 경우 Macie Classic 은(는) 마스터 계정.

Macie Classic과 다른 계정을 통합한 경우 이러한 계정을 멤버 계정이라고 합니다.

Note

멤버 계정의 사용자에게는 Macie Classic 콘솔에 대한 액세스 권한이 부여되지 않습니다. 마스터 계정 사용자만 Macie Classic 콘솔을 통해 Macie Classic 마스터 및 멤버 계정의 리소스를 모니터링하고 보호합니다.

알림

잠재적인 보안 문제에 대한 알림 Macie Classic 은(는) 을(를) 검색합니다. 경고가 Macie Classic 콘솔을 사용하여 지난 24시간 동안 발생한 모든 활동에 대한 포괄적인 설명을 제공합니다.

Macie Classic는 다음과 같은 유형의 알림을 제공합니다.

- 기본 알림 – 보안 검사에 의해 생성되는 알림은 Macie Classic 를 수행합니다. Macie Classic에는 두 가지 유형의 기본 알림이 있습니다.
  - 관리(다음에 의해 처리됨) Macie Classic) 기본 알림을 수정할 수 없습니다. 기존 관리형 기본 알림은 활성화하거나 비활성화할 수만 있습니다.
  - 정확한 사양에 따라 생성하고 수정할 수 있는 사용자 정의 기본 경고.
- 예측 경보 – 내 활동에 따른 자동 알림 AWS 설정된 정상 활동 기준선을 벗어나는 인프라. 보다 구체적으로, Macie Classic 지속적으로 모니터링 IAM 사용자 및 역할 활동 AWS 일반적인 동작의 모델을 구축합니다. 그런 다음 정상 기준선과의 편차를 찾고 이러한 활동을 감지하면 자동 예측 경고를 생성합니다. 예를 들어, 하루에 많은 수의 S3 객체를 업로드하거나 다운로드하는 사용자는 일반적으로 일주일에 한 두 개의 S3 객체를 다운로드하는 경우 경고를 트리거할 수 있습니다.

Macie Classic 알림의 콘텐츠에 대한 자세한 설명과 알림 범주를 비롯한 자세한 내용은 Amazon Macie Classic 알림 (p. 48) 단원을 참조하십시오.

데이터 원본

한 세트의 데이터의 출처 또는 위치. 데이터를 분류하고 보호하기 위하여 Macie Classic는 다음 데이터 소스의 정보를 분석하고 처리합니다.

AWS CloudTrail 이벤트 로그(다음 포함) Amazon S3 개체 수준 API 작업

AWS CloudTrail 은(는) 다음 이력을 제공합니다. AWS 다음을 사용하여 수행된 API 호출을 포함하여 귀하의 계정에 대한 API 호출 AWS Management 콘솔, AWS SDK, 명령줄 도구 및 상위 수준 AWS 서비스. AWS CloudTrail 또한 은(는) AWS 지원 서비스를 위한 API CloudTrail, 호출이 수행된 원본 IP 주소 및 호출이 발생한 시기입니다. 자세한 내용은 AWS CloudTrail란 무엇입니까?를 참조하십시오.

데이터 분류를 위해, Macie Classic 에서 기능을 사용합니다. CloudTrail S3 개체(데이터 이벤트)에 대한 개체 수준 API 활동을 캡처합니다. 자세한 내용은 CloudTrail 로그 파일 작업을 참조하십시오.

Amazon S3

이번 릴리스에서는 Macie Classic 에 저장된 데이터를 분석하고 처리합니다. Amazon S3 버킷. Macie Classic에서 분류하고 모니터링하게 하려는 객체를 포함하는 S3 버킷을 선택할 수 있습니다.

Amazon Simple Storage Service (Amazon S3)는 인터넷용 스토리지입니다. Amazon S3 는 데이터를 버킷 에 있는 개체로 저장합니다. 객체는 파일과 해당 파일을 설명하는 메타데이터(선택 사항)로 구성됩니다. 개체를 에 저장하려면 Amazon S3, 버킷 에 저장할 파일을 업로드합니다. 버킷은 객체의 컨테이너입니다. 자세한 내용은 Amazon Simple Storage Service 시작하기를 참조하십시오.

User

다음 맥락에서 Macie Classic, 사용자는 AWS Identity and Access Management (IAM) 요청을 하는 ID. Macie Classic 은(는) CloudTrail `userIdentity` 요소를 사용하여 다음 사용자 유형을 구분합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

- 루트 – 귀하의 계정 자격 증명 (으)로 요청이 이루어졌습니다.
- IAM 사용자 – 이 요청은 IAM 사용자.
- 가정된 역할 – 에 대한 호출을 통해 역할로 획득한 임시 보안 자격 증명으로 요청이 이루어졌습니다. AWS Security Token Service (AWS STS) `AssumeRole` API 작업.
- 통합 사용자 – 임시 보안 자격 증명으로 요청이 이루어졌으며, 이 자격 증명은 AWS STS `GetFederationToken` API 작업.
- AWS 계정 – 다른 계정 이(가) 요청했습니다.
- AWS 서비스 – 이 요청은 다음에 속하는 계정에 의해 이루어졌습니다. AWS 서비스.

에서 사용자를 지정할 때 Macie Classic 특수 Macie Classic 형식 호출됨 `macieUniqueId`. 사용자 지정의 예로는 사용자 탭, 연구 기본 경고의 사용자에게 클라우드트레일 데이터. 더 `macieUniqueId` IAM의 조합입니다. `UserIdentity` 요소 및 `recipientAccountId`. 자세한 내용은 이전 목록을 참조하십시오. `UserIdentity` 및 정의 `recipientAccountId` 에서 CloudTrail 레코드 내용. 다음 예제는 의 다양한 구조를 나열합니다. `macieUniqueId`사용자 ID 유형에 따라 다음을 수행합니다.

- `123456789012:root`
- `123456789012:user/Bob`
- `123456789012:assumed-role/Accounting-Role/Mary`

더 많은 예제를 보려면 사용자 활동별로 Amazon Macie Classic–에서 모니터링하는 데이터 분석 (p. 54) 단원을 참조하십시오.

Amazon Macie Classic 설정

AWS에 가입할 때 AWS 계정은 AWS의 모든 서비스에 자동으로 등록되며, Macie Classic을 활성화하는 데 사용한 AWS 계정은 마스터 계정으로 자동 지정됩니다. 자세한 내용은 개념 및 용어 (p. 10) 단원을 참조하십시오.

Macie Classic을 활성화하면 Macie Classic에서 서비스 연결 역할이 생성됩니다. 이 역할과 관련된 IAM 정책에 대한 자세한 내용은 Amazon Macie Classic에 대한 서비스 연결 역할 (p. 16) 단원을 참조하십시오.

Macie Classic을 활성화하면 알림을 생성하기 위해 즉시 AWS CloudTrail에서 독립적인 데이터 스트림을 수집하여 분석하기 시작합니다. Macie Classic는 잠재적 보안 문제가 있는지 확인하는 용도로만 이 데이터를 사용하며, Macie Classic는 사용자를 위해 CloudTrail를 관리하거나 이러한 이벤트와 로그를 사용자에게 제공하지 않습니다. Macie Classic과 독립적으로 CloudTrail을 활성화한 경우 CloudTrail 콘솔 또는 API를 통해 설정을 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail User Guide 단원을 참조하십시오.

언제든지 Macie Classic를 비활성화하여 CloudTrail 이벤트의 처리 및 분석을 중지할 수 있습니다. 자세한 내용은 Amazon Macie Classic 비활성화 및 수집한 메타데이터 삭제 (p. 88) 단원을 참조하십시오.

Amazon S3와 Macie Classic 통합

데이터를 분류하고 보호하기 위해 Macie Classic는 CloudTrail 및 Amazon S3의 정보를 분석하고 처리합니다. Macie Classic을 사용하려면 계정에서 CloudTrail을 활성화해야 합니다. S3를 Macie Classic와 통합할 필요는 없습니다. 그러나 Macie Classic 설정의 일부로 Amazon S3와 통합하는 것이 좋습니다. Macie Classic의 데이터 분류 방식에 대한 자세한 내용은 Amazon Macie Classic를 사용하여 데이터 분류 (p. 21) 단원을 참조하십시오.

Amazon S3와 통합할 경우 Macie Classic는 Amazon S3 객체 수준 API 활동(데이터 이벤트)에 대한 로그를 저장하기 위해 버킷과 추적 기록을 생성하며, 이를 다른 CloudTrail 로그와 함께 분석하고 처리합니다.

사전 조건

- 통합하는 데 사용하는 IAM 자격 증명(사용자, 역할, 그룹)에는 필수 권한이 있어야 합니다. 필요한 권한을 부여하려면 AmazonMacieFullAccess 관리형 정책을 이 자격 증명에 연결합니다. 자세한 내용은 Macie Classic에 대한 미리 정의된 AWS 관리형 정책 (p. 14)을 참조하십시오.

Amazon S3와 통합하려면

1. Macie Classic 마스터 계정 역할을 하는 계정의 자격 증명으로 AWS에 로그인합니다.
2. Amazon Macie 콘솔을 열고 탐색 창에서 Macie Classic을 선택합니다.
3. 탐색 창에서 통합을 선택합니다.
4. S3 리소스를 선택하고 계정(마스터 또는 멤버) 옆의 선택을 선택합니다.
5. S3 리소스와 Macie Classic 통합 페이지에서 추가를 선택합니다. 현재 AWS 리전에서 최대 250개의 Amazon S3 리소스를 선택한 다음 추가를 선택합니다.
6. 기존 객체의 분류에 대해 기본 설정인 전체를 유지합니다. 일회 분류 방법은 선택한 S3 버킷의 기존 모든 객체에 한 번만 적용됩니다.

   Macie Classic에는 선택한 각 버킷에 대해 다음 정보가 표시됩니다.

   - 총 객체 – 총 객체 수입니다.
   - 처리된 추정치 – Macie Classic가 분류할 데이터의 총 크기입니다.
   - 비용 추정치 – 모든 객체를 분류하기 위한 비용 추정치입니다.

Macie Classic에는 선택한 모든 버킷에 대해 다음 합계도 표시됩니다.

- 총 크기 – 데이터의 총 크기입니다.
- 총 객체 수 – 총 객체 수입니다.
- 처리된 추정치 – Macie Classic가 분류할 데이터의 총 크기입니다.
- 총 비용 추정치 – 모든 객체를 분류하기 위한 비용 추정치입니다.

각 버킷의 비용 추정치는 처리된 추정치 값을 기준으로 합니다. 총 비용 추정치는 접두사가 아니라, S3 버킷에 대해서만 제공됩니다. 자세한 내용은 Amazon Macie Classic 요금을 참조하십시오.

일회 분류 비용 추정치는 버킷 접두사당이 아니라 S3 버킷당으로만 계산됩니다. 버킷 접두사를 선택하면 전체 S3 버킷에 대한 비용 추정치가 총 비용 추정치에 포함됩니다. 동일한 S3 버킷의 여러 접두사를 선택하면 전체 S3 버킷에 대한 비용 추정치가 총 비용 추정치에 한 번만 포함됩니다.

7. 선택을 마쳤으면 검토를 선택합니다.
8. 선택 검토를 마쳤으면 Start classification(분류 시작)을 선택합니다.

Amazon Macie Classic에 대한 액세스 제어

AWS는 보안 자격 증명을 사용하여 사용자를 식별하고 AWS 리소스에 대한 액세스 권한을 부여합니다. AWS Identity and Access Management(IAM) 의 기능을 사용하면 다른 사용자, 서비스 및 애플리케이션이 AWS 리소스를 완전히 또는 제한된 방식으로 사용할 수 있습니다. 이를 위해 보안 자격 증명을 공유하지 않아도 됩니다.

기본값으로 IAM 사용자는 AWS 리소스를 생성, 확인 또는 수정할 수 있는 권한이 없습니다. IAM 사용자가 로드 밸런서와 같은 리소스에 액세스하여 작업을 수행하도록 허용하려면 다음을 수행하십시오.

1. IAM 사용자에게 특정 리소스와 API 작업을 사용할 권한을 부여하는 IAM 정책을 생성합니다.
2. 정책을 IAM 사용자 또는 IAM 사용자가 속한 그룹에 연결합니다.

사용자 또는 사용자 그룹에 정책을 연결하면 지정된 리소스에 대해 지정된 작업을 수행할 권한이 허용되거나 거부됩니다.

예를 들어 IAM을 사용하여 AWS 계정 아래에 사용자 및 그룹을 생성할 수 있습니다. IAM 사용자는 사용자, 시스템 또는 애플리케이션입니다. 그런 다음 정책을 사용하여 지정된 리소스에 대한 특정 작업을 수행할 수 있도록 사용자 및 그룹에 권한을 부여합니다.

자세한 내용은 IAM 사용 설명서 단원을 참조하십시오.

Macie Classic에 관리자 액세스 권한 부여

마스터 계정 사용자는 Macie Classic 콘솔에 액세스한 후 Macie Classic를 구성하여 마스터와 멤버 계정에서 리소스를 모니터링하고 보호하도록 할 수 있습니다. 마스터 및 멤버 계정에 대한 자세한 내용은 개념 및 용어 (p. 10) 및 Amazon Macie Classic에서 멤버 계정 및 Amazon S3 통합 (p. 19) 단원을 참조하십시오.

마스터 계정 사용자가 Macie Classic 콘솔을 사용하려면 필요한 권한을 부여받아야 합니다. 이렇게 하려면 다음 정책 문서를 사용하여 IAM 정책을 만든 후 마스터 Macie Classic 계정에 속하는 사용자 자격 증명 유형에 연결할 수 있습니다. 이 정책은 Macie Classic 콘솔의 전체 기능을 사용할 수 있는 마스터 계정 사용자 권한을 부여합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
```

```
      {
         "Effect": "Allow",
         "Resource": "*",
         "Action":[
            "macie:*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "*",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "macie.amazonaws.com"
            }
         }
      }
   ]
}
```

Macie Classic에 읽기 전용 액세스 권한 부여

사용자가 Macie Classic 콘솔의 모든 데이터를 보려면 필요한 권한을 부여받아야 합니다. 읽기 전용 액세스 권한을 부여하려면 다음 정책 문서를 사용하여 사용자 지정 정책을 만들고 이를 IAM 사용자, 그룹 또는 역할에 연결하면 됩니다. 이 정책은 사용자에게 Macie Classic 콘솔의 정보를 볼 권한만 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "macie:Get*",
                "macie:List*",
                "macie:Describe*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Macie Classic에 대한 미리 정의된 AWS 관리형 정책

AWS가 생성한 관리형 정책은 일반 사용 사례에서 필요한 권한을 부여합니다. Macie Classic에 필요한 액세스를 기반으로 AWS 계정의 IAM 사용자에게 이러한 정책을 연결할 수 있습니다.

- AmazonMacieFullAccess – Macie Classic에 대한 전체 액세스 권한을 부여합니다.
- AmazonMacieHandshakeRole – Macie Classic에 대한 서비스 연결 역할을 생성할 수 있는 권한을 부여합니다.

다음은 서비스 연결 역할로 대체된 레거시 정책입니다. 자세한 내용은 Macie Classic의 레거시 역할 (p. 18) 단원을 참조하십시오.

- AmazonMacieServiceRole – 데이터 분석을 활성화하기 위해 계정의 리소스 종속성에 대한 읽기 전용 액세스를 Macie Classic에 부여합니다.
- AmazonMacieSetupRole – AWS 계정에 대한 액세스 권한을 Macie Classic에 부여합니다.

핸드셰이크 역할 생성

다음과 같이 마스터 계정에서 Macie Classic에 AmazonMacieHandshakeRole 정책의 권한을 부여하는 역할을 생성할 수 있습니다.

IAM 콘솔을 사용하여 AWSMacieServiceCustomerHandshakeRole을 생성하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Roles(역할)를 선택합니다.
3. [Create role]을 선택하고 다음 작업을 수행합니다.
   a. 신뢰할 수 있는 유형의 엔터티 선택에서 AWS 서비스를 선택합니다.
   b. 사용 사례 선택에서 EC2를 선택합니다.
   c. Next: Permissions(다음: 권한)를 선택합니다.
4. 권한 정책 연결 페이지에서 AmazonMacieHandshakeRole 정책의 확인란을 선택하고 다음: 태그를 선택합니다.
5. (선택 사항) 역할에 태그를 추가한 다음 Next: Review(다음: 검토)를 선택하십시오.
6. 검토 페이지에서 다음을 수행합니다.
   a. 역할 이름에 AWSMacieServiceCustomerHandshakeRole을 입력합니다.
   b. 역할 설명에 다음을 입력합니다. 마스터 계정이 멤버 계정에서 서비스 연결 역할을 생성할 수 있도록 허용합니다.
   c. 역할 생성을 선택합니다.
7. 다음과 같이 신뢰 정책을 편집합니다.
   a. 방금 생성한 AWSMacieServiceCustomerHandshakeRole을 선택합니다.
   b. 신뢰 관계 탭에서 신뢰 관계 편집을 선택합니다.
   c. 다음 신뢰 정책을 입력합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "macie.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "master-account-id"
        }
      }
    }
  ]
}
```

   d. Update Trust Policy(신뢰 정책 업데이트)를 선택합니다.

AWS CLI를 사용하여 WSMacieServiceCustomerHandshakeRole을 생성하려면

1. 다음 트러스트 정책을 생성하고 `macie-handshake-trust-policy.json`이라는 텍스트 파일로 저장합니다.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "macie.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "master-account-id"
        }
      }
    }
  ]
}
```

2. 역할을 생성하고 이전 단계에서 create-role 명령을 사용하여 생성한 신뢰 정책을 지정합니다.

```
aws iam create-role --role-name AWSMacieServiceCustomerHandshakeRole --assume-role-
policy-document file://macie-handshake-trust-policy.json
```

3. attach-role-policy 명령을 사용하여 AmazonMacieHandshakeRole 정책을 역할에 연결합니다.

```
aws iam attach-role-policy --role-name AWSMacieServiceCustomerHandshakeRole --policy-
arn arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole
```

Amazon Macie Classic에 대한 서비스 연결 역할

Amazon Macie Classic는 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용하여 사용자를 대신해 다른 AWS 서비스를 호출합니다. Macie Classic만 서비스 연결 역할을 수임할 수 있으므로 서비스 연결 역할은 권한을 Macie Classic에 위임할 수 있는 안전한 방법을 제공합니다.

서비스 연결 역할에 의해 부여된 권한

Macie Classic에서는 AWSServiceRoleForAmazonMacie라는 이름의 서비스 연결 역할을 사용합니다. 이는 allows Amazon Macie to discover, classify, and protect sensitive data in AWS on your behalf입니다.

이 역할은 해당 역할을 수임할 `macie.amazonaws.com` 서비스를 신뢰합니다.

역할은 다음과 같은 AWS 관리형 정책으로 구성됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetEventSelectors",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:ListTags",
                "cloudtrail:LookupEvents",
                "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"
            ]
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:cloudtrail:*:*:trail/AWSMacieTrail-DO-NOT-EDIT",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:PutEventSelectors"
            ]
        },
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::awsmacie-*",
                "arn:aws:s3:::awsmacietrail-*",
                "arn:aws:s3:::*-awsmacietrail-*"
            ],
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteBucketPolicy",
                "s3:DeleteBucketWebsite",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersion",
                "s3:DeleteObjectVersionTagging",
                "s3:PutBucketPolicy"
            ]
        }
    ]
}
```

Macie Classic에 대한 서비스 연결 역할 생성

AWSServiceRoleForAmazonMacie 역할을 수동으로 생성할 필요는 없습니다. Macie Classic는 다음과 같이 사용자를 대신해 이 역할을 생성합니다.

- 마스터 계정 — 처음 Macie Classic를 활성화하면 AWSServiceRoleForAmazonMacie 역할이 자동으로 생성됩니다.
- 멤버 계정 — 마스터 계정이 멤버 계정을 Macie Classic에 연결할 때 AWSServiceRoleForAmazonMacie 역할이 생성됩니다. 마스터 Macie Classic 계정에 대해 생성하지 않은 서비스 연결 역할은 멤버 Macie Classic 계정에 적용되지 않습니다.

Macie Classic가 사용자를 대신해 서비스 연결 역할을 생성하려면 필수 권한이 있어야 합니다. 사용자, 그룹 또는 역할과 같은 IAM 엔터티에 필요한 권한을 부여하려면 AmazonMacieFullAccess 정책을 연결합니다. 자세한 내용은 Macie Classic에 대한 미리 정의된 AWS 관리형 정책 (p. 14) and 서비스 링크된 역할 권한 in the IAM 사용 설명서.

AWSServiceRoleForAmazonMacie 역할을 수동으로 생성할 수도 있습니다. 자세한 내용은 서비스 연결 역할 만들기 in the IAM 사용 설명서.

Macie Classic의 레거시 역할

서비스 연결 역할 지원이 시작된 June 21, 2018 전에 Macie Classic를 사용한 경우, Macie Classic에 사용자를 대신해 다른 AWS 서비스를 호출할 권한을 부여하는 IAM 역할이 AWS 계정(Macie Classic 마스터 또는 멤버)에 이미 있습니다. 이러한 역할은 AmazonMacieServiceRole 및 AmazonMacieSetupRole입니다. 이러한 역할은 Macie Classic 설정의 일부로 마스터 계정에 대한 Macie Classic AWS CloudFormation 템플릿 또는 멤버 계정에 대한 Macie Classic AWS CloudFormation 템플릿을 시작할 때 생성되었습니다.

서비스 연결 역할이 (마스터 및 멤버 계정에 있는) 이전에 생성된 이러한 IAM 역할을 대체합니다. 이전에 생성한 역할은 삭제되지 않았지만 사용자를 대신해 다른 서비스를 호출할 권한을 Macie Classic에 부여하는 데 더 이상 사용되지 않습니다. IAM 콘솔을 사용하여 이전에 생성된 역할을 삭제할 수 있습니다.

Macie Classic에 대한 서비스 연결 역할 편집

서비스 연결 역할을 생성한 후에는 역할의 이름을 변경할 수 없습니다. 그러나 IAM를 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하십시오.

Macie Classic에 대한 서비스 연결 역할 삭제

이제 Amazon Macie Classic를 사용할 필요가 없는 경우 AWSServiceRoleForAmazonMacie 역할을 삭제하는 것이 좋습니다.

마스터 계정의 경우 Macie Classic를 비활성화해야 Macie Classic 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 Macie Classic 리소스에 대한 권한을 실수로 제거할 수 없습니다. 멤버 계정의 경우 마스터 계정에서 먼저 이를 Macie Classic에서 연결 해제해야 합니다. 자세한 정보는 Amazon Macie Classic 비활성화 및 수집한 메타데이터 삭제 (p. 88) 단원을 참조하십시오.

Macie Classic를 비활성화하면 AWSServiceRoleForAmazonMacie 역할이 삭제되지 않습니다. Macie Classic를 다시 활성화하면 기존 AWSServiceRoleForAmazonMacie 역할이 사용됩니다.

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 AWSServiceRoleForAmazonMacie 역할을 삭제할 수 있습니다. 자세한 내용은 서비스 연결 역할 삭제 in the IAM 사용 설명서.

Amazon Macie Classic에서 멤버 계정 및 Amazon S3 통합

멤버 계정을 Macie Classic와 통합하고 Amazon S3를 Macie Classic와 통합할 있습니다. 마스터 및 멤버 계정에 대한 자세한 내용은 개념 및 용어 (p. 10) 단원을 참조하십시오.

목차

멤버 계정과 Macie Classic 통합

멤버 계정을 Macie Classic와 통합할 때, 해당 멤버 계정에서 리소스와 활동을 모니터링하도록 Macie Classic를 활성화합니다.

사전 조건

- AWSServiceRoleForAmazonMacie 서비스 연결 역할을 생성하는 데 필요한 권한을 멤버 계정에 부여하는 역할을 생성합니다. 자세한 내용은 핸드셰이크 역할 생성 (p. 15) 단원을 참조하십시오.

멤버 계정을 Macie Classic와 통합하려면

1. Macie Classic 마스터 계정 역할을 하는 AWS 계정의 자격 증명으로 AWS에 로그인합니다.
2. Macie Classic 콘솔을 열고 탐색 창에서 통합을 선택합니다.
3. 계정을 선택하고 멤버 AWS 계정 옆에 있는 더하기 아이콘(+)을 선택합니다.
4. 메시지가 표시되면 쉼표로 구분하여 하나 이상의 계정 ID를 입력합니다. [Add accounts]를 선택합니다.
5. (선택 사항) Macie Classic가 통합한 각 멤버 계정에 AWSServiceRoleForAmazonMacie 역할을 생성했는지 확인합니다. 자세한 내용은 Macie Classic에 대한 서비스 연결 역할 생성 (p. 17) 단원을 참조하십시오.

Macie Classic가 모니터링할 데이터 지정

Macie Classic가 모니터링할 데이터가 포함된 S3 버킷과 접두사를 지정할 수 있습니다.

사전 조건

- 통합하는 데 사용하는 IAM 자격 증명(사용자, 역할, 그룹)에는 필수 권한이 있어야 합니다. 필요한 권한을 부여하려면 AmazonMacieFullAccess 관리형 정책을 이 자격 증명에 연결합니다. 자세한 내용은 Macie Classic에 대한 미리 정의된 AWS 관리형 정책 (p. 14)을 참조하십시오.

Amazon S3와의 통합을 업데이트하려면

1. Macie Classic 마스터 계정 역할을 하는 계정의 자격 증명으로 AWS에 로그인합니다.
2. Macie Classic 콘솔을 열고 탐색 창에서 통합을 선택합니다.

3. S3 리소스를 선택하고 계정(마스터 또는 멤버) 옆의 선택을 선택합니다.
4. S3 리소스와 Macie Classic 통합 페이지에서 편집을 선택하여 이미 통합된 버킷/접두사를 편집하거나 추가를 선택하여 새 버킷/접두사를 통합합니다.
5. 기존 객체의 분류에 대해 기본 설정인 전체를 유지합니다. 일회 분류 방법은 선택한 S3 버킷의 기존 모든 객체에 한 번만 적용됩니다.

   Macie Classic에는 선택한 각 버킷에 대해 다음 정보가 표시됩니다.

   - 총 객체 – 총 객체 수입니다.
   - 처리된 추정치 – Macie Classic가 분류할 데이터의 총 크기입니다.
   - 비용 추정치 – 모든 객체를 분류하기 위한 비용 추정치입니다.

   Macie Classic에는 선택한 모든 버킷에 대해 다음 합계도 표시됩니다.

   - 총 크기 – 데이터의 총 크기입니다.
   - 총 객체 수 – 총 객체 수입니다.
   - 처리된 추정치 – Macie Classic가 분류할 데이터의 총 크기입니다.
   - 총 비용 추정치 – 모든 객체를 분류하기 위한 비용 추정치입니다.

   각 버킷의 비용 추정치는 처리된 추정치 값을 기준으로 합니다. 총 비용 추정치는 접두사가 아니라, S3 버킷에 대해서만 제공됩니다. 자세한 내용은 Amazon Macie Classic 요금을 참조하십시오.

   일회 분류 비용 추정치는 버킷 접두사당이 아니라 S3 버킷당으로만 계산됩니다. 버킷 접두사를 선택하면 전체 S3 버킷에 대한 비용 추정치가 총 비용 추정치에 포함됩니다. 동일한 S3 버킷의 여러 접두사를 선택하면 전체 S3 버킷에 대한 비용 추정치가 총 비용 추정치에 한 번만 포함됩니다.
6. 선택을 마쳤으면 검토를 선택합니다.
7. 선택 검토를 마쳤으면 Start classification(분류 시작)을 선택합니다.

암호화된 객체

Amazon S3 버킷에 저장된 객체가 암호화된 경우, Macie Classic는 다음과 같은 이유로 해당 객체를 읽거나 분류할 수 없을 수도 있습니다.

- Amazon S3 관리형 암호화 키(SSE-S3)를 사용하여 Amazon S3 객체를 암호화한 경우, Macie Classic는 설정 프로세스 중에 생성된 역할을 사용하여 객체를 읽고 분류할 수 있습니다.
- AWS KMS 관리형 키(SSE-KMS)를 사용하여 Amazon S3 객체를 암호화한 경우, Macie Classic는 `AWSMacieServiceCustomerServiceRole` IAM 역할 또는 `AWSServiceRoleForAmazonMacie` 서비스 연결 역할을 KMS 고객 마스터 키(CMK)에 대한 키 사용자로 추가한 경우에만 객체를 읽고 분류할 수 있습니다. 이러한 역할 중 하나를 KMS CMK에 대한 키 사용자로 추가하지 않으면 Macie Classic가 객체를 읽거나 분류할 수 없습니다. 그러나 는 여전히 객체를 보호하는 데 사용되는 KMS CMK를 비롯하여 객체에 대한 메타데이터를 저장합니다.
- 클라이언트 측 암호화를 사용하여 Amazon S3 객체가 암호화된 경우, Macie Classic는 객체를 읽고 분류할 수 없으나 객체에 대한 메타데이터는 저장할 수 있습니다.

Amazon Macie Classic를 사용하여 데이터 분류

Macie Classic를 사용하여 AWS 클라우드에 저장되어 있는 중요하고 민감한 데이터를 분류할 수 있습니다. 현재 Macie Classic는 Amazon S3 버킷에 저장된 데이터를 분석하고 처리합니다. 또한 Macie Classic는 데이터를 분류하기 위해 AWS CloudTrail의 기능을 사용하여 S3 객체에 대한 객체 수준 API 활동(데이터 이벤트)을 캡처합니다. 그러나 Macie Classic가 S3 버킷을 하나 이상 모니터링하도록 지정해야 Macie Classic에서 CloudTrail 데이터 이벤트만 모니터링합니다.

Macie Classic가 모니터링할 S3 버킷을 지정한 후, 새로운 데이터가 AWS 인프라로 유입될 때 Macie Classic가 이를 지속적으로 모니터링하고 검색하도록 활성화합니다. 자세한 정보는 Macie Classic가 모니터링할 데이터 지정 (p. 19) 단원을 참조하십시오.

제한

- Macie Classic는 계정에서 분류할 수 있는 데이터 양에 기본 한도를 둡니다. 이 데이터 제한에 도달하면 Macie Classic는 이 계정의 데이터 분류를 중지합니다. 기본 데이터 분류 한도는 3TB입니다. AWS Support에 문의하여 기본 한도 증가를 요청할 수 있습니다.
- Macie Classic에서 지원되지 않는 형식의 파일이 포함된 S3 버킷을 지정하는 경우, Macie Classic는 이를 분류하지 않습니다.
- Macie Classic의 콘텐츠 분류 엔진은 S3 객체의 첫 20MB까지 처리합니다.

Macie Classic 사용 요금에는 Macie Classic에서 처리하는 콘텐츠에 대한 비용만 포함됩니다. 예를 들어 Macie Classic는 .wav 파일(이미지 또는 동영상)에서 텍스트를 추출할 수 없으므로 해당 콘텐츠를 처리하지 않으며 이에 대한 요금이 청구되지 않습니다.

목차

지원되는 압축 및 보관 파일 형식

현재 Macie Classic는 다음 압축 및 보관 파일 형식을 지원합니다.

- bzip
- GZIP
- LZO
- RAR
- SNAPPY
- AR

- CPIO
- Unix 덤프
- TAR
- zip
- XZ
- Pack200
- bzip2
- 7z
- ARJ
- LZMA
- DEFLATE
- Brotli

콘텐츠 유형

Macie Classic는 데이터를 모니터링하기 시작한 후 여러 콘텐츠 자동 분류 방법을 사용하여 중요하고 민감한 데이터를 식별하고 우선 순위를 지정하여 데이터에 비즈니스 가치를 정확하게 할당합니다. 이러한 방법 중 하나는 콘텐츠 유형별로 분류하는 것입니다.

Macie Classic는 콘텐츠 유형별로 데이터 객체를 분류하기 위해 파일 헤더에 포함된 식별자를 사용합니다. Macie Classic는 일련의 관리형(Macie Classic 큐레이트) 콘텐츠 유형을 제공하며, 각 유형에는 1부터 10까지 위험 수준이 지정되어 있습니다. 여기서 10은 위험 수준이 가장 높고 1은 위험 수준이 가장 낮습니다.

Macie Classic는 객체 하나에 콘텐츠 유형 하나만 할당할 수 있습니다.

기존의 콘텐츠 유형을 수정하거나 새로운 콘텐츠 유형을 추가할 수는 없습니다. 기존 콘텐츠 유형을 활성화하거나 비활성화할 수 있으며 따라서 Macie Classic를 활성화하거나 비활성화하여 분류 프로세스 중에 객체에 이를 할당할 수 있습니다.

콘텐츠 유형을 보거나, 활성화하거나 비활성화하려면

1. Macie Classic 콘솔에서 설정 페이지로 이동합니다.
2. Classify data(데이터 분류) 섹션에서 콘텐츠 유형을 선택합니다.
3. 세부 정보를 보려면 목록에서 관리형 콘텐츠 유형을 선택합니다.

   세부 정보 페이지에서 콘텐츠 유형을 활성화하거나 비활성화하려면, Enabled/Disabled(활성화됨/비활성화됨) 드롭다운 메뉴를 사용하여 저장을 선택합니다.

다음 목록에서는 Macie Classic가 객체에 할당할 수 있는 모든 콘텐츠 유형 목록을 설명합니다.

이름	설명
application/cap	WireShark 또는 Tcpdump 패킷 캡처
application/epub+zip	application/epub
application/illustrator	Adobe Illustrator
application/java	이진수(Java)
application/java-archive	application/java-archive
application/java-Serialized-object	application/java-Serialized-object

application/java-vm	application/java-vm
application/javascript	application/javascript
application/json	JSON
application/msaccess	application/msaccess
application/msexcel	Microsoft Excel
application/msonenote	application/msonenote
application/mspowerpoint	Microsoft PowerPoint
application/msword	Microsoft Word
application/octet-stream	application/octet-stream
application/octet-stream+fon	application/octet-stream+fon
application/ogg	application/ogg
application/onenote	application/onenote
application/pdf	Adobe PDF
application/pgp	application/pgp
application/pgp-encrypted	application/pgp-encrypted
application/pgp-keys	PGP 키
application/pgp-signature	PGP 서명
application/postscript	Adobe Postscript
application/rar	RAR 압축된 아카이브
application/rdf+xml	application/rdf+xml
application/rss+xml	application/rss+xml
application/rtf	application/rtf
application/tar	TAR 아카이브
application/unknown	application/unknown
application/vnd.3gpp.pic-bw-small	application/vnd.3gpp.pic-bw-small
application/vnd.android.package-archive	Android 패키지
application/vnd.audiograph	application/vnd.audiograph
application/vnd.balsamiq.bmpr	Balsamiq 목업
application/vnd.cups-ppd	application/vnd.cups-ppd
application/vnd.curl.car	application/vnd.curl.car
application/vnd.dvb.ait	application/vnd.dvb.ait
application/vnd.google-apps.document	Google Apps 문서
application/vnd.google-apps.drawing	application/vnd.google-apps.drawing

application/vnd.google-apps.form	Google Apps 양식
application/vnd.google-apps.map	Google Apps 맵
application/vnd.google-apps.presentation	Google Apps 프레젠테이션
application/vnd.google-apps.script	Google Apps 스크립트
application/vnd.google-apps.spreadsheet	Google Apps 스프레드시트
application/vnd.google-earth.kmz	Google Earth KMZ
application/vnd.jcp.javame.midlet-rms	application/vnd.jcp.javame.midlet-rms
application/vnd.jgraph.mxfile	application/vnd.jgraph.mxfile
application/vnd.jgraph.mxfile.realtime	application/vnd.jgraph.mxfile.realtime
application/vnd.jgraph.mxfile.rtlegacy	application/vnd.jgraph.mxfile.rtlegacy
application/vnd.kde.kontour	application/vnd.kde.kontour
application/vnd.lotus-1-2-3	application/vnd.lotus-1-2-3
application/vnd.lotus-organizer	application/vnd.lotus-organizer
application/vnd.mozilla.xul+xml	application/vnd.mozilla.xul+xml
application/vnd.ms-excel	Excel
application/vnd.ms-excel.addin.macroEnabled.12	application/vnd.ms-excel.addin.macroEnabled.12
application/vnd.ms-excel.sheet.binary.macroEnabled.12	Microsoft Excel - 매크로 사용
application/vnd.ms-excel.sheet.macroEnabled.12	Microsoft Excel - 매크로 사용
application/vnd.ms-excel.sheet.macroenabled.12	application/vnd.ms-excel.sheet.macroenabled.12
application/vnd.ms-excel.template.macroenabled.12	application/vnd.ms-excel.template.macroenabled.12
application/vnd.ms-fontobject	application/vnd.ms-fontobject
application/vnd.ms-htmlhelp	application/vnd.ms-htmlhelp
application/vnd.ms-officetheme	application/vnd.ms-officetheme
application/vnd.ms-package.relationships+xml	application/vnd.ms-package.relationships+xml
application/vnd.ms-pki.seccat	Microsoft Exchange Server Certificate Store
application/vnd.ms-powerpoint	Microsoft PowerPoint
application/vnd.ms-powerpoint.presentation.macroEnabled.12	application/vnd.ms-powerpoint.presentation.macroEnabled.12
application/vnd.ms-powerpoint.slideshow.macroEnabled.12	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
application/vnd.ms-powerpointtd	Microsoft PowerPoint
application/vnd.ms-project	application/vnd.ms-project

application/vnd.ms-publisher	application/vnd.ms-publisher
application/vnd.ms-word.document.macroEnabled.12	Microsoft Word - 매크로 사용
application/vnd.ms-xpsdocument	application/vnd.ms-xpsdocument
application/vnd.oasis.opendocument.chart	application/vnd.oasis.opendocument.chart
application/vnd.oasis.opendocument.graphics	application/vnd.oasis.opendocument.graphics
application/vnd.oasis.opendocument.presentation	표시
application/vnd.oasis.opendocument.spreadsheet	스프레드시트
application/vnd.oasis.opendocument.text	Open Document Text
application/vnd.openxmlformats-officedocument.presentationml.presentation	Microsoft PowerPoint
application/vnd.openxmlformats-officedocument.presentationml.slide	Microsoft Powerpoint
application/vnd.openxmlformats-officedocument.presentationml.slideshow	Microsoft Powerpoint
application/vnd.openxmlformats-officedocument.presentationml.template	application/vnd.openxmlformats-officedocument.presentationml.template
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Microsoft Excel
application/vnd.openxmlformats-officedocument.spreadsheetml.template	application/vnd.openxmlformats-officedocument.spreadsheetml.template
application/vnd.openxmlformats-officedocument.wordprocessingml.document	Microsoft Word
application/vnd.openxmlformats-officedocument.wordprocessingml.template	application/vnd.openxmlformats-officedocument.wordprocessingml.template
application/vnd.palm	application/vnd.palm
application/vnd.symbian.install	application/vnd.symbian.install
application/vnd.tcpdump.pcap	Wireshark 또는 Tcpdump 패킷 캡처
application/vnd.visio	Microsoft Visio
application/vns.ms-outlook	Microsoft Outlook 메시지
application/x-7z-compressed	7zip 압축된 아카이브
application/x-adobeaamdetect	Adobe Application Manager
application/x-adobeexmandetect	application/x-adobeexmandetect
application/x-apple-diskimage	Apple 디스크 이미지
application/x-bittorrent	application/x-bittorrent
application/x-bzip2	application/x-bzip2
application/x-cab	application/x-cab

application/x-cfs-compressed	application/x-cfs-compressed
application/x-coredump	application/x-coredump
application/x-couponprinterplugin	application/x-couponprinterplugin
application/x-dbm	application/x-dbm
application/x-dosexec	실행 가능
application/x-dvi	application/x-dvi
application/x-executable	실행 가능
application/x-fla	application/x-fla
application/x-font	application/x-font
application/x-font-otf	application/x-font-otf
application/x-font-ttf	application/x-font-ttf
application/x-font-type1	application/x-font-type1
application/x-font-woff	application/x-font-woff
application/x-freemind	application/x-freemind
application/x-gtar	GNU tar 압축된 아카이브
application/x-gzip	GNU Zip 압축된 아카이브
application/x-iso9660-image	application/x-iso9660-image
application/x-iwork-keynote-sffkey	application/x-iwork-keynote-sffkey
application/x-iwork-numbers-sffnumbers	application/x-iwork-numbers-sffnumbers
application/x-iwork-pages-sffpages	application/x-iwork-pages-sffpages
application/x-javascript	application/x-javascript
application/x-maker	application/x-maker
application/x-mobipocket-ebook	application/x-mobipocket-ebook
application/x-ms-shortcut	application/x-ms-shortcut
application/x-ms-wmz	application/x-ms-wmz
application/x-msdos-program	Microsoft Windows 응용 프로그램
application/x-msi	application/x-msi
application/x-msmetafile	application/x-msmetafile
application/x-mspublisher	application/x-mspublisher
application/x-nawk	application/x-nawk
application/x-ns-proxy-autoconfig	application/x-ns-proxy-autoconfig
application/x-object	application/x-object
application/x-perl	Perl 소스 코드

application/x-pkcs12	PKI 인증서
application/x-pkcs7-crl	PKI 파일
application/x-python-code	소스 코드(python)
application/x-rar-compressed	RAR 압축된 아카이브
application/x-redhat-package-manager	application/x-redhat-package-manager
application/x-sas	통계 분석
application/x-sharedlib	application/x-sharedlib
application/x-shellscript	셸 스크립트
application/x-shockwave-flash	application/x-shockwave-flash
application/x-silverlight-app	application/x-silverlight-app
application/x-stuffit	Stuffit 압축된 아카이브
application/x-subrip	application/x-subrip
application/x-tar	TAR 아카이브
application/x-tex-tfm	Apache 글꼴
application/x-texinfo	application/x-texinfo
application/x-troff-man	application/x-troff-man
application/x-wais-source	application/x-wais-source
application/x-x509-ca-cert	application/x-x509-ca-cert
application/x-xcf	application/x-xcf
application/x-xfig	application/x-xfig
application/x-xpinstall	application/x-xpinstall
application/x-zip	Zip 압축된 아카이브
application/xhtml+xml	application/xhtml+xml
application/xmind	application/xmind
application/xml	XML 텍스트
application/xv+xml	application/xv+xml
application/zip	Zip 압축된 아카이브
binary/octet-stream	binary/octet-stream
chemical/x-cache	chemical/x-cache
chemical/x-cerius	chemical/x-cerius
chemical/x-gamess-input	chemical/x-gamess-input
chemical/x-genbank	chemical/x-genbank
chemical/x-mdl-sdfile	chemical/x-mdl-sdfile

chemical/x-pdb	Protein Databank chemical/x-pdb
chemical/x-rosdal	chemical/x-rosdal
message/rfc822	message/rfc822
text/cache-manifest	text/cache-manifest
text/calendar	text/calendar
text/css	text/css
text/csv	쉼표로 구분된 값
text/html	text/html
text/json	JavaScript Object Notation
text/plain	일반 텍스트
text/rtf	text/rtf
text/tab-separated-values	탭으로 구분된 값
text/texmacs	text/texmacs
text/vnd.graphviz	text/vnd.graphviz
text/x-asm	소스 코드(Assembly)
text/x-bibtex	text/x-bibtex
text/x-c	소스 코드(c)
text/x-c++hdr	소스 코드(C++ headers)
text/x-c++src	소스 코드(c++)
text/x-chdr	소스 코드(C headers)
text/x-component	text/x-component
text/x-csh	소스 코드(C shell)
text/x-csharp	소스 코드(C#)
text/x-csrc	소스 코드(C)
text/x-diff	text/x-diff
text/x-dsrc	text/x-dsrc
text/x-java	소스 코드(Java)
text/x-java-source	소스 코드(Java)
text/x-markdown	text/x-markdown
text/x-nfo	text/x-nfo
text/x-objcsrc	소스 코드(Objective-C)
text/x-pascal	소스 코드(Pascal)
text/x-perl	소스 코드(Perl)

text/x-python	소스 코드(Python)
text/x-sfv	text/x-sfv
text/x-sh	소스 코드(x-sh)
text/x-sql	소스 코드(SQL)
text/x-tex	text/x-tex
text/x-url	text/x-url
text/x-vcard	text/x-vcard
text/xml	XML 텍스트

파일 확장명

Macie Classic는 데이터를 모니터링하기 시작한 후 여러 콘텐츠 자동 분류 방법을 사용하여 중요하고 민감한 데이터를 식별하고 우선 순위를 지정하여 데이터에 비즈니스 가치를 정확하게 할당합니다. 이러한 방법 중 하나는 파일 확장명별로 분류하는 것입니다.

Macie Classic는 객체를 파일 확장명별로 분류할 수도 있습니다. Macie Classic는 관리형 파일 확장명을 여러 개 제공하며, 각 유형에는 1부터 10까지 위험 수준이 지정되어 있습니다. 여기서 10은 위험 수준이 가장 높고 1은 위험 수준이 가장 낮습니다.

Macie Classic는 객체 하나에 파일 확장명 하나만 할당할 수 있습니다.

기존의 파일 확장명을 수정하거나 새로운 파일 확장명을 추가할 수는 없습니다. 기존 파일 확장명을 활성화하거나 비활성화할 수 있으며 따라서 Macie Classic를 활성화하거나 비활성화하여 분류 프로세스 중에 객체에 이를 할당할 수 있습니다.

파일 확장명을 보거나, 활성화하거나 비활성화하려면

1. Macie Classic 콘솔에서 설정 페이지로 이동합니다.
2. Classify data(데이터 분류) 섹션에서 File extensions(파일 확장명)를 선택합니다.
3. 세부 정보를 보려면 목록에서 관리형 파일 확장명을 선택합니다.

   세부 정보 페이지에서 파일 확장명을 활성화하거나 비활성화하려면, Enabled/Disabled(활성화됨/비활성화됨) 드롭다운 메뉴를 사용하여 저장을 선택합니다.

다음은 Macie Classic가 분류 중에 객체에 할당할 수 있는 전체 파일 확장명 목록입니다.

이름	설명
7z	7-Zip 압축 파일
abc	SolidWorks CAD
accdb	Microsoft Access 데이터베이스
apk	Android에 설치 가능한 애플리케이션
bat	배치 파일
bin	압축된 아카이브. Java로 읽기 가능. 7-zip으로 압축 풀기 가능
gzip	Bzip2 압축된 아카이브

bzip2	Bzip2 압축된 아카이브
c	C 소스 코드
c#	C# 소스 코드
cab	Microsoft 캐비닛. ZIP을 통해 압축 풀기 가능
cc	C++ 소스 코드
cer	PKI 인증서
cpp	C++ 소스 코드
csv	쉼표로 구분된 값
cxx	C++ 소스 코드
dbf	dBase 데이터베이스
dbx	Microsoft Outlook Express
deb	Debian Linux 설치 패키지
dmg	Apple OS X 응용 프로그램 설치 관리자
doc	Microsoft Word
docx	Microsoft Word
dot	Microsoft Word
dotx	Microsoft Word
dwg	AutoDesk CAD
dxf	AutoCAD
eml	MIME 이메일
emlx	Apple Mail 이메일 메시지
exe	Microsoft Windows PE 실행 파일
gpg	PGP 인증서
gz	GNU Zip 압축된 아카이브
gzip	GNU Zip 압축된 아카이브
html	하이퍼 텍스트 마크업 언어
iwa	Apple iWork 문서 아카이브 파일
jar	Java 소스 코드 아카이브
java	Java 소스 코드
json	JSON(Java Script Object Notation) 값
키	Apple 기조 연설 발표
기조 연설	Apple 기조 연설 발표
lua	Lua 소스 코드

mdb	Microsoft Access 데이터베이스
msg	Microsoft Outlook 메시지
msi	Microsoft Windows 응용 프로그램 설치 관리자
odp	OpenOffice.org OpenDocument 프레젠테이션 파일
oos	OpenOffice.org 스프레드시트 파일
p12	PKI 인증서
pages	Apple Pages
pdf	Adobe PDF
perl	Perl 소스 코드
pgp	PGP 인증서
pl	Perl 소스 코드
pot	Microsoft PowerPoint
pps	Microsoft PowerPoint
ppt	Microsoft PowerPoint
pptx	Microsoft PowerPoint
pst	Microsoft Outlook
py	Python 소스 코드
rar	RAR 아카이브. 7-zip으로 압축 풀기 가능
rtf	서식 있는 텍스트
sdp	OpenOffice.org 프레젠테이션 파일
sdw	OpenOffice.org 텍스트 문서 파일
sldasm	SolidWorks CAD
slddrw	SolidWorks CAD
sldprt	SolidWorks CAD
sql	구조화 질의 언어
sxi	OpenOffice.org 프레젠테이션 파일
sxw	OpenOffice.org 쓰기 문서 파일
tar.gz	GNU Zip 압축된 아카이브
tsv	탭으로 구분된 값
txt	텍스트 문서
vdx	Microsoft Visio
vsd	Microsoft Visio
vss	Microsoft Visio

vst	Microsoft Visio
vsx	Microsoft Visio
vtw	Microsoft Visio
vtx	Microsoft Visio
xls	Microsoft Excel
xlsx	Microsoft Excel
xlw	Microsoft Excel
xml	확장형 마크업 언어(XML)
xps	Open XML 문서 사양
zip	ZIP 압축된 아카이브

주제

Macie Classic는 데이터를 모니터링하기 시작한 후 여러 콘텐츠 자동 분류 방법을 사용하여 중요하고 민감한 데이터를 식별하고 우선 순위를 지정하여 데이터에 비즈니스 가치를 정확하게 할당합니다. 이러한 방법 중 하나는 주제별로 분류하는 것입니다.

주제별 객체 분류는 Macie Classic가 데이터 객체의 콘텐츠를 검토할 때 검색하는 키워드를 기반으로 합니다. Macie Classic는 관리형 주제를 여러 개 제공하며, 각 유형에는 1부터 10까지 위험 수준이 지정되어 있습니다. 여기서 10은 위험 수준이 가장 높고 1은 위험 수준이 가장 낮습니다.

Macie Classic는 객체 하나에 주제를 하나 이상 할당할 수 있습니다.

기존의 주제를 수정하거나 새로운 주제를 추가할 수는 없습니다. 기존 테마를 활성화하거나 비활성화할 수 있으며 따라서 Macie Classic를 활성화하거나 비활성화하여 분류 프로세스 중에 객체에 이를 할당할 수 있습니다.

주제를 보거나, 활성화하거나 비활성화하려면

1. Macie Classic 콘솔에서 설정 페이지로 이동합니다.
2. Classify data(데이터 분류) 섹션에서 Themes(주제)를 선택합니다.
3. 세부 정보를 보려면 목록에서 관리형 주제를 선택합니다.

   세부 정보 페이지에서 주제를 활성화하거나 비활성화하려면, Enabled/Disabled(활성화됨/비활성화됨) 드롭다운 메뉴를 사용한 후 저장을 선택합니다.

다음은 Macie Classic가 분류 중에 객체에 할당할 수 있는 전체 주제 목록입니다.

주제 제목	최소 키워드 조합
American Express 신용카드 키워드	1
변호사 비밀유지특권	2
감사 키워드	3
은행 키워드	1
빅 데이터 프레임워크	2

Cisco 분석 키워드	1
기밀 표시	2
기업 성장 키워드	3
기업 프로젝트 계획	3
기업 제안	3
신용카드 키워드	1
암호화된 데이터 키워드	1
금융 키워드	1
해커 키워드	2
극한 분포 표시	3
Mastercard 신용카드 키워드	1
Metasploit 프레임워크 키워드	1
NMAP OS 지문	1
네트워크 스캐너 키워드	1
네트워크 서비스 지문 키워드	1
네트워크 트래픽 분석 키워드	1
OS 백도어 키워드	1
오프라인 공격 키워드	1
온라인 공격 키워드	1
Oracle DB 분석 키워드	1
암호 키워드	2
프로젝트 추적 키워드	2
소유 표시	2
실시간 처리 프레임워크	2
제한 표시	2
SSL 법의학 분석 키워드	1
암호 표시	3
중요 표시	3
사회 보장 키워드	2
주식 키워드	3
납세자 EIN 키워드	2
터널링 공격 키워드	1
미분류 표시	2

VISA 신용카드 키워드	1
취약성 평가 키워드	2
웹 익스플로이테이션 도구 키워드	1
웹 취약성 스캐너 키워드	1
pof OS 지문	2

Regex

Macie Classic는 데이터를 모니터링하기 시작한 후 여러 콘텐츠 자동 분류 방법을 사용하여 중요하고 민감한 데이터를 식별하고 우선 순위를 지정하여 데이터에 비즈니스 가치를 정확하게 할당합니다. 이러한 방법 중 하나는 regex별로 분류하는 것입니다.

regex별 객체 분류는 Macie Classic가 데이터 객체의 콘텐츠를 검토할 때 검색하는 특정 데이터 또는 데이터 패턴을 기반으로 합니다. Macie Classic는 관리형 regex를 여러 개 제공하며, 각 유형에는 1부터 10까지 위험 수준이 지정되어 있습니다. 여기서 10은 위험 수준이 가장 높고 1은 위험 수준이 가장 낮습니다.

Macie Classic는 객체 하나에 regex를 하나 이상 할당할 수 있습니다.

기존의 regex를 수정하거나 새로운 regex를 추가할 수는 없습니다. 기존 regex를 활성화하거나 비활성화할 수 있으며 따라서 Macie Classic를 활성화하거나 비활성화하여 분류 프로세스 중에 객체에 이를 할당할 수 있습니다.

regex를 보거나, 활성화하거나 비활성화하려면

1. Macie Classic 콘솔에서 설정 페이지로 이동합니다.
2. Classify data(데이터 분류) 섹션에서 Regex를 선택합니다.
3. 세부 정보를 보려면 목록에서 관리형 regex를 선택합니다.

   세부 정보 페이지에서 regex를 활성화하거나 비활성화하려면, Enabled/Disabled(활성화됨/비활성화됨) 드롭다운 메뉴를 사용하여 저장을 선택합니다.

다음은 Macie Classic가 분류 중에 객체에 할당할 수 있는 전체 regex 목록입니다.

이름	분류
Arista 네트워크 구성	Regex
BBVA Compass 송금 번호 – 캘리포니아	Regex
Bank of America 송금 번호 – 캘리포니아	Regex
Box 링크	Regex
CVE 번호	Regex
캘리포니아 운전 면허증	Regex
Chase 송금 번호 – 캘리포니아	Regex
Cisco 라우터 구성	Regex
Citibank 송금 번호 - 캘리포니아	Regex
DSA 프라이빗 키	Regex

Dropbox 링크	Regex
EC 프라이빗 키	Regex
암호화된 DSA 프라이빗 키	Regex
암호화된 EC 프라이빗 키	Regex
암호화된 프라이빗 키	Regex
암호화된 PuTTY SSH DSA 키	Regex
암호화된 PuTTY SSH RSA 키	Regex
암호화된 RSA 프라이빗 키	Regex
Google 애플리케이션 식별자	Regex
HIPAA PHI 국가 의약품 코드	Regex
Huawei 구성 파일	Regex
개인 납세자 식별 번호(ITIN)	Regex
John the Ripper	Regex
KeePass 1.x CSV 암호	Regex
KeePass 1.x XML 암호	Regex
다수의 미국 전화 번호	Regex
다수의 미국 우편 번호	Regex
Lightweight Directory Access Protocol	Regex
Metasploit 모듈	Regex
MySQL 데이터베이스 덤프	Regex
MySQLite 데이터베이스 덤프	Regex
네트워크 프록시 자동 구성	Regex
Nmap 스캔 보고서	Regex
PGP 헤더	Regex
PGP 프라이빗 키 블록	Regex
PKCS7 암호화된 데이터	Regex
암호 etc passwd	Regex
암호 etc shadow	Regex
일반 텍스트 프라이빗 키	Regex
PuTTY SSH DSA 키	Regex
PuTTY SSH RSA 키	Regex
Public Key Cryptography System(PKCS)	Regex
퍼블릭 암호화 키	Regex

RSA 프라이빗 키	Regex
SSL 인증서	Regex
SWIFT 코드	Regex
Samba 암호 구성 파일	Regex
Simple Network Management Protocol 객체 식별자	Regex
Slack 2FA 백업 코드	Regex
영국 운전 면허증 번호	Regex
영국 여권 번호	Regex
USBank 송금 번호 - 캘리포니아	Regex
United Bank 송금 번호 - 캘리포니아	Regex
Wells Fargo 송금 번호 - 캘리포니아	Regex
aws_access_key	Regex
aws_credentials_context	Regex
aws_secret_key	Regex
facebook_secret	Regex
github_key	Regex
google_two_factor_backup	Regex
heroku_key	Regex
microsoft_office_365_oauth_context	Regex
pgSQL 연결 정보	Regex
slack_api_key	Regex
slack_api_token	Regex
ssh_dss_public	Regex
ssh_rsa_public	Regex

개인 식별 정보

개인 식별 정보(PII)별 객체 분류는 NIST-80-122 및 FIPS 199 등과 같은 업계 표준에 따라 개인 정보를 식별하여 이루어집니다. Macie Classic는 다음과 같은 PII 아티팩트를 식별할 수 있습니다.

- 전체 이름
- 우편 주소
- 이메일 주소
- 신용 카드 번호
- IP 주소(IPv4 및 IPv6)

- 운전 면허증(미국)
- 국적 식별 번호(미국)
- 생년월일

PII 객체 분류의 일부로 Macie Classic는 다음 기준을 사용하여 일치하는 각 객체에 PII 영향(높음, 보통, 낮음)을 할당하기도 합니다.

- 높음
  - >= 신용카드 및 전체 이름 1개 이상
  - 기타 PII 조합 및 이름 또는 이메일 50개 이상
- 보통
  - 기타 PII 조합 및 이름 또는 이메일 5개 이상
- 낮음
  - PII 조합 및 이름 또는 이메일 1–5개
  - 위의 PII 속성(이름 또는 이메일 제외)

SVM(Support Vector Machine) 기반 분류자

Macie Classic가 S3 객체를 분류하는 데 사용하는 또 한 가지 방법은 SVM(Support Vector Machine) 분류자입니다. 이는 콘텐츠를 기반으로 정확하게 분서를 분류하기 위해 Macie Classic에서 모니터링하는 S3 객체(텍스트, 토큰 n-gram, 문자 n-gram) 내 콘텐츠와 그 메타데이터 기능(문서 길이, 확장명, 인코딩, 헤더)을 분류하는 SVM(Support Vector Machine) 분류자입니다. 이 Macie Classic 관리형 분류자는 다양한 유형의 대용량 코퍼스로 많은 훈련 데이터를 통해 훈련되었고, 소스 코드, 애플리케이션 로그, 규제 문서, 데이터베이스 백업을 포함한 여러 콘텐츠 유형을 정확하게 감지하도록 최적화되었습니다. 이 분류자는 감지한 내용을 일반화할 수도 있습니다. 예를 들어 인식하도록 학습된 소스 코드 유형과 일치하지 않는 새로운 소스 코드 유형을 감지한 경우, 감지 내용을 "소스 코드"로 일반화할 수 있습니다.

> Note
>
> 이 데이터 분류 방법은 설정 페이지에 표시되지 않습니다. Macie Classic는 다음 아티팩트 목록을 관리합니다. 편집, 활성화하거나 비활성화할 수 없습니다.

Macie Classic에서 SVM 분류자는 다음 콘텐츠 유형을 감지하도록 학습됩니다.

- 전자책
- 이메일
- 일반적인 암호화 키
- 금융
  - SEC 규제 양식
- JSON
  - AWS CloudTrail 로그
  - Jupyter 노트북
- 애플리케이션 로그
  - Apache 형식
  - Amazon S3 서버 로그
  - Linux syslog
- 데이터베이스
  - MongoDB 백업

  - MySQL 백업
  - MySQL 스크립트
- 소스 코드
  - F#
  - VimL
  - ActionScript
  - Assembly
  - Bash
  - Batchfile
  - C
  - Clojure
  - Cobol
  - CoffeeScript
  - CUDA
  - Erlang
  - Fortran
  - Go
  - Haskell
  - Java
  - JavaScript
  - LISP
  - Lua
  - Matlab
  - ObjectiveC
  - Perl
  - PHP
  - PowerShell
  - 처리 중
  - Python
  - R
  - Ruby
  - Scala
  - Swift
  - VHDL
- 웹 언어
  - CSS
  - HTML
  - XML

객체 위험 수준

Macie Classic가 모니터링하는 객체에는 위에 설명된 자동 분류 방법을 통해 각 콘텐츠 유형, 파일 확장명, 주제, regex 및 할당되는 SVM 아티팩트를 기반으로 다양한 위험 수준이 할당됩니다. 객체의 종합(최종) 위험 수준은 할당된 위험 수준의 가장 높은 값으로 설정됩니다.

S3 메타데이터의 보존 기간

Macie Classic는 S3 객체에 대한 메타데이터를 기본 1개월 동안 저장합니다. 이 기간을 최대 12개월까지 연장할 수 있습니다.

Amazon Macie Classic로 데이터 보호

Macie Classic를 통해 클라우드에 저장되어 있는 중요하고 민감한 비즈니스 데이터가 어떻게 사용되는지를 모니터링할 수 있습니다. Macie Classic는 인공 지능을 적용하여 기록 데이터의 액세스 패턴을 파악하고 사용자, 애플리케이션 및 서비스 계정의 활동을 자동으로 평가합니다. 이를 통해 무단 액세스를 감지하고 데이터 유출을 방지할 수 있습니다.

Macie Classic를 활성화하면 다음과 같은 자동화된 방법을 사용하여 데이터를 보호합니다.

주제

AWS CloudTrail 이벤트

Macie Classic는 인프라 내에서 발생할 수 있는 관리 이벤트(API 호출) 및 CloudTrail 로깅 데이터 일부를 분석하고 처리합니다. Macie Classic는 지원되는 각 CloudTrail 이벤트에 대해 위험 수준을 1부터 10까지 지정합니다.

기존의 이벤트를 수정하거나 새로운 CloudTrail 이벤트를 Macie Classic 관리형 목록에 추가할 수는 없습니다. 지원되는 CloudTrail 이벤트를 활성화하거나 비활성화하여, Macie Classic가 데이터 보안 프로세스에서 이벤트를 포함하거나 제외하도록 지정할 수 있습니다.

지원되는 CloudTrail 이벤트를 보거나 활성화하거나 비활성화하려면

1. Macie Classic 콘솔에서 설정 페이지로 이동합니다.
2. Protect data(데이터 보호) 섹션에서 AWS CloudTrail 이벤트를 선택합니다.
3. 세부 정보를 보려면 목록에서 이벤트를 선택합니다.

   세부 정보 페이지에서 이벤트를 활성화하거나 비활성화하려면, Enabled/Disabled(활성화됨/비활성화됨) 드롭다운 메뉴를 사용한 후 저장을 선택합니다.

AWS CloudTrail 오류

Macie Classic는 인프라 내에서 관리 이벤트(API 호출) 및 CloudTrail 로깅 데이터 일부로 인해 발생할 수 있는 오류를 분석하고 처리합니다. Macie Classic는 지원되는 각 CloudTrail 오류에 대해 위험 수준을 1부터 10까지 지정합니다. 여기서 10은 위험 수준이 가장 높고 1은 위험 수준이 가장 낮습니다.

기존의 오류를 수정하거나 새로운 CloudTrail 오류를 Macie Classic 관리형 목록에 추가할 수는 없습니다. 지원되는 CloudTrail 오류를 활성화하거나 비활성화하여, Macie Classic가 데이터 보안 프로세스에서 이벤트를 포함하거나 제외하도록 지정할 수 있습니다.

지원되는 CloudTrail 오류를 보거나 활성화하거나 비활성화하려면

1. Macie Classic 콘솔에서 설정 페이지로 이동합니다.
2. Protect data(데이터 보호) 섹션에서 AWS CloudTrail 오류를 선택합니다.
3. 세부 정보를 보려면 목록에서 오류를 선택합니다.

   세부 정보 페이지에서 오류를 활성화하거나 비활성화하려면, Enabled/Disabled(활성화됨/비활성화됨) 드롭다운 메뉴를 사용한 후 저장을 선택합니다.

Amazon Macie Classic가 모니터링하는 데이터 및 활동 보기

Macie Classic 대시보드는 Macie Classic에서 모니터링한 모든 데이터와 활동을 종합적으로 보여줍니다. 이 주제에서는 대시보드에서 다양한 관심 요소별로 분류된 모니터링 데이터를 보기 위해 사용할 수 있는 측정치와 보기에 대해 설명합니다. 각 측정치와 보기는 Macie Classic 콘솔의 Research(조사) 탭으로 이동하는 하나 이상의 방법을 제공합니다. 쿼리 구문 분석기에서 쿼리를 작성 및 실행하고 Macie Classic에서 모니터링하는 데이터와 활동을 심층적으로 연구 조사할 수 있습니다.

대시보드 측정치

다음 대시보드 측정치를 통해 여러 주요 관심 요소별로 분류된 모니터링 데이터를 확인할 수 있습니다.

- 고위험 S3 객체 – Macie Classic는 데이터 분류 (p. 21) 시, 모니터링한 각 데이터 객체에 위험 값을 지정합니다. 는 이러한 방식으로 비즈니스에 중요한 데이터를 상대적으로 덜 중요한 데이터와 식별하고 우선 순위를 지정합니다. 이 측정치를 통해 에서 모니터링하는 데이터 객체 중 위험 수준이 8~10인 모든 데이터 객체를 확인할 수 있습니다.
- 이벤트 발생 총수 – 데이터 보안 (p. 40)의 일환으로 Macie Classic는 인프라 내에서 발생하는 AWS CloudTrail 로깅 이벤트(API 호출)를 분석하고 처리합니다. 이 측정치는 Macie Classic를 활성화한 후 인프라 내에서 발생한 Macie Classic 모니터링 이벤트의 총수를 제공합니다.
- 사용자 세션 총수 – 사용자 세션은 CloudTrail 데이터를 5분간 집계합니다. 이 측정치는 Macie Classic를 활성화한 후 분석되고 처리된 CloudTrail 데이터의 모든 사용자 세션 총수를 제공합니다.

대시보드 보기

다음 절차에 따라 미리 정의된 Macie Classic 대시보드 보기를 사용하여 Macie Classic에서 모니터링하는 데이터 및 활동의 개별 하위 집합을 생성합니다.

Macie Classic 대시보드 보기를 사용하려면

1. 해당 아이콘을 선택한 후 다음 보기를 선택하여 Macie Classic에서 모니터링하는 데이터 및 활동의 다양한 하위 집합을 표시합니다.
   - 선택한 시간 범위의 S3 객체 (p. 42)
   - S3 객체 (p. 42)
   - PII별 S3 객체 (p. 43)
   - 버킷별 S3 퍼블릭 객체 (p. 43)
   - ACL별 S3 객체 (p. 43)
   - CloudTrail 이벤트 및 연결된 사용자 (p. 44)
   - CloudTrail 오류 및 연결된 사용자 (p. 45)
   - 활동 위치 (p. 46)
   - AWS CloudTrail 이벤트 (p. 46)
   - 활동 ISP (p. 46)

- AWS CloudTrail 사용자 자격 증명 유형 (p. 47)

2. 선택한 보기에 Minimum risk(최소 위험) 슬라이더가 있으면 슬라이더를 원하는 값으로 이동합니다. Minimum risk(최소 위험) 슬라이더를 사용하면 선택한 값과 같거나 더 큰 위험이 지정된 항목만 볼 수 있습니다.

선택한 시간 범위의 S3 객체

이 보기에는 모니터링한 S3 객체 중에서 다음 검색 조건과 일치하는 객체가 표시됩니다.

- 지정된 객체 주제 중 적어도 한 개 이상이 가장 자주 지정되는 상위 20개에 포함됩니다.
- 객체에 지정된 위험은 Minimum risk(최소 위험) 슬라이더에서 선택한 값과 같거나 큽니다.
- 객체가 다음 시간 범위 중 하나에서 마지막으로 수정되었습니다.
  - 지난 6개월
  - Macie Classic가 활성화된 날짜부터 오늘 기준으로 6개월 전 날짜 사이

이 보기에서 Research(조사) 탭으로 이동하려면 표시된 시간 범위 또는 주제를 나타내는 사각형을 선택(두 번 클릭)합니다. 선택한 항목은 자동으로 쿼리 구문 분석기의 Research(조사) 탭에 나타나는 쿼리로 변환됩니다.

다음 예제 절차를 참조하십시오.

1. Macie Classic 대시보드에서 S3 objects over selected time range(선택한 시간 범위의 S3 객체) 보기를 선택합니다.
2. Minimum risk(최소 위험) 슬라이더를 5로 설정합니다.
3. 생성된 그래프에서 Range: 0 - 6 months ago(범위: 0 - 6개월 전) 옆에 있는 사각형을 두 번 클릭합니다.

   그러면 쿼리 구문 분석기에 다음 쿼리가 자동으로 표시되는 Research(조사) 탭으로 리디렉션됩니다.

   ```
   themes:* AND dlp_risk:[5 TO *] AND @timestamp:[now-6M/M TO now]
   ```

   이 쿼리는 Macie Classic 모니터링 S3 객체 중에서, 가장 자주 지정된 상위 20개 주제 중 한 개 이상이 지정되고, 위험도 5 이상이 지정되었으며, 지난 6개월 동안 마지막으로 수정된 객체를 보기 위해 선택한 설정과 일치합니다. 이 쿼리의 결과도 표시됩니다. 그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

S3 객체

이 보기는 Macie Classic에서 모니터링하는 S3 객체의 전체 목록을 지정된 주제별로 분류하여 보여줍니다. 각 주제에 대해 Macie Classic에서 모니터링하는 S3 객체 총수에 대한 이 주제의 비율 및 이 주제가 지정된 S3 객체의 총수가 표시됩니다.

이 보기에서 Research(조사) 탭으로 이동하려면 표시된 테마 옆의 돋보기 아이콘을 선택하면 됩니다. 선택한 항목은 자동으로 쿼리 구문 분석기의 Research(조사) 탭에 나타나는 쿼리로 변환됩니다.

다음 예제 절차를 참조하십시오.

1. Macie Classic 대시보드에서 S3 객체 보기를 선택합니다.
2. 예를 들어 S3 객체의 생성 목록에서 json/aws_cloudtrail_logs 옆에 있는 돋보기 아이콘을 선택합니다.

   그러면 쿼리 구문 분석기에 다음 쿼리가 자동으로 표시되는 Research(조사) 탭으로 리디렉션됩니다.

   ```
   themes:"json/aws_cloudtrail_logs"
   ```

이 쿼리는 json/aws_cloudtrail_logs 주제가 지정된 Macie Classic 모니터링 S3 객체를 보기 위해 선택한 설정과 일치합니다. 이 쿼리의 결과도 표시됩니다. 그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

PII 별 S3 객체

이 보기는 다음 목록을 제공합니다.

- PII 우선 순위별 S3 객체

  PII 아티팩트를 포함하는 S3 객체의 전체 목록을 Macie Classic 지정 PII 우선 순위별로 분류하여 보여줍니다. 각 PII 우선 순위 수준에 대해, PII 정보를 포함하는 S3 객체의 총수 중 이 수준을 갖는 객체 수의 비율과, 이 PII 우선 순위 수준을 가진 S3 객체의 총수가 표시됩니다.
- PII 유형별 S3 객체

  PII 정보를 포함하는 S3 객체의 전체 목록을, PII 정보 유형별로 분류하여 보여 줍니다. 각 PII 정보 유형에 대해, PII 정보를 포함하는 S3 객체의 총수 중 이 유형의 PII 정보를 포함하는 객체 수의 비율과, 이 유형의 PII 정보를 포함하는 S3 객체의 총수가 표시됩니다.

PII 기반 객체 분류에 대한 자세한 내용은 Amazon Macie Classic를 사용하여 데이터 분류 (p. 21) 단원을 참조하십시오.

이 보기에서 Research(조사) 탭으로 이동하려면 표시된 PII 영향 또는 PII 유형 옆의 돋보기 아이콘을 선택하면 됩니다. 선택한 항목은 자동으로 쿼리 구문 분석기의 Research(조사) 탭에 나타나는 쿼리로 변환됩니다.

다음 예제 절차를 참조하십시오.

1. Macie Classic 대시보드에서 S3 objects by PII(PII 별 S3 객체) 보기를 선택합니다.
2. 예를 들어 PII 우선 순위가 낮은 S3 객체의 목록을 생성해 보겠습니다. S3 objects by PII priority(PII 우선 순위별 S3 객체) 목록에서 낮은 PII 우선 순위 옆에 있는 돋보기 아이콘을 선택합니다.

   그러면 쿼리 구문 분석기에 다음 쿼리가 자동으로 표시되는 Research(조사) 탭으로 리디렉션됩니다.

   ```
   pii_impact:"low"
   ```

   이 쿼리의 결과도 표시됩니다. 그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

버킷별 S3 퍼블릭 객체

퍼블릭 S3 객체가 저장된 버킷별로 그룹화된 퍼블릭 S3 객체의 전체 목록입니다. 각 버킷에 대해 Macie Classic에서 관리하는 S3 객체 총수에 대한 이 버킷의 객체 비율 및 이 버킷에 저장된 S3 객체의 총 수가 표시됩니다.

이 보기에서 Research(조사) 탭으로 이동하려면 표시된 버킷 옆의 돋보기 아이콘을 선택하면 됩니다. 선택한 항목은 자동으로 쿼리 구문 분석기의 Research(조사) 탭에 나타나는 쿼리로 변환됩니다.

ACL별 S3 객체

이 보기는 다음 목록을 제공합니다.

- ACL URI별 S3 객체

다음은 S3 객체에 연결된 ACL(액세스 제어 목록)에 표시되는 URI의 전체 목록입니다. 각 URI에 대해, ACL이 연결된 S3 객체의 총수 중 이 URI를 포함하는 ACL이 연결된 객체 수의 비율과, 이 URI를 포함하는 ACL이 연결된 S3 객체의 총수가 표시됩니다.

- ACL 표시 이름별 S3 객체

  S3 객체에 연결된 ACL에 표시되는 사용자 표시 이름의 전체 목록입니다. 각 표시 이름에 대해, ACL이 연결된 S3 객체의 총수 중 이 표시 이름을 포함하는 ACL이 연결된 객체 수의 비율과, 이 표시 이름을 포함하는 ACL이 연결된 S3 객체의 총수가 표시됩니다.

- ACL 권한별 S3 객체

  S3 객체에 연결된 ACL에 표시되는 액세스 권한의 전체 목록입니다. 각 권한 수준에 대해, ACL이 연결된 S3 객체의 총수 중 이 권한 수준을 포함하는 ACL이 연결된 객체 수의 비율과, 이 권한 수준을 포함하는 ACL이 연결된 S3 객체의 총수가 표시됩니다.

이 보기에서 Research(조사) 탭으로 이동하려면 표시된 URI, ACL 표시 이름, ACL 권한 옆의 돋보기 아이콘을 선택합니다. 선택한 항목은 Research(조사) 탭에서 쿼리 구문 분석기에 표시되는 쿼리로 자동 변환됩니다.

다음 예제 절차를 참조하십시오.

1. Macie Classic 대시보드에서 ACL별 S3 객체 보기를 선택합니다.
2. 예를 들어 전체 제어 권한이 포함된 ACL에 연결된 S3 객체의 목록을 생성해 보겠습니다. S3 objects by ACL permissions(ACL 권한별 S3 객체) 목록에서 FULL_CONTROL 권한 옆에 있는 돋보기 아이콘을 선택합니다.

   그러면 쿼리 구문 분석기에 다음 쿼리가 자동으로 표시되는 Research(조사) 탭으로 리디렉션됩니다.

   ```
   object_acl.Grants.Permission:"FULL_CONTROL"
   ```

   이 쿼리의 결과도 표시됩니다. 그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

CloudTrail 이벤트 및 연결된 사용자

이 보기는 다음 목록을 제공합니다.

- AWS CloudTrail 이벤트

  지난 60일간 발생한 CloudTrail 데이터 및 관리 이벤트의 상위 20개(배정된 위험 및 Minimum risk(최소 위험) 슬라이더로 선택한 값 기준)를 시각적으로 보여줍니다. 일별 또는 매주 옵션 버튼으로 그래프를 수정하여 일별 또는 매주 결과를 볼 수 있습니다.

  이 보기에서 Research(조사) 탭으로 이동하려면 자세히 조사할 특정 이벤트를 나타내는 사각형을 선택(두 번 클릭)합니다. 이벤트 옆에 있는 괄호 안의 수는 이 이벤트가 있는 사용자 세션의 수를 나타냅니다(CloudTrail 데이터 5분간 집계). Research(조사) 탭에서 선택 항목은 쿼리 구문 분석기에 나타나는 쿼리로 자동 변환됩니다.

- AWS CloudTrail 연동되어 있는 사용자

  지난 60일간 발생한 CloudTrail 데이터 및 관련 이벤트 상위 20개(배정된 위험 및 Minimum risk(최소 위험) 슬라이더로 선택한 값 기준)와 연결된 사용자를 시각적으로 보여줍니다. 일별 또는 매주 옵션 버튼으로 그래프를 수정하여 일별 또는 매주 결과를 볼 수 있습니다.

  이 보기에서 Research(조사) 탭으로 이동하려면 자세히 조사할 특정 오류를 나타내는 사각형을 선택(두 번 클릭)합니다. 사용자 이름 옆에 있는 괄호 안의 수는 이 사용자가 연결된 사용자 세션의 수를 나타냅니다

(CloudTrail 데이터 5분간 집계). Research(조사) 탭에서 선택 항목은 쿼리 구문 분석기에 나타나는 쿼리로 자동 변환됩니다.

다음 예제 절차를 참조하십시오.

1. Macie Classic 대시보드에서 CloudTrail events and associated users(이벤트 및 연결된 사용자) 보기를 선택합니다.
2. Minimum risk(최소 위험) 슬라이더를 1로 설정합니다.
3. 예를 들어 PutRestApi 이벤트가 있는 사용자 세션의 목록을 생성해 보겠습니다. PutRestApi 옆의 사각형을 두 번 클릭합니다.

   그러면 쿼리 구문 분석기에 다음 쿼리가 자동으로 표시되는 Research(조사) 탭으로 리디렉션됩니다.

   ```
   eventNameIsp.key.keyword:"PutRestApi" AND @timestamp:[now-60d TO now]
   ```

   이 쿼리의 결과도 표시됩니다. 그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

CloudTrail 오류 및 연결된 사용자

이 보기는 다음 목록을 제공합니다.

- AWS CloudTrail 오류

  지난 60일간 발생한 CloudTrail 오류 상위 20개(배정된 위험 및 Minimum risk(최소 위험) 슬라이더에서 선택한 값 기준)를 시각적으로 보여줍니다. 일별 또는 매주 옵션 버튼으로 그래프를 수정하여 일별 또는 매주 결과를 볼 수 있습니다.

  이 보기에서 Research(조사) 탭으로 이동하려면 자세히 조사할 특정 오류를 나타내는 사각형을 선택(두 번 클릭)합니다. 오류 이름 옆에 있는 괄호 안의 수는 이 오류가 있는 사용자 세션의 수를 나타냅니다(CloudTrail 데이터 5분간 집계). Research(조사) 탭에서 선택 항목은 쿼리 구문 분석기에 나타나는 쿼리로 자동 변환됩니다.
- AWS CloudTrail 연동되어 있는 사용자

  지난 60일간 발생한 CloudTrail 오류 중 상위 20개(배정된 위험 및 Minimum risk(최소 위험) 슬라이더에서 선택한 값 기준)와 연결된 사용자를 시각적으로 보여줍니다. 일별 또는 매주 옵션 버튼으로 그래프를 수정하여 일별 또는 매주 결과를 볼 수 있습니다.

  이 보기에서 Research(조사) 탭으로 이동하려면 자세히 조사할 특정 오류를 나타내는 사각형을 선택(두 번 클릭)합니다. 사용자 이름 옆에 있는 괄호 안의 수는 이 사용자가 연결된 사용자 세션의 수를 나타냅니다(CloudTrail 데이터 5분간 집계). Research(조사) 탭에서 선택 항목은 쿼리 구문 분석기에 나타나는 쿼리로 자동 변환됩니다.

다음 예제 절차를 참조하십시오.

1. Macie Classic 대시보드에서 CloudTrail events and associated users(오류 및 연결된 사용자) 보기를 선택합니다.
2. Minimum risk(최소 위험) 슬라이더를 1로 설정합니다.
3. 예를 들어 Client.InvalidPermission.NotFound 오류가 있는 사용자 세션의 목록을 생성해 보겠습니다. Client.InvalidPermission.NotFound 옆의 사각형을 두 번 클릭합니다.

   그러면 쿼리 구문 분석기에 다음 쿼리가 자동으로 표시되는 Research(조사) 탭으로 리디렉션됩니다.

```
eventNameErrorCode.secondary:"Client.InvalidPermission.NotFound" AND
@timestamp:[now-60d TO now]
```

이 쿼리의 결과도 표시됩니다. 그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

활동 위치

이 보기에는 선택한 기간 동안 Macie Classic에서 모니터링하는 활동의 위치를 보여 주는 맵이 포함되어 있습니다. 자세히 보려면 시간 기간 풀다운 메뉴(지난 15일, 지난 30일, 지난 90일 또는 작년)를 사용한 후 위치 고정 핀을 선택합니다.

이 보기에서 Research(조사) 탭으로 이동하려면 위치 고정 핀에 대한 도구 설명 창에 표시되는 이벤트 수를 선택합니다. Research(조사) 탭에서 선택 항목은 쿼리 구문 분석기에 나타나는 쿼리로 자동 변환됩니다. 예를 들어 시애틀에서 지난 15일간 발생한 사용자 세션의 목록을 표시하도록 다음 쿼리를 자동 생성할 수 있습니다.

```
geoLocation.key:"Seattle:UnitedStates:47.6145:-122.348" AND @timestamp:[now-15d
TO now]
```

그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

AWS CloudTrail 이벤트

이 보기는 Macie Classic에서 모니터링하는 CloudTrail 데이터 및 관리 이벤트의 전체 목록을 제공합니다. 각 이벤트에 대해, 이 이벤트가 있는 사용자 세션의 총수(CloudTrail 데이터 5분 집계)와, 사용자 세션 총수에 대한 해당 비율이 나타납니다.

이 보기에서 Research(조사) 탭으로 이동하려면 표시된 이벤트 옆의 돋보기 아이콘을 선택하면 됩니다. 선택한 항목은 자동으로 쿼리 구문 분석기의 Research(조사) 탭에 나타나는 쿼리로 변환됩니다. 예를 들어 AssumeRole 이벤트가 있는 모든 사용자 세션을 확인하도록 다음 쿼리를 자동 생성할 수 있습니다.

```
eventNameIsp.key.keyword:"AssumeRole"
```

그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

활동 ISP

이 보기는 Macie Classic에서 모니터링하는 CloudTrail 데이터 및 관리 이벤트의 전체 목록을 관련된 인터넷 서비스 제공업체(ISP)별로 분류하여 제공합니다. 각 ISP에 대해, 이 ISP가 있는 사용자 세션의 총수(CloudTrail 데이터 5분 집계)와, 사용자 세션 총수에 대한 해당 비율이 나타납니다.

이 보기에서 Research(조사) 탭으로 이동하려면 표시된 테마 옆의 돋보기 아이콘을 선택하면 됩니다. 선택한 항목은 자동으로 쿼리 구문 분석기의 Research(조사) 탭에 나타나는 쿼리로 변환됩니다. 예를 들어 Amazon과 관련된 모든 사용자 세션을 확인하도록 다음 쿼리를 자동 생성할 수 있습니다.

```
eventNameIsp.secondary.keyword:"Amazon"
```

그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

AWS CloudTrail 사용자 자격 증명 유형

이 보기는 Macie Classic에서 모니터링하는 CloudTrail 데이터 및 관리 이벤트의 전체 목록을 사용자 자격 증명 유형별로 분류하여 보여줍니다. 자세한 내용은 개념 및 용어 (p. 10)에서 사용자에 대한 정의를 참조하십시오. 각 사용자 자격 증명 유형에 대해, 이 사용자 자격 증명 유형이 있는 사용자 세션의 총수(CloudTrail 데이터 5분 집계)와, 사용자 세션 총수에 대한 해당 비율이 표시됩니다.

이 보기에서 Research(조사) 탭으로 이동하려면 표시된 테마 옆의 돋보기 아이콘을 선택하면 됩니다. 선택한 항목은 자동으로 쿼리 구문 분석기의 Research(조사) 탭에 나타나는 쿼리로 변환됩니다. 예를 들어 AssumedRole 사용자 자격 증명 유형에서 시작된 요청을 포함하는 모든 사용자 세션을 확인하도록 다음 쿼리를 자동 생성할 수 있습니다.

```
userIdentityType.key:"AssumedRole"
```

그 다음 Research(조사) 탭에서 쿼리 결과 컨트롤을 수정한 후 다시 쿼리를 실행하여 생성된 결과를 심층적으로 연구 조사할 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

Amazon Macie Classic 알림

알림은 Amazon Macie Classic에서 발견한 잠재적 보안 문제에 대한 알림입니다.

주제

기본 및 예측 Macie Classic 알림

Macie Classic는 다음 두 가지 유형의 알림을 생성합니다.

- 기본 알림 – Macie Classic가 수행하는 보안 검사에서 생성된 알림입니다. 에는 두 가지 유형의 기본 알림이 있습니다.
  - 수정할 수 없는 관리형(Macie Classic 큐레이트) 기본 알림. 기존 관리형 기본 알림을 활성화하거나 비활성화할 수 있습니다.

    Note

    설정 탭의 기본 알림 목록의 생성한 사람 필드에 있는 `Default` 값으로 관리형 기본 알림을 식별할 수 있습니다.
  - 해당 사양에 맞게 생성하여 수정할 수 있는 사용자 지정 기본 알림. 자세한 내용은 새/기존 사용자 지정 기본 알림 추가 및 편집 (p. 50) 단원을 참조하십시오.
- 예측 알림 – AWS 인프라 내에서 설정된 '정상' 활동 기준과 벗어나는 활동이 발생할 때 자동으로 생성되는 알림입니다. 즉, Macie Classic가 AWS 인프라 내에서 활동을 지속적으로 모니터링하고 정상 동작의 기준을 설정합니다. 그런 다음 정상 기준과의 차이를 검사하여 그러한 활동을 감지하면 자동으로 예측 알림을 생성합니다. 예를 들어 하루에 많은 양의 S3 객체를 업로드하거나 다운로드하는 사용자가 한 주 동안 한 개 내지 두 개의 S3 객체만 다운로드할 경우 알림이 발생할 수 있습니다.

Macie Classic의 알림 범주

Macie Classic의 기본 알림(관리형 및 사용자 지정)은 다음 범주 중 하나일 수 있습니다.

- 구성 규정 준수 – 규정 준수가 관리되는 콘텐츠, 정책, 구성 설정, 제어 및 데이터 영역 로깅, 패치 수준과 관련됩니다.
- 데이터 규정 준수 – 규정 준수 또는 보안 관리 콘텐츠(예: 개인 식별 정보(PII) 또는 액세스 자격 증명을 포함하는 콘텐츠)의 검색과 관련됩니다.
- 파일 호스팅 – 보안이 침해된 호스트 또는 스토리지 서비스를 통해 맬웨어, 안전하지 않은 소프트웨어 또는 공격자의 명령 및 제어 인프라를 호스팅하는 경우와 관련됩니다.
- 서비스 중단 – 환경의 리소스에 액세스하지 못하도록 할 수 있는 구성 변경입니다.

- 랜섬웨어 – 금액이 지불될 때까지 컴퓨터 시스템에 대한 액세스를 차단하기 위해 설계된 악의적인 소프트웨어 또는 활동입니다.
- 의심스러운 액세스 – 위험하고 비정상적인 IP 주소, 사용자 또는 시스템(예: 손상된 호스트를 통해 연결을 위장하는 공격자)에서 시도하는 리소스에 대한 액세스입니다.
- 자격 증명 열거 – 공격 또는 손상된 자격 증명의 초기 단계를 나타낼 수 있는 시스템에 대한 액세스 수준을 열거하는 일련의 API 호출 또는 액세스입니다.
- 권한 상승 – 애플리케이션 또는 사용자로부터 정상적으로 보호되는 리소스에 대한 상승된 액세스 권한을 얻기 위한 성공하거나 실패한 시도, 또는 장기간 시스템 또는 네트워크에 대한 액세스 권한을 얻기 위한 시도입니다.
- 익명 액세스 – 사용자의 실제 신원을 숨길 의도로 IP 주소, 사용자 또는 서비스에서 리소스에 대해 시도한 액세스입니다. 예를 들어 프록시 서버 사용, 가상 프라이빗 네트워크, Tor와 같은 익명 서비스 등이 포함됩니다.
- 개방 권한 – 지나치게 허용적일 수 있는(따라서 위험한) 액세스 제어 메커니즘으로 보호되는 민감한 리소스가 확인됩니다.
- 위치 비정상 – 민감한 데이터에 대한 비정상적이고 위험한 액세스 시도 위치입니다.
- 정보 손실 – 민감한 데이터에 대한 비정상적이고 위험한 액세스입니다.
- 자격 증명 손실 – 자격 증명이 손상될 가능성입니다.

특정 범주의 기존 알림 목록을 보려면 Macie Classic 콘솔의 알림 탭에 있는 범주 목록에서 해당 범주를 선택합니다.

Macie Classic에서 알림의 심각도 수준

각 Macie Classic 알림에는 심각도 수준이 할당되어 있습니다. 이는 분석에서 알림의 우선 순위를 지정할 필요성을 줄여 줍니다. 또한 알림이 잠재적인 문제를 강조 표시할 때 응답을 결정하는 데 도움이 될 수도 있습니다. 심각, 높음, 중간, 낮음 수준은 인프라 내 정보 기밀성, 무결성 및 가용성이 손상될 수 있는 보안 문제를 나타냅니다. 정보 수준은 Macie Classic에서 모니터링하는 인프라의 보안 구성 세부 정보를 강조 표시합니다. 다음은 각각의 수준에 대응하는 권장 방법입니다.

- 심각 – 인프라 내 정보 기밀성, 무결성 및 가용성이 손상될 수 있는 보안 문제를 설명합니다. 이 보안 문제는 긴급으로 처리하고 즉각적으로 해결하는 것이 좋습니다. 심각 심각도와 높음 심각도 간의 주요 차이점은 심각 심각도 알림은 다수의 리소스 또는 시스템의 보안 손상을 알리는 것일 수 있다는 점입니다. 높음 심각도 알림은 하나 이상의 리소스 또는 시스템의 보안 손상을 알립니다.
- 높음 – 인프라 내 정보 기밀성, 무결성 및 가용성이 손상될 수 있는 보안 문제를 설명합니다. 이 보안 문제는 긴급으로 처리하고 즉각적으로 해결하는 것이 좋습니다.
- 중간 – 인프라 내 정보 기밀성, 무결성 및 가용성이 손상될 수 있는 보안 문제를 설명합니다. 가능한 다음 기회(예: 다음 서비스 업데이트)에 이 문제를 해결하는 것이 좋습니다.
- 낮음 – 인프라 내 정보 기밀성, 무결성 및 가용성이 손상될 수 있는 보안 문제를 설명합니다. 이후 서비스 업데이트 시 이 문제를 해결하는 것이 좋습니다.
- 정보 – 인프라의 특정 보안 구성 세부 정보를 설명합니다. 비즈니스 및 조직 목표에 따라 이 정보를 기록해 두거나 이 정보를 사용하여 시스템과 리소스의 보안을 강화할 수 있습니다.

Macie Classic 알림 찾기 및 분석

다음 절차를 사용하여 기존 알림을 찾고 분석할 수 있습니다.

1. 생성된 알림(Active(활성) 및 Archived(보관된) 기본 또는 예측 알림)을 보려면 Macie Classic 콘솔에서 알림 페이지로 이동합니다.

   각 알림에는 다음 정보가 포함된 요약 섹션이 있습니다.

- 알림 심각도로, 이는 심각, 높음, 중간, 낮음 또는 정보일 수 있습니다. 자세한 내용은 Macie Classic에서 알림의 심각도 수준 (p. 49) 단원을 참조하십시오.
- 알림이 생성되었거나 마지막으로 업데이트된 시기를 나타내는 타임스탬프
- 알림 범주입니다. 자세한 내용은 Macie Classic의 알림 범주 (p. 48) 단원을 참조하십시오.
- 다음 중 하나:
  - 알림의 인덱스가 CloudTrail 데이터인 경우, Macie Classic가 알림을 생성하도록 유도한 활동에 관여한 사용자. 자세한 내용은 개념 및 용어 (p. 10)에서 Macie Classic의 맥락에서의 사용자 개념의 정의를 참조하십시오.
  - 알림의 인덱스가 S3 bucket properties(S3 버킷 속성) 또는 S3 objects(S3 객체)인 경우, Macie Classic가 알림을 생성하도록 유도한 활동에 관여한 객체와 관련되었거나 이 객체를 포함한 버킷 이름

    Important

    Macie Classic에서 각 알림은 다음 중 하나에 기반합니다.
    - 인덱스가 CloudTrail 데이터인 알림의 경우, Macie Classic가 알림을 생성하도록 유도한 활동을 수행한 단 한 명의 사용자, 즉 IAM 자격 증명.
    - 인덱스가 S3 bucket properties(S3 버킷 속성) 또는 S3 objects(S3 객체)인 알림의 경우, Macie Classic가 알림을 생성하도록 유도한 활동에 관여한 객체와 관련되었거나 이 객체를 포함한 단 하나의 S3 버킷
- 알림에 남겨진 의견 수.
- 총 결과 수로, 이는 알림의 정의에 포함된 쿼리와 일치하는 사용자 세션 목록, S3 버킷 목록, S3 객체 목록으로 구성될 수 있습니다. 자세한 내용은 새/기존 사용자 지정 기본 알림 추가 및 편집 (p. 50) 단원을 참조하십시오.
- 알림의 조회 수.
- 이 알림에 캡처된 활동이 발생한 AWS 리전.

2. 알림을 추가로 분석하려면 해당 알림을 선택하여 세부 정보 창을 확장합니다. 다음 정보가 알림 세부 정보에 포함되어 있습니다.

   - 설명 및 총 결과 수(알림의 정의에 포함된 쿼리와 일치하는 사용자 세션 수, S3 버킷 수 또는 S3 객체 수)가 포함된 알림 요약.
   - 알림 결과 목록. 이는 사용자 세션, S3 버킷 또는 S3 객체 목록으로, 이 알림의 정의에 지정된 인덱스에 따라 다릅니다. 자세한 내용은 새/기존 사용자 지정 기본 알림 추가 및 편집 (p. 50) 단원을 참조하십시오.
     - 인덱스로 CloudTrail data를 지정한 경우, 알림 세부 정보에는 특정 사용자의 알림 정의에 지정된 쿼리와 일치하는 사용자 세션 목록이 포함됩니다.
     - 인덱스로 S3 buckets을 지정한 경우, 알림 세부 정보에는 특정 사용자의 알림 정의에 지정된 쿼리와 일치하는 S3 버킷 목록이 포함됩니다.
     - 인덱스로 S3 objects(S3 객체)를 지정한 경우, 알림 세부 정보에는 특정 사용자의 알림 정의에 지정된 쿼리와 일치하는 S3 객체 목록이 포함됩니다.

   각 결과를 선택하여 이를 검토하고 해당하는 모든 필드를 볼 수 있습니다. 자세한 내용은 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58)의 AWS 데이터 조사, S3 버킷 속성 데이터 조사 또는 S3 객체 데이터 조사 단원을 참조하십시오.

   Research(조사) 돋보기 아이콘을 사용하여 Research(조사) 탭으로 이동하고 거기에서 특정 알림의 결과를 볼 수도 있습니다. Research(조사) 탭의 쿼리 구문 분석기는 이러한 결과를 생성하는 데 사용할 수 있는 쿼리로 미리 채워져 있습니다.

새/기존 사용자 지정 기본 알림 추가 및 편집

다음 절차를 사용하여 새/기존 사용자 지정 기본 알림을 추가 및 편집할 수 있습니다.

1. Macie Classic 콘솔에서 설정 페이지로 이동하고 기본 알림 아이콘을 선택합니다.
2. Basic alerts(기본 알림) 페이지에서 수정할 알림의 편집 아이콘을 선택하거나, 기본 알림을 추가하려면 새로 추가를 선택합니다.
3. 다음 중 하나를 수행합니다.

   - 기존 알림을 편집하려는 경우 알림 활성화 또는 비활성화 등의 변경을 한 후 저장을 선택합니다.
   - 새 알림을 추가하려는 경우 Basic alert definition(기본 알림 정의) 페이지에서 다음을 지정합니다.
     - 알림 제목 – 예: "S3 버킷에 모든 사람에게 읽기 권한을 부여하는 S3 버킷 정책 또는 S3 ACL이 있습니다."
     - 알림에 대한 설명 – 예: "S3 버킷의 S3 버킷 정책 또는 S3 ACL에는 모든 사용자에게 읽기 액세스 권한을 효과적으로 부여하는 절이 포함되어 있습니다. 이 S3 버킷과 그 데이터를 감사하고 이것이 의도한 바인지 확인하는 것이 좋습니다.
     - 알림 범주 – 자세한 내용은 Macie Classic의 알림 범주 (p. 48)를 참조하십시오.
     - 알림 쿼리 – Macie Classic에서 알림을 생성하도록 할 활동을 설명하는 쿼리입니다. 예: `s3_world_readability:"true"`. 이 쿼리는 모든 사용자에게 읽기 액세스 권한을 부여하는 S3 버킷의 S3 버킷 정책 또는 S3 ACL 정책을 찾습니다. 쿼리 생성에 대한 자세한 내용은 Macie Classic에서 쿼리 작성 (p. 58) 단원을 참조하십시오.

       Note

       기존 알림 옆의 돋보기 아이콘을 사용하여 Research(조사) 탭으로 이동할 수 있습니다. 그러면 이 알림의 쿼리가 Query Parser(쿼리 구문 분석기)에 자동으로 표시되고, 이 쿼리의 결과가 Research(조사) 탭에 표시됩니다.
     - 쿼리 인덱스 – 이는 Macie Classic가 이 알림에 지정된 쿼리를 실행할 데이터의 리포지토리입니다. CloudTrail 데이터, S3 버킷 또는 S3 객체 중에 선택할 수 있습니다. 사용자가 선택한 항목에 따라 알림에는 알림에서 정의한 활동과 일치하는 CloudTrail 사용자 세션(원시 CloudTrail 데이터의 5분 집계), S3 버킷 또는 S3 객체 목록이 포함됩니다.
     - 알림이 생성되기 전에 발생해야 하는 최소 활동 일치 수
     - 알림 심각도 – 자세한 내용은 Macie Classic에서 알림의 심각도 수준 (p. 49) 단원을 참조하십시오.
     - 선택한 알림 인덱스에 따라 알림이 정의하는 활동을 수행하도록 명시적으로 허용된 사용자 또는 버킷입니다. 사용자 또는 버킷을 명시적으로 허용하면 이 사용자 또는 버킷이 알림에서 정의한 활동에 관여할 때 Macie Classic는 이에 대한 알림을 생성하지 않습니다.

       Important

       Macie Classic에서 각 알림은 다음 중 하나에 기반합니다.

       - 인덱스가 CloudTrail 데이터인 알림의 경우, Macie Classic가 알림을 생성하도록 유도한 활동을 수행한 단 한 명의 사용자, 즉 IAM 자격 증명.
       - 인덱스가 S3 bucket properties(S3 버킷 속성) 또는 S3 objects(S3 객체)인 알림의 경우, Macie Classic가 알림을 생성하도록 유도한 활동에 관여한 객체와 관련되었거나 이 객체를 포함한 단 하나의 S3 버킷

     인덱스가 CloudTrail 데이터인 기본 알림에서 사용자를 명시적으로 허용할 때 `macieUniqueId`라는 특별한 Macie Classic 형식을 사용해야 합니다. 예를 들어 사용자의 자격 증명 유형에 따라 `123456789012:root`, `123456789012:user/Bob` 및 `123456789012:assumed-role/Accounting-Role/Mary` 등이 있습니다. 자세한 내용은 사용자 활동별로 Amazon Macie Classic–에서 모니터링하는 데이터 분석 (p. 54)에서 사용자의 정의를 참조하십시오.
     - 이 알림을 활성화할지 비활성화할지 지정

기존 알림 작업

다음 절차를 사용하여 알림을 보관 또는 보관 취소하거나 기존 기본 알림을 편집할 수 있습니다.

1. Macie Classic 콘솔에서 알림 페이지로 이동하고 보관, 보관 취소(보관된 알림의 경우) 또는 편집할 알림을 찾습니다.
2. 알림 요약 창에서 아래쪽 화살표를 선택한 후 다음 중 하나를 선택합니다.

   - 아카이브

     Note

     또는 Unarchive(보관 취소)(보관된 알림의 경우)
   - Edit basic alert(기본 알림 편집)

     Important

     이 옵션은 예측 알림에는 사용할 수 없습니다. AWS 인프라 내에서 설정된 정상 알림 기준을 벗어나는 활동을 기반으로 Macie Classic에서 자동으로 생성하는 예측 알림은 편집할 수 없습니다. 자세한 내용은 기본 및 예측 Macie Classic 알림 (p. 48) 단원을 참조하십시오.

보관 알림 그룹화

다음 절차를 사용하여 보관 알림을 그룹화할 수 있습니다.

1. Macie Classic 콘솔의 알림 페이지에서 Group Archive(보관 그룹화)를 선택합니다.
2. Group archive(보관 그룹화) 창에서 사용 가능한 설정을 사용하여 동시에 여러 알림을 보관하거나 보관 취소합니다.

기본 알림에 대해 사용자 또는 버킷을 명시적으로 허용

Macie Classic를 사용하여 관리형 및 사용자 지정 기본 알림 모두에 대해 사용자(알림의 인덱스가 CloudTrail 데이터인 경우) 및 버킷(알림의 인덱스가 S3 bucket properties(S3 버킷 속성) 또는 S3 objects(S3 객체)인 경우)을 명시적으로 허용할 수 있습니다. (예측 알림에 이 작업을 수행할 수 없습니다.)

다음 절차를 사용하여 Macie Classic가 특정 알림을 생성하도록 유도한 활동에 참여했거나 관여한 특정 사용자 또는 특정 버킷을 명시적으로 허용합니다.

Important

Macie Classic에서 각 알림은 다음 중 하나에 기반합니다.

- 인덱스가 CloudTrail 데이터인 알림의 경우, Macie Classic가 알림을 생성하도록 유도한 활동을 수행한 단 한 명의 사용자, 즉 IAM 자격 증명.
- 인덱스가 S3 bucket properties(S3 버킷 속성) 또는 S3 objects(S3 객체)인 알림의 경우, Macie Classic가 알림을 생성하도록 유도한 활동에 관여한 객체와 관련되었거나 이 객체를 포함한 단 하나의 S3 버킷

알림 탭을 사용하여 사용자 지정 기본 알림에 대해 사용자 또는 S3 버킷을 명시적으로 허용

1. Macie Classic 콘솔의 알림 탭에서 알림의 요약에 나열된 사용자 또는 S3 버킷을 명시적으로 허용할 사용자 지정 기본 알림을 찾습니다.
2. 알림 요약 창에서 아래쪽 화살표를 선택한 후 Whitelist user(사용자를 허용)(이 알림의 인덱스가 CloudTrail 데이터인 경우) 또는 Whitelist bucket(버킷을 허용)(이 알림의 인덱스가 S3 bucket properties(S3 버킷 속성) 또는 S3 objects(S3 객체)인 경우)을 선택합니다.

3. 표시되는 창에서 허용할 사용자 또는 버킷을 확인한 후(자동으로 미리 선택되어 있고 알림의 요약에 나열된 사용자 또는 버킷과 일치), 제출을 선택합니다.

다음 절차를 사용하여 사용자 지정 기본 알림에 대해 동시에 여러 사용자 또는 버킷을 명시적으로 허용할 수 있습니다.

설정 탭을 사용하여 사용자 지정 기본 알림에 대해 사용자 또는 S3 버킷을 명시적으로 허용

1. Macie Classic 콘솔의 설정 탭에서 기본 알림을 선택한 후 사용자 또는 S3 버킷을 명시적으로 허용할 사용자 지정 기본 알림을 찾습니다.
2. 알림 옆의 편집 아이콘을 선택합니다.
3. Whitelisted users(허용된 사용자)(이 알림의 인덱스가 CloudTrail 데이터인 경우) 또는 Whitelisted buckets(허용된 버킷)(이 알림의 인덱스가 S3 bucket properties(S3 버킷 속성) 또는 S3 objects(S3 객체)인 경우) 필드에서 허용할 사용자 또는 S3 버킷을 지정한 후 저장을 선택합니다.

   Note

   인덱스가 CloudTrail 데이터인 기본 알림에서 사용자를 명시적으로 허용할 때 `macieUniqueId`라는 특별한 Macie Classic 형식을 사용해야 합니다. 예를 들어 사용자의 자격 증명 유형에 따라 `123456789012:root`, `123456789012:user/Bob` 및 `123456789012:assumed-role/Accounting-Role/Mary` 등이 있습니다. 자세한 내용은 사용자 활동별로 Amazon Macie Classic–에서 모니터링하는 데이터 분석 (p. 54)에서 사용자 개념의 정의를 참조하십시오.

Macie Classic 관리형 기본 알림에 대해 사용자 또는 S3 버킷을 명시적으로 허용

1. Macie Classic 콘솔의 알림 탭에서 사용자 또는 S3 버킷을 명시적으로 허용할 Macie Classic 관리형 기본 알림을 찾습니다.
2. 알림 요약 창에서 아래쪽 화살표를 선택한 후 Whitelist user(사용자를 허용)(이 알림의 인덱스가 CloudTrail 데이터인 경우) 또는 Whitelist bucket(버킷을 허용)(이 알림의 인덱스가 S3 bucket properties(S3 버킷 속성) 또는 S3 objects(S3 객체)인 경우)을 선택합니다.
3. 표시되는 창에서 Clone and disable the default managed alert(기본 관리형 알림 복제 및 비활성화) 확인란을 선택한 후 제출을 선택합니다.
4. Macie Classic 콘솔의 설정 탭으로 이동합니다.

   이전 단계에서 작업한 원래 관리형 알림이 이제 비활성화됩니다. 또한 이 알림은 새 사용자 지정 기본 알림에 복제되었습니다. 예를 들어 원래 관리형 기본 알림 제목이 "S3 버킷에 모든 사람에게 읽기 권한을 부여하는 S3 버킷 정책 또는 S3 ACL이 있습니다"인 경우, 이 알림이 이제 비활성화되고 "S3 버킷에 모든 사람에게 읽기 권한을 부여하는 S3 버킷 정책 또는 S3 ACL이 있습니다(수정됨)"라는 (복제된) 사용자 지정 기본 알림이 생성됩니다.
5. 복제된 사용자 지정 기본 알림 옆의 편집 아이콘을 선택합니다.
6. Whitelisted users(허용된 사용자)(이 알림의 인덱스가 CloudTrail 데이터인 경우) 또는 Whitelisted buckets(허용된 버킷)(이 알림의 인덱스가 S3 bucket properties(S3 버킷 속성) 또는 S3 objects(S3 객체)인 경우) 필드에서 명시적으로 허용할 사용자 또는 S3 버킷을 지정한 후 저장을 선택합니다.

   Note

   인덱스가 CloudTrail 데이터인 기본 알림에서 사용자를 명시적으로 허용할 때 `macieUniqueId`라는 특별한 Macie Classic 형식을 사용해야 합니다. 예를 들어 사용자의 자격 증명 유형에 따라 `123456789012:root`, `123456789012:user/Bob` 및 `123456789012:assumed-role/Accounting-Role/Mary` 등이 있습니다. 자세한 내용은 사용자 활동별로 Amazon Macie Classic–에서 모니터링하는 데이터 분석 (p. 54)에서 사용자의 정의를 참조하십시오.

사용자 활동별로 Amazon Macie Classic–에서 모니터링하는 데이터 분석

The 사용자 탭을 통해 모니터링되는 모든 데이터와 활동을 종합적으로 파악할 수 있습니다. Macie Classic 특정 사용자 에 대해 를 선택합니다. 이 항목에서는 사용자 탭. 또한 이 탭에서 사용할 수 있는 보기는 다양한 이자 포인트로 그룹화된 선택한 사용자의 모니터링되는 데이터를 볼 수 있습니다. 각 보기는 Macie Classic 콘솔 연구 탭. 여기서 쿼리를 구사하고 쿼리할 수 있으며, 데이터 및 활동에 대한 심층적인 조사 연구를 수행할 수 있습니다. Macie Classic 를 선택합니다.

주제

Macie ClassicUniqueID

다음과 같은 맥락에서 Macie Classic사용자는 AWS Identity and Access Management (IAM) 특정 요청을 만드는 ID입니다. Macie Classic 사용 AWS CloudTrail `userIdentity` 요소를 사용하여 다음 사용자 유형을 구분합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

- 뿌리 – 요청이 AWS 계정 자격 증명.
- IAM 사용자 – 이 요청은 IAM 사용자.
- 추정 역할 – 요청을 통해 받은 임시 보안 자격 증명으로 요청이 이루어졌습니다. AWS Security Token Service (AWS STS)) `AssumeRole` API 작업.
- 연합 사용자 – 요청은 AWS STS `GetFederationToken` API 작업.
- AWS 계정 – 다른 계정으로 요청을 했습니다.
- AWS 서비스 – 이 요청은 AWS 서비스.

사용자를 Macie Classic 콘솔을 사용하여 Macie Classic 형식 `macieUniqueId`. 사용자를 지정하는 예는 사용자 탭, 연구 탭 및 명시적으로 허용하는 기본 경고의 사용자를 CloudTrail 데이터. The `macieUniqueId` 은(는) IAM `UserIdentity` 요소 및 `recipientAccountId`. 자세한 내용은 CloudTrail 사용자 ID 요소 그리고 `recipientAccountId` 에서 CloudTrail 내용 기록.

다음 예는 다양한 구조를 나열합니다. `macieUniqueId`, 사용자 ID 유형에 따라 에 따라

userIdentity	MacieUniqueId
`"userIdentity": { "type": "AssumedRole" "arn": "arn:aws:sts::123456789012:assumed-role/Accounting-Role/Mary" }`	`123456789012:assumed-role/accounting-role`
`"userIdentity": {`	`123456789012:user:bob`

userIdentity	MacieUniqueId

<pre>"type": "IAMUser",
"arn":
"arn:aws:iam::123456789012:user/
Bob",
"userName": "Bob"
}</pre>	

<pre>"userIdentity": {
"type": "FederatedUser"
"arn":
"arn:aws:sts::123456789012:federated-
user/Alice",
"principalId":
"123456789012:Alice",
}</pre>
	123456789012:federated-user:alice

<pre>"recipientAccountId":
"123456789012",
"userIdentity": {
"type": "AWSAccount"
"accountId":
"ANONYMOUS_PRINCIPAL",
}</pre>
	123456789012:ANONYMOUS_PRINCIPAL

<pre>"macieUniqueId":
"123456789012:root:root",
"userIdentity": {
"type": "Root"
"sourceARN":
"arn:aws:iam::123456789012:root",
}</pre>
	123456789012:root:root

<pre>"recipientAccountId":
"123456789012",
"userIdentity": {
"invokedBy":
"codepipeline.amazonaws.com",
"type": "AWSService"
}</pre>
	123456789012:codepipeline.amazonaws.com

<pre>"recipientAccoundId":
"123456789012",
"userIdentity": {
"type": "AWSAccount"
"accountId":
"987654321098",
"principalId":
"AIDABCDEFGHI123456XYZ",
}</pre>
	123456789012:AIDABCDEFGHI123456XYZ

Macie Classic의 사용자 범주

Macie Classic의 사용자는 활동(API 호출)에 따라 다음 범주로 그룹화됩니다.

- 플래티넘 – 이러한 IAM 사용자 또는 역할은 사용자 생성, 보안 그룹 수집 권한 부여 또는 정책 업데이트 등 관리자 또는 루트 사용자를 나타내는 고위험 API 호출의 이력을 갖습니다. 이러한 계정의 경우 계정 손상의 징후를 면밀하게 모니터링해야 합니다.
- 금 – 이러한 IAM 사용자 또는 역할은 인프라 관련 API 호출의 이력이 있습니다. 예를 들어 인스턴스 실행 또는 데이터 쓰기와 같은 Amazon Simple Storage Service (Amazon S3)). 이러한 계정의 경우 계정 손상의 징후를 면밀하게 모니터링해야 합니다.
- 실버 – 이러한 IAM 사용자 또는 역할은 다음과 같은 많은 양의 중간 위험 API 호출을 발행하는 이력이 있습니다. `Describe*` and `List*` 읽기 전용 액세스 요청 Amazon S3.
- 브론즈 – 이러한 IAM 사용자 또는 역할은 일반적으로 `Describe*` and `List*` API 호출 AWS 환경.

사용자 조사

이 절차에 따라 모니터링되는 모든 데이터와 활동의 종합적인 그림을 생성하십시오. Macie Classic 지정한 사용자.

1. 에서 Macie Classic 콘솔 사용자 탭, 검색 필드를 입력하고 Enter 키를 누릅니다.

   Note

   사용자를 지정할 때, Macie Classic 형식 마시니크예: `123456789012:root`, `123456789012:user/Bob`, 또는 `123456789012:assumed-role/Accounting-Role/Mary`사용자의 ID 유형에 따라. 자세한 내용은 사용자 에서 개념 및 용어 (p. 10).
2. 사용자 데이터가 생성되면 해당 아이콘을 선택하여 다음 보기 중 하나를 선택하여 이 사용자의 데이터 및 활동의 다양한 하위 집합을 표시합니다. Macie Classic 모니터:

   - 고위험 CloudTrail 이벤트 (p. 56)
   - 고위험 CloudTrail 오류 (p. 56)
   - 활동 위치 (p. 57)
   - CloudTrail .events (p. 57)
   - 활동 ISP (p. 57)
   - CloudTrail 사용자 ID 유형 (p. 57)
3. 선택한 보기에 Minimum risk(최소 위험) 슬라이더가 있으면 슬라이더를 원하는 값으로 이동합니다. The 최소 위험 슬라이더를 사용하면 지정된 위험이 선택한 값과 같고 선택한 값만 볼 수 있습니다.

고위험 CloudTrail 이벤트

이 보기는 상위 20의 시각적 표현을 제공합니다(할당된 위험에 따라, 그리고 최소 위험 슬라이더) CloudTrail 선택한 사용자 에 대해 지난 60일 동안 발생한 데이터 및 관리 이벤트입니다. 사용 가능한 매일 또는 매주 일일 또는 주간 결과를 보려면 그래프를 수정하기 위한 라디오 버튼.

이 보기에서 연구 탭을 클릭하고, 추가로 조사할 특정 이벤트를 나타내는 모든 사각형을 선택합니다. 이벤트 이름 옆의 괄호 안의 숫자는 사용자 세션 수(5분 집계)를 나타냅니다. CloudTrail 이 이벤트가 에 나와 있습니다. 에서 연구 탭에서는 선택 항목이 쿼리 파서 에 나타나는 쿼리로 자동 전송됩니다. 자세한 정보는 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

고위험 CloudTrail 오류

이 보기는 선택한 사용자에 대해 지난 60일간 발생한 CloudTrail 오류 중 상위 20개(배정된 위험 및 Minimum risk(최소 위험) 슬라이더로 선택한 값 기준)를 시각적으로 보여 줍니다. Daily(일별) 또는 Weekly(주별) 옵션 버튼으로 그래프를 수정하여 일별 또는 주별 결과를 볼 수 있습니다.

이 보기에서 연구 탭을 클릭하고, 추가로 조사하려는 특정 오류를 나타내는 모든 사각형을 선택합니다. 오류 이름 옆의 괄호 안의 숫자는 사용자 세션 수(5분 집계)를 나타냅니다. CloudTrail 이 오류가 에 나와 있습니

다. 에서 연구 탭에서는 선택 항목이 쿼리 파서 에 나타나는 쿼리로 자동 전송됩니다. 자세한 정보는 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

활동 위치

이 보기에는 지정된 사용자에 대해 선택한 기간 동안 Macie Classic에서 모니터링하는 활동의 위치를 보여주는 맵이 포함되어 있습니다. 세부 정보를 보려면 사용 가능한 기간 드롭다운(지난 15일, 지난 30일, 지난 90일 또는 작년)을 사용하고, 모든 위치 핀을 선택합니다.

이 보기에서 연구 탭, 위치 핀에 대한 도구 팁 창에 나타나는 이벤트 수를 선택합니다. 에서 연구 탭에서는 선택 항목이 쿼리 파서 에 나타나는 쿼리로 자동 전송됩니다. 자세한 정보는 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

CloudTrail 이벤트

이 보기는 CloudTrail 데이터 및 관리 이벤트 모니터링 Macie Classic 지정한 사용자. 각 이벤트에 대해 총 사용자 세션 수(5분 통합) CloudTrail (데이터) 이 이벤트가 존재하고 총 사용자 세션의 총 개수가 표시되는 백분율을 표시합니다.

이 보기에서 연구 tab, 표시된 이벤트 옆에 있는 보기 유리 아이콘을 선택합니다. 선택은 쿼리 파서에 있는 쿼리에 자동으로 변환됩니다. 연구 탭. 자세한 정보는 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

활동 ISP

이 보기는 CloudTrail 데이터 및 관리 이벤트 모니터링 Macie Classic지정된 사용자 에 대해 연결된 인터넷 서비스 공급자(isps)가 그룹화했습니다. 각 ISP에 대해 사용자 세션의 총 카운트는 CloudTrail (데이터) 이 ISP가 존재하고 총 사용자 세션의 총 개수가 표시되는 백분율을 표시합니다.

이 보기에서 연구 탭, 표시된 테마 옆에 있는 보기 유리 아이콘을 선택합니다. 선택은 쿼리 파서에 있는 쿼리에 자동으로 변환됩니다. 연구 탭. 자세한 정보는 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

CloudTrail 사용자 ID 유형

이 보기는 CloudTrail 데이터 및 관리 이벤트 모니터링 Macie Classic, 지정된 사용자의 사용자 ID 유형별로 그룹화됩니다. 자세한 내용은 정의를 참조하십시오. 사용자 에서 개념 및 용어 (p. 10). 사용자 ID 유형에 대해 사용자 세션의 총 카운트는 CloudTrail 데이터) 이 사용자 ID 유형이 나타나고 총 사용자 세션의 총 표시가 표시되는 백분율을 표시합니다.

이 보기에서 연구 탭, 표시된 테마 옆에 있는 보기 유리 아이콘을 선택합니다. 선택은 쿼리 파서에 있는 쿼리에 자동으로 변환됩니다. 연구 탭. 자세한 정보는 Amazon Macie Classic에서 모니터링한 데이터 조사 (p. 58) 단원을 참조하십시오.

Amazon Macie Classic에서 모니터링한 데이터 조사

Macie Classic 콘솔의 Research(조사) 탭을 사용하여 쿼리 구문 분석기에서 쿼리를 작성 및 실행하고 Macie Classic에서 모니터링하는 데이터와 활동을 심층적으로 연구 조사할 수 있습니다. 언제든지 Research(조사) 탭으로 이동하여 빈 구문 분석기에서 쿼리를 작성할 수 있습니다. 자세한 내용은 Macie Classic에서 쿼리 작성 (p. 58) 단원을 참조하십시오. Macie Classic 콘솔 전체의 다양한 위치에서 Research(조사) 탭으로 리디렉션될 수 있습니다. 예를 들어 대시보드 보기(Amazon Macie Classic가 모니터링하는 데이터 및 활동 보기 (p. 41) 참조) 또는 Basic alerts(기본 알림) 목록(Amazon Macie Classic 알림 (p. 48) 참조)에서 이 탭으로 리디렉션될 수 있습니다. 콘솔의 다른 위치에서 Research(조사) 탭으로 리디렉션되면 데이터 선택이 자동 생성되는 쿼리로 변환되어 쿼리 구문 분석기에 표시됩니다.

주제

Macie Classic에서 쿼리 작성

Macie Classic Research(조사) 탭의 쿼리 구문 분석기에서 쿼리를 작성할 수 있습니다. 이 쿼리 구문 분석기는 JavaCC를 사용하여 문자열을 Lucene 쿼리로 해석하는 Lexer입니다. 쿼리 구문에 대한 자세한 내용은 Apache Lucene - 쿼리 구문 분석기 구문을 참조하십시오.

다음은 일반 검색을 위한 예제 쿼리입니다.

- Amazon에서 소유한 IP 주소가 출처가 아닌 콘솔 로그인을 검색하려면: `eventNameIsp.compound:/ConsoleLogin:~(Amazon.*)/`
- 퍼블릭 S3 버킷 내 PII 아티팩트를 검색하려면: `filesystem_metadata.bucket:"my-public-bucket" AND (pii_impact:"moderate" OR pii_impact:"high")`

다음 표에 Macie Classic 날짜, 정수 및 문자열 필드 유형에 대한 쿼리 예제제가 나와 있습니다.

쿼리 예제: 날짜 필드 유형

예제 쿼리	설명	데이터 리포지토리
`objectsRead.key:* AND @timestamp:[2017-08-01 TO 2017-12-31]`	2017년 4분기에 읽은 S3 객체를 검색합니다.	CloudTrail 데이터
`sourceIPAddress.ip_intel.type:TOR AND @timestamp:[now-1M TO now]`	지난 달 동안 Tor 출구 노드의 Macie Classic 모니터링 데이터에 대한 익명 액세스를 검색합니다.	CloudTrail 데이터

예제 쿼리	설명	데이터 리포지토리
`macieUniqueId:"085924634393:assumed-role\:malicious_user" AND @timestamp: [2018-01-18 TO *]`	2018년 1월 18일부터 AWS 계정 ID 085924634393의 "malicious_user"라는 위임된 역할의 AWS 활동을 검색합니다.	CloudTrail 데이터

쿼리 예제: 정수 필드 유형

예제 쿼리	설명	데이터 리포지토리
`dlp_risk>6 AND filesystem_metadata.server_encryption:aws:kms`	`dlp_risk` 점수가 6보다 크고 서버 측 암호화가 있는 S3 객체를 검색합니다.	S3 객체
`filesystem_metadata.size: [10240 TO 1024000] AND pii_types:*`	크기가 10MB~1GB이고 잠재적 PII 데이터가 포함된 S3 객체를 검색합니다.	S3 객체

쿼리 예제: 문자열 필드 유형

예제 쿼리	설명	데이터 리포지토리
`dlp_risk>5 AND key: /.*contract.*|.*agreement.*|.*terms.*/ AND @timestamp:[now-1M/M TO now]`	키워드 "contract", "agreement" 또는 "terms"가 포함되어 있고, `dlp_risk` 점수가 5보다 크며, 한 달 미만 전에 마지막으로 수정된 S3 객체 키(이름)를 검색합니다. **Note** 일부 regex 쿼리는 검색 시간이 오래 걸릴 수 있습니다. 제한된 시간 동안 검색을 수행하는 것이 좋습니다.	S3 객체
`mimetypes:"Adobe PDF \(application/pdf\)" AND key: /~(.*\.pdf|.*\.PDF)/`	PDF 데이터를 포함하지만 파일 확장명이 PDF/pdf가 아닌 파일의 S3 객체를 검색합니다. **Note** 이 쿼리는 PDF 문서가 포함된 보관된 객체(zip,7z 등)도 반환합니다.	S3 객체
`acl.Grants.Grantee.DisplayName: admin`	ACL 피부여자 표시 이름이 "admin"으로 설정된 S3 버킷을 검색합니다.	S3 버킷 속성
`acl.Grants.Grantee.DisplayName: admi?`	ACL 피부여자 표시 이름이 "admi(?)"(와일드카드)("admin" 포	S3 버킷 속성

예제 쿼리	설명	데이터 리포지토리
	함)으로 설정된 S3 버킷을 검색합니다.	
`bucket: *test*`	키워드가 "test"인 S3 버킷을 검색합니다.	S3 버킷 속성

Research 필터

Macie Classic Research(조사) 탭에서 다음 필터를 검색에 적용할 수 있습니다.

데이터 인덱스

첫 번째 Research(조사) 탭 필터(드롭다운)는 CloudTrail data 기본값이 미리 선택되어 있으며 이를 통해 Macie Classic에서 검색하려는 인덱스(또는 데이터 리포지토리)를 지정할 수 있습니다. 이 필터에는 다음 옵션이 포함되어 있습니다.

- CloudTrail data – 원시 CloudTrail 데이터의 5분 집계 모음
- S3 버킷 속성 – Macie Classic에서 모니터링하는 S3 버킷에 대한 메타데이터 모음
- S3 객체 – Macie Classic에서 모니터링하는 버킷에 저장된 S3 객체에 대한 메타데이터 모음

표시할 결과 수

Research(조사) 탭의 다음 필터는 Top 10(상위 10) 기본값이 사전 선택되어 있으며, 이를 통해 처음 검색을 수행할 때 표시할 결과의 개수와 추가로 결과가 있을 때 표시할 추가 결과 수를 제어할 수 있습니다. 이 필터에는 다음 옵션이 포함되어 있습니다.

- 상위 10개
- 상위 50개
- 상위 100개
- 상위 500개

시간 범위

Research(조사) 탭의 세 번째 필터는 Past 30 days(지난 30일) 기본값이 사전 선택되어 있으며, 이를 통해 검색 결과를 표시하려는 시간 범위를 지정할 수 있습니다. 이 필터에는 다음 옵션이 포함되어 있습니다.

- 지난 7일
- 지난 30일
- 지난 90일
- 지난 365일
- 모두
- 사용자 지정 시간 범위

쿼리를 알림으로 저장

다음 절차를 사용하여 쿼리 구문 분석기에 표시된 쿼리를 기본 알림으로 저장할 수 있습니다. 기본 알림에 대한 자세한 내용은 Amazon Macie Classic 알림 (p. 48) 단원을 참조하십시오.

1. Macie Classic 콘솔의 Research(조사) 탭에서 쿼리 구문 분석기에 쿼리를 자동 생성하거나 작성합니다.
2. Save query as alert(쿼리를 알림으로 저장) 아이콘을 선택합니다.
3. Basic alert definition(기본 알림 정의) 양식을 작성한 후 저장을 선택합니다. 자세한 내용은 새/기존 사용자 지정 기본 알림 추가 및 편집 (p. 50) 단원을 참조하십시오.

즐겨 사용하는 쿼리

자주 실행하는 쿼리를 즐겨찾기로 표시하거나 즐겨 사용하는 쿼리 목록을 확인할 수 있습니다.

1. Macie Classic 콘솔의 Research(조사) 탭에서 쿼리 구문 분석기에 쿼리를 자동 생성하거나 작성합니다.
2. Mark query favorite(쿼리를 즐겨찾기로 표시) 아이콘을 선택합니다.
3. Favorite query definition(즐겨 사용하는 쿼리 정의) 양식에서 즐겨 사용하는 쿼리의 이름과 설정을 지정하고 저장을 선택합니다.
4. 즐겨 사용하는 쿼리 목록을 보려면 Macie Classic 콘솔의 Research(조사) 탭에서 Favorite queries(즐겨 사용하는 쿼리) 아이콘을 선택합니다.

조사 AWS CloudTrail 데이터

주제

분석 CloudTrail 검색 결과

다음 섹션에서는 사용자가 데이터를 사용할 때 표시되는 검색 결과의 요소에 대해 설명합니다. 연구 탭을 클릭하여 Macie Classic-모니터링됨 CloudTrail 데이터.

Research(조사) 탭에서 다음 단계를 수행하십시오.

1. 선택 CloudTrail 데이터 첫 번째 필터 드롭다운에서.
2. 이 예에서는 상위 10 두 번째 필터 드롭다운에서.
3. 이 예에서는 과거 90 세 번째 필터 드롭다운에서 일 수 있습니다.
4. 돋보기 아이콘 버튼을 선택하여 검색을 시작합니다.

검색을 수행하면 다음 항목이 생성됩니다.

- The 총 결과 수 고객과 CloudTrail 선택한 시간 범위에 대한 데이터 검색.
- The 그래픽 표현 of CloudTrail 선택한 시간 범위에 대한 데이터 검색 결과입니다.

  Note

  데이터세트가 매우 크고 매우 넓은 시간 범위를 지정하는 경우 데이터가 제대로 렌더링되지 않을 수 있으며 이 그래프는 검색 결과 중 하나로 표시되지 않을 수 있습니다.

  Important

  그래프를 사용하여 검색 범위를 좁히고 이전 단계에서 원래 선택 항목에서 생성된 결과의 하위 집합을 생성하는 쿼리를 생성하고 실행할 수 있습니다. 그래프의 결과를 두 번 클릭하면 선택 항목이 쿼리 파서에 자동으로 나타나는 새 쿼리로 변환됩니다. 연구 탭은 이 새 쿼리 결과를 사용하여 새로 고쳐집니다.

- 검색 결과 요약 – 검색에서 가장 중요한 필드 목록. 첫 번째 줄에는 각 필드에 대한 상위(또는 하단) 세 개의 값이 포함됩니다. 둘째 줄에는 각 필드의 상위(또는 하위) 10개 값이 들어 있습니다.

  Important

  검색 결과 요약의 필드를 사용하여 검색 범위를 좁히고 이전 단계에서 원래 선택 항목에서 생성된 결과의 하위 집합을 생성하는 쿼리를 생성하고 실행할 수 있습니다. 결과 첫째 줄이나 둘째 줄의 필드를 선택하고 확장된 결과 항목에서 결과 옆에 있는 돋보기 아이콘을 선택합니다. 그런 다음 선택 항목이 쿼리 파서 및 연구 탭은 이 새 쿼리 결과를 사용하여 새로 고쳐집니다.
- 목록 사용자 세션 (5분 응집체 CloudTrail 데이터)를 선택합니다. 확장하려면 사용자 세션을 선택하고 세부 정보를 봅니다.

CloudTrail 데이터 필드 및 샘플 쿼리

다음 표에는 귀하의 결과에 나타날 수 있는 필드가 포함되어 있습니다. CloudTrail 데이터 검색.

- 첫 번째 표에는 Macie Classic 추출물 CloudTrail. 이 필드에는 또한 Amazon S3 데이터 이벤트. 예를 들어, `accountId` 에서 Macie Classic 에 `userIdentity.accountId` 에서 CloudTrail, 그리고 `eventNameErrorCode.key` 에서 Macie Classic 에 `eventName` 에서 CloudTrail.
- 두 번째 표에는 다음 필드가 포함됩니다. Macie Classic 조사 결과를 기반으로 보안 인텔리전스 및 컨텍스트를 제공하는 데 CloudTrail 데이터. 예를 들어, `isp.key` 에 대한 API 요청이 있는 조직 또는 ISP에 대해 설명합니다. AWS 리소스 출시 `sourceIPAddress.ip_intel.type` 에서는 IP 주소 기록을 설명합니다. 예를 들어, API 요청을 시작하는 데 사용되는 TOR 종료 노드인지 여부 AWS 자원.

CloudTrail 데이터 필드 Macie Classic 추출물

Note

이 데이터 저장소의 경우CloudTrail)님, 검색은 항상 사용자 세션 목록을 반환합니다: 5분 간격으로 CloudTrail 데이터. 사용자 세션은 Macie Classic 고유 ID: 고유한 형식입니다. Macie Classic 사용자 지정 Macie Classic 고유 ID는 IAM `UserIdentity` 요소 및 `recipientAccountId`.

Macie Classic 필드 이름	CloudTrail 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`accountId`	`userIdentity.accountId`	: 문자열	AWS 계정 ID	특정 계정과 관련된 액세스 권한이 있는 사용자 세션을 검색합니다. • accountId:"110912345678"
`awsRegion.key`	`awsRegion`	: 문자열	The AWS 요청이 에 이루어진 지역.	사용자 세션 검색 AWS 지역별 API 호출: • awsRegion.key:"us-west-2" • awsRegion.key:"us-east-1"
`eventNameErrorCode.key`	`eventName`	: 문자열	오류 코드를 반환한(있는 경우) 이벤트 이름	• 사용자 세션 검색 AWS `ConsoleLogin` 전화: • eventNameErrorCode.key:Console • 사용자 세션 검색 AWS `Delete` 전화:

Macie Classic 필드 이름	CloudTrail 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
				• eventNameErrorCode.key:Delete*
eventNameErrorCode.secondary	errorCode	문자열	실패한 API 요청 후 반환된 오류 코드	사용자 세션 검색 AccessDenied 전체 오류 CloudTrail API 이벤트: • eventNameErrorCode.secondary:"Ac
eventSource.key	eventSource	: 문자열	요청이 이루어진 서비스입니다.	특정 API 호출을 사용하여 사용자 세션을 검색합니다. AWS 서비스: • eventSource.key:"s3.amazonaws.com • eventSource.key:"lambda.amazonaw
eventType.key	eventType	: 문자열	이벤트 레코드를 생성한 이벤트의 유형(예: AwsApiCall, AwsServiceEvent, 또는 AwsConsoleSignIn)).	사용자 세션 검색 AWS API 전화를 eventType: • eventType.key:"AwsApiCall"

Macie Classic 필드 이름	CloudTrail 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`objectsDeleted.key`	`resources[0].ARN`	문자열	S3 물체 아랍, S3 버킷 아암 또는 접두어의 일부인 `DeleteObject` 또는 `DeleteObjects` API 전화. Note S3 버킷을 삭제하는 경우 `DeleteBucket` and `DeleteObjects` 별칭. 다음 주소를 가진 집계 레코드 `DeleteObjects` 호출에 삭제된 버킷이나 접두어가 나열되어 있으며 삭제된 개별 개체가 모두 아닙니다. Note 실패한 물체 `DeleteObject` 또는 `DeleteObjects` API 호출은 또한 `objectsDeleted.key`. Note 검색 결과를 반환하는 사용자 세션 `objectsDeleted.key` 은(는) 최대 250 개의 레코드가 있습니다.	특정 버킷 또는 접두사에서 삭제된 객체를 모두 검색합니다. • objectsDeleted.key:/arn:aws:s3:::my_sensitive_bucket.*/ 모두 검색 `Delete` 또는 사용자 또는 역할로 이루어진 특정 물체의 요청. • objectsDeleted.key:"arn:aws:s3:::my-bucket-name/sshKeys" 둘 다 포함하는 사용자 세션을 검색합니다. `DeleteObject:AccessDenied` 특정 민감한 객체, 버킷 또는 접두사를 삭제하려고 시도하는 경우 • objectsDeleted.key:/arn:aws:s3:::my_sensitive_bucket.*/ AND eventNameErrorCode.compound:"De 외부에서 S3 개체를 삭제할 시도(또는 시도)가 모두 포함된 사용자 세션을 검색합니다. AWS 특정 민감한 객체, 버킷 또는 접두사를 삭제하려고 시도하는 경우: • objectsDeleted.key:/arn:aws:s3:::my_sensitive_bucket.*/ AND eventNameIsp.compound:/DeleteObject:~(Amazon.*)/ 알려진 중요한 객체의 익명 삭제 요청을 검색합니다. • objectsDeleted.key:/arn:aws:s3:::my_sensitive_bucket.*/ AND accountId:"ANONYMOUS_PRINCIPA

Macie Classic 필드 이름	CloudTrail 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`objectsRead.key`	`resources[0].ARN`	문자열	A3 객체 아랫 목록 `GetObject` API 전화. Note 실패한 물체 `GetObject` API 호출 은 또한 `objectsRead.key`. Note 검색 결과를 반환하는 사용자 세션 `objectsRead.key` 은(는) 최대 250 개의 레코드가 있습니다.	특정 버킷 또는 접두사에서 읽는 모든 객체가 있는 사용자 세션을 검색합니다. • objectsRead.key:/ arn:aws:s3:::my_sensitive_bucket.*/ 익명으로 또는 사용자나 역할이 수행한 특정 객체에 대한 액세스 시도를 모두 검색합니다. • objectsRead.key:"arn:aws:s3:::my-bucket-name/ sshKeys" 둘 다 포함하는 사용자 세션을 검색합니다. `GetObject:AccessDenied` 특정 민감한 객체, 버킷 또는 접두사를 읽으려는 시도. • objectsRead.key:/ arn:aws:s3:::my_sensitive_bucket.*/ AND eventNameErrorCode.compound:"Ge 외부에서 S3 객체를 읽는 시도(또는 시도)가 모두 포함된 사용자 세션을 검색합니다. AWS 특정 민감한 객체, 버킷 또는 접두사를 읽으려는 시도: • objectsRead.key:/ arn:aws:s3:::my_sensitive_bucket.*/ AND eventNameIsp.compound:/ GetObject:~(Amazon.*)/ 알려진 중요한 객체 또는 버킷에 대한 익명 읽기 액세스를 검색합니다. • objectsRead.key:/ arn:aws:s3:::my_sensitive_bucket.*/ AND accountId:"ANONYMOUS_PRINCIPA

Macie Classic 필드 이름	CloudTrail 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`objectsWritten.key`	`resources[0].ARN`	문자열	A3 객체 아랫 목록 `PutObject`, `CopyObject`, 또는 `CompleteMultipartUpload` API 전화. Note 실패한 물체 `PutObject` API 호출은 또한 `objectsWritten.key` Note 검색 결과를 반환하는 사용자 세션 `objectsWritten.key` 은(는) 최대 250 개의 레코드가 있습니다.	특정 버킷에 기록된 모든 객체가 있는 사용자 세션을 검색합니다. • objectsWritten.key:/arn:aws:s3:::my_bucket_name.*/ 익명으로 또는 사용자나 역할이 수행한 특정 객체에 대한 모든 쓰기 요청이 있는 사용자 세션을 검색합니다. • objectsWritten.key: "arn:aws:s3:::my-bucket-name/sshKeys" 둘 다 포함하는 사용자 세션을 검색합니다. `PutObject:AccessDenied` 특정 민감한 객체, 버킷 또는 접두사를 읽으려는 시도. • objectsWritten.key:/arn:aws:s3:::my_sensitive_bucket.*/ AND eventNameErrorCode.compound:"Pu 외부에서 S3 개체를 쓰기 위한 시도(또는 시도)가 모두 포함된 사용자 세션을 검색합니다. AWS 특정 민감한 객체, 버킷 또는 접두사를 쓰려고 시도하는 경우: • objectsWritten.key:/arn:aws:s3:::my_sensitive_bucket.*/ AND eventNameIsp.compound:/PutObject:~(Amazon.*)/ 중요한 객체 또는 버킷에 대한 익명 쓰기 요청을 검색합니다. • objectsWritten.key:/arn:aws:s3:::my_sensitive_bucket.*/ AND accountId:"ANONYMOUS_PRINCIPA

Macie Classic 필드 이름	CloudTrail 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`principalId`	`userIdentity.principalId`	문자열	The IAM 주요 ID. Note 추정된 역할이 요청을 할 경우 세션 이름은 주 ID 에서 제거됩니다.	특정 주 ID의 액세스 요청을 사용하여 사용자 세션을 검색합니다. • principalId:"AIDAIMABCKFJSKEOAK
`recipientAccountId`	`recipientAccountId`	문자열	수신된 계정 ID CloudTrail 이벤트.	특정 계정의 모든 활동을 검색합니다. • recipientAccountId:"110912345678" 특정 계정에 대한 액세스 요청을 검색합니다. • recipientAccountId:"110912345678" AND accountId: "ANONYMOUS_PRINCIPAL"
`resourceOwnerAccountIds.key`	`Resources[].accountId`	문자열	목록 AWS 리소스 소유자. 예는 S3 객체 또는 버킷을 소유한 계정 ID 목록입니다.	특정 계좌에서 소유한 리소스에 대한 활동을 검색합니다. • resourceOwnerAccountIds.key: "110951234567"
`resources.key`	`Resources[0].accountId`	문자열	리소스 목록(S3 버킷만 해당) CloudTrail 사용자 세션의 이벤트.	특정 S3 버킷에 대한 액세스 요청을 검색합니다. • resources.key: "arn:aws:s3:::my-bucket-name" 알려진 중요한 버킷에 대한 익명 액세스 요청을 검색합니다. • resources.key: "arn:aws:s3:::my-super-sensitive-bucket" AND accountId:"ANONYMOUS_PRINCIPA

Macie Classic 필드 이름	CloudTrail 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`sessionName.key`	`userIdentity.principalId`	문자열	위임된 역할 세션의 식별자. 추정된 역할이 요청하면 세션 이름이 원금 ID에서 제거되고 `sessionName.key`. 추정된 역할 이외의 ID가 요청되는 경우 `sessionName.key` 이(가) `None`.	세션 이름에서 추정된 역할 액세스 요청 검색 `examplesession-cli`: • sessionName.key:"examplesession-cli" 세션 이름에 EC2 인스턴스 ID 검색: • (sessionName.key:/i-[0-9a-f]{8}/ OR sessionName.key:/i-[0-9a-f]{17}/) 역할 액세스 요청을 검색하여 `sessionName` 이외 `examplesession-cli` regex negation 사용: • macieUniqueId: "123456789123:assumed-role:co-admin" AND sessionName.key:/~(examplesession-cli)/
`sourceARN`	`userIdentity.arn`	문자열	요청을 하는 데 사용된 ARN Note 추정된 역할이 이 요청을 하면 세션 이름은 `sourceARN`.	특정 ARN의 액세스 요청이 있는 사용자 세션을 검색합니다. • sourceARN:"arn:aws:iam::12345678 cluster-api"

Macie Classic 필드 이름	CloudTrail 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`sourceIPAddress.key`	`sourceIPAddress`	문자열	요청이 이루어진 IP 주소입니다. Note 검색 결과를 반환하는 사용자 세션 `sourceIPAddress.key` 은(는) 최대 한도 60,000의 기록을 갖습니다.	특정 소스 IP 주소의 액세스 요청이 있는 사용자 세션을 검색합니다. • sourceIPAddress.key:"194.68.22.22" 와일드카드를 사용하여 소스 IP 주소가 있는 사용자 세션을 검색합니다. • sourceIPAddress.key:194.68.*.* 10개 이상의 사용자 세션 검색 `RunInstances` 이벤트 및 `autoscaling` 그룹: • eventNameErrorCode.RunInstances_ AND NOT (sourceIPAddress.key:"autoscaling.a
`userAgent.key`	`userAgent`	: 문자열	만드는 데 사용되는 클라이언트 사용자 에이전트 문자열 목록 AWS API 전화.	API 호출을 사용하여 사용자 세션 검색 Amazon S3: • userAgent.key:"s3.amazonaws.com"
`userIdentityType.key`	`userIdentity.type`	문자열	의 ID 유형 목록 AWS.	계정의 루트 ID에 의해 액세스 요청을 사용하여 사용자 세션을 검색합니다. • userIdentityType.key:"Root"

필드 Macie Classic 생성

Note

이 데이터 저장소의 경우CloudTrail)님, 검색은 항상 사용자 세션 목록을 반환합니다: 5분 간격으로 CloudTrail 데이터. 사용자 세션은 Macie Classic 고유 ID: 고유한 형식입니다. Macie Classic 사용자 지정 The Macie Classic 고유 ID는 IAM `UserIdentity` 요소 및 `recipientAccountId`.

Macie Classic 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`@timestamp`	날짜	사용자 세션의 시작 시간	특정 시간 이후의 액세스 요청이 있는 사용자 세션을 검색합니다. • @timestamp:>"2017-02-06T23:01:08Z" • @timestamp:>"2017-02-06"

Macie Classic 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
			두 시간 간격 사이의 액세스 요청이 있는 사용자 세션을 검색합니다. • @timestamp:[2017-02-01 TO 2017-02-27]
countLongLifeAccessToken	정수	의 GetSessionToken 기본 43,200초보다 수명이 긴 API 호출.	기본 수명보다 긴 임시 액세스 토큰을 생성하는 사용자 또는 역할이 있는 사용자 세션을 검색합니다. • countLongLifeAccessToken:>0
dcObjectsDeleted	: 정수	사용자 세션에서 삭제된 고유한 S3 객체의 수 Note 검색 결과를 반환하는 사용자 세션 dcObjectsDeleted 은(는) 최대 한도가 250개 입니다.	25개 이상의 개체가 삭제된 사용자 세션을 검색하여 AWS 사용자 또는 역할: • dcObjectsDeleted:>25 • dcObjectsDeleted:[25 TO 100]
dcObjectsRead	: 정수	사용자 세션에서 읽은 고유한 S3 객체의 수 Note 검색 결과를 반환하는 사용자 세션 dcObjectsRead 은(는) 최대 한도가 250개 입니다.	25개 이상의 개별 객체가 있는 사용자 세션을 검색하여 AWS 사용자 또는 역할: • dcObjectsRead:>25 • dcObjectsRead:[25 TO 100] 사용자 세션 중에 익명의 보안 주체가 읽은 25개 이상의 고유 객체를 검색합니다. • dcObjectsRead:>25 AND accountId:"ANONYMOUS_PRINCIPAL"
dcObjectsWritten	: 정수	사용자 세션에 기록된 고유한 S3 객체의 수 Note 검색 결과를 반환하는 사용자 세션 dcObjectsWritten 은(는) 최대 한도가 250개 입니다.	25개 이상의 개별 객체를 사용하여 사용자 세션을 검색합니다. AWS 사용자 또는 역할: • dcObjectsWritten:>25 • dcObjectsWritten:[25 TO 100]

Macie Classic 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`distinctEventName`	정수	사용자 세션에서 발생한 고유한 이벤트 이름의 수	사용자 또는 역할에 의해 생성되는 25개 이상의 고유한 API 호출으로 사용자 세션을 검색합니다. • distinctEventName:>25 • distinctEventName:[25 TO 100]
`distinctSourceIPAddress`	정수	사용자 세션에서 발생한 활동에 관여한 고유한 소스 IP 주소의 수. 최대값은 60,000입니다.	사용자 또는 역할에 대해 관찰된 고유 소스 IP 주소가 25개 이상인 사용자 세션을 검색합니다. • distinctSourceIPAddress:>25 • distinctSourceIPAddress:[25 TO 100]
`distinctUserAgent`	정수	사용자 세션에서 발생한 활동에 관여한 고유한 클라이언트 사용자 에이전트의 수. 최대값은 60,000입니다.	사용자 또는 역할에 대해 관찰된 사용자 에이전트가 25개 이상인 사용자 세션을 검색합니다. • distinctUserAgent:>25 • distinctUserAgent:[25 TO 100]
`eventNameErrorCode.compound`	문자열	각각 요약한 화합물 집선 CloudTrail 이벤트 이름과 API 호출과 관련된 오류 코드와 함께 형식은 `EventName:ErrorCode` 가치를 창출하는 Macie Classic API 이벤트 이름을 오류 코드(있는 경우)와 연결하려면 반환됩니다. 이벤트에 대한 오류 코드가 없는 경우, 다음과 같이 값이 API 이름으로만 설정됩니다. `PutObject`.	사용자 세션 검색 `AccessDenied` 오류 발생 중 오류 발생 `GetObject` 전화: • eventNameErrorCode.compound:"GetObje 다음과 관련된 오류가 있는 사용자 세션을 검색합니다. `PutObject` 전화: • eventNameErrorCode.compound:/PutObject:.*/
`eventNameIsp.compound`	문자열	각각 요약한 화합물 집선 CloudTrail 이(가) 에서 생성했던 인터넷 서비스 공급자(ISP)와 함께 이벤트 이름을 입력합니다. 형식은 `EventName:ISP` 가치를 창출하는 Macie Classic API 작업 이름을 에서 시작한 ISP와 연결합니다.	사용자 세션 검색 `ConsoleLogin` 전화를 받지 않음AWS 정규식을 사용하는 IPS: • eventNameIsp.compound:/ConsoleLogin:~(Amazon.*)/

Macie Classic 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`eventNameIsp.secondary`	문자열	ISP는 AWS API 호출은 에서 이루어졌습니다.	사용자 세션 검색 AWS Amazon IP 주소 외부에서 API 호출 발생: • eventNameIsp.secondary:/~(Amazon.*)/
`macieUniqueId`	: 문자열	고유한 포맷 Macie Classic 사용자 지정 The Macie Classic 고유 ID는 IAM `UserIdentity` 요소 및 `recipientAccountId`. 자세한 내용은 Macie ClassicUniqueID (p. 54).	특정 역할, 사용자 또는 루트 계정의 액세스가 있는 사용자 세션을 검색합니다. • macieUniqueId:"123456789123:assumed-role:co-admin" • macieUniqueId:"123456789123:root:root" • macieUniqueId:"123456789123:user:exam
`sourceIPAddress.ip_intel.type`	문자열	소스 IP 주소와 연결된 IP 인텔리전스 범주	Tor 네트워크에서 시작한 모든 액세스가 있는 사용자 세션을 검색합니다. • sourceIPAddress.ip_intel.type:"TOR" 위협 인텔리전스 입력 피드에서 시작한 모든 액세스가 있는 사용자 세션을 검색합니다. • sourceIPAddress.ip_intel.type:*
`windowStartTimeInMillis`	정수	사용자 세션의 시작에 대한 epoch 타임스탬프	첫 번째 이벤트 시간이 지정된 epoch 시간보다 큰 사용자 세션을 검색합니다. • windowStartTimeInMillis:>1424476529
`windowEndTimeInMillis`	정수	사용자 세션의 종료에 대한 epoch 타임스탬프	마지막 이벤트 시간이 지정된 epoch 시간보다 작은 사용자 세션을 검색합니다. • windowEndTimeInMillis:<1424476987
`ipLocation.key`	: 문자열	IP 지리적 위치(도시 및 국가)가 Macie Classic 모니터.	사용자 세션 검색 AWS 로스앤젤레스에서 시작된 API 호출 이벤트: • ipLocation.key:"LosAngeles:UnitedStates" 사용자 세션 검색 AWS 미국 외 지역에서 발생한 API 호출 이벤트: • ipLocation.key:/~(.*UnitedStates)/

Macie Classic 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예제
`isp.key`	: 문자열	ISP는 AWS API 호출이 에서 생성되었습니다.	사용자 세션 검색 AWS Amazon IP 주소 외부에서 API 호출 발생: • isp.key:/~(Amazon.*)/

S3 버킷 속성 데이터 조사

주제

S3 버킷 속성 검색 결과 분석

다음 단원에서는 Research(조사) 탭을 사용하여 Macie Classic에서 모니터링한 S3 버킷 속성 데이터를 조사할 경우 표시되는 검색 결과 항목에 대해 설명합니다.

Research(조사) 탭에서 다음 단계를 수행하십시오.

1. 첫 번째 필터 드롭다운 목록에서 S3 bucket properties(S3 버킷 속성)를 선택합니다.
2. 이 예에서는 두 번째 필터 드롭다운 목록에서 Top 10(상위 10)을 선택합니다.
3. 이 예에서는 세 번째 필터 드롭다운 목록에서 Past 90(지난 90)일을 선택합니다.
4. 돋보기 아이콘 버튼을 선택하여 검색을 시작합니다.

검색 결과에는 다음 항목이 포함됩니다.

- 선택한 시간 범위 동안의 S3 버킷 속성 데이터 검색과 일치하는 총 결과 수.
- 선택한 시간 범위 동안의 S3 버킷 속성 데이터 검색 결과의 그래픽 보기.

  Note

  데이터 세트가 매우 크고 시간 범위를 매우 광범위하게 지정하면 데이터가 제대로 렌더링 되지 않아서 검색 결과 항목 중 하나로 이 그래프가 표시되지 않을 수 있습니다.

  Important

  그래프를 사용하여 검색 범위를 더 좁히고, 앞 단계의 원래 건택을 통해 생성된 결과의 부분 집합을 생성하는 쿼리를 생성하여 실행할 수 있습니다. 그래프 결과를 두 번 클릭하면 선택 항목이 새 쿼리로 변환되어 쿼리 구문 분석기에 자동으로 표시되고 Research(조사) 탭이 이 새 쿼리의 결과로 새로 고쳐집니다.
- 검색 결과 요약 – 검색에서 가장 유의미한 필드 목록입니다. 첫 줄에는 각 필드의 상위(또는 하위) 3개 값이 들어 있습니다. 둘째 줄에는 각 필드의 상위(또는 하위) 10개 값이 들어 있습니다.

  Important

  검색 결과 요약의 필드를 사용하여 검색 범위를 더 좁히고, 앞 단계의 원래 건택을 통해 생성된 결과의 부분 집합을 생성하는 쿼리를 생성하여 실행할 수 있습니다. 결과 첫째 줄이나 둘째 줄의 필드를 선택하고 확장된 결과 항목에서 결과 옆에 있는 돋보기 아이콘을 선택합니다. 선택 항목이 새 쿼리로 변환되어 쿼리 구문 분석기에 자동으로 표시되고 Research(조사) 탭이 이 새 쿼리의 결과로 새로 고쳐집니다.

- 검색 조건과 일치하는 S3 버킷의 목록. 버킷을 선택하여 확장하고 자세한 내용을 확인합니다.

S3 버킷 속성 데이터 필드 및 예제 쿼리

다음 표에는 S3 버킷 메타데이터 검색의 결과에 나타날 수 있는 필드가 나와 있습니다.

- 첫 번째 표에는 Macie Classic가 Amazon S3 버킷 API 메타데이터에서 추출하는 필드가 나와 있습니다. 예를 들어 Macie Classic의 `acl.Grants.Grantee.DisplayName`은 Amazon S3 `getbucket-acl` API 응답의 `Grants.Grantee.DisplayName`에 해당합니다.
- 두 번째 표에는 검사한 S3 버킷 메타데이터를 기반으로 추가 보안 인텔리전스 및 컨텍스트를 제공하도록 Macie Classic에서 생성하는 필드가 나와 있습니다. 예를 들어 `s3_world_readability`는 Amazon S3 ACL 및 버킷(IAM) 정책 평가의 일부로 모든 사람이 S3 버킷을 읽을 수 있는지 여부에 대한 true/false/unknown 상태 조건을 설명합니다.

Macie Classic에서 추출하는 S3 버킷 속성 데이터 필드

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
`acl.Grants.Grantee.DisplayName`	`Grantee.DisplayName`	`get-bucket-acl`	문자열	S3 버킷 ACL 피부여자의 표시 이름	John Doe가 액세스할 수 있는 S3 버킷을 검색합니다. • acl.Grants.Grantee.DisplayName
`acl.Grants.Grantee.ID`	`Grantee.ID`	`get-bucket-acl`	문자열	버킷 소유자에 의해 S3 버킷에 대한 액세스 권한을 부여받은 자격 증명의 ID	특정 정식 ID가 있는 S3 버킷의 피부여자를 검색합니다. • acl.Grants.Grantee.ID:"75bee88c
`acl.Grants.Grantee.Type`	`Grantee.Type`	`get-bucket-acl`	문자열	S3 버킷 ACL 피부여자의 사용자 유형	`Users`에게 부여된 S3 버킷을 모두 검색합니다. • acl.Grants.Grantee.Type:Canonic `Groups`에게 부여된 S3 버킷을 모두 검색합니다. • acl.Grants.Grantee.Type:Group
`acl.Grants.Grantee.URI`	`Grantee.URI`	`get-bucket-acl`	문자열	S3 버킷 ACL 피부여자의 URI 식별자	`LogDelivery` 그룹에 속한 S3 버킷을 제외한 S3 버킷을 모두 검색합니다. • acl.Grants.Grantee.URI:"http://acs.amazonaws.com/groups/s3/LogDelivery"

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
					전역 공유 권한이 있는 S3 버킷을 모두 검색합니다. • acl.Grants.Grantee.URI:"http://acs.amazonaws.com/groups/global/AllUsers" AWS 인증 사용자에게 액세스를 허용하는 S3 버킷을 모두 검색합니다. • acl.Grants.Grantee.URI:"http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
acl.Grants.Permission	Grants.Permission	get-bucket-acl	문자열	ACL 피부여자에게 할당된 권한 수준	모든 사람에게 모든 (읽기/쓰기) 액세스 권한을 부여하는 S3 버킷을 검색합니다. • acl.Grants.Grantee.URI:"http://acs.amazonaws.com/groups/global/AllUsers" AND acl.Grants.Permission:"FULL_CO
acl.Owner.DisplayName	Owner.DisplayName	get-bucket-acl	문자열	S3 버킷 소유자의 표시 이름	John Doe가 소유한 S3 버킷을 검색합니다. • acl.Owner.DisplayName: "JohnDoe"
acl.Owner.ID	Owner.ID	get-bucket-acl	문자열	S3 버킷 소유자의 ID	특정 S3 버킷 소유자의 ID를 검색합니다. • acl.Owner.ID:"73bee78dfe7b89b

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
location.LocationConstraint	LocationConstraint	bucket-location	문자열	S3 버킷이 있는 AWS 리전. Note 기본적으로 us-east-1 리전의 버킷에는 S3 API 호출에서 반환된 리전이 없습니다. Macie Classic는 검색을 용이하게 하기 위해 이를 "us-east-1" 문자열로 자동으로 채웁니다.	us-west-2 리전에서 호스팅되는 버킷을 검색합니다. • location.LocationConstraint:"us-west-2" us-east-1 리전에서 호스팅되는 버킷을 검색합니다. • location.LocationConstraint:"us-east-1"
logging.LoggingEnabled.TargetBucket	LoggingEnabled.TargetBucket	bucket-logging	문자열	로깅 상태를 반환 중인 버킷.	S3 객체 수준 로깅이 활성화된 버킷을 모두 검색합니다. • logging.LoggingEnabled.TargetB
logging.LoggingEnabled.TargetPrefix	LoggingEnabled.TargetPrefix	bucket-logging	문자열	특정 S3 버킷에 대한 객체 수준 로깅 데이터를 포함하는 구성된 접두사 또는 폴더	접두사 하위 문자열이 "Production"으로 구성된 버킷을 검색합니다. • logging.LoggingEnabled.TargetP "Production"
policy.Policy.Id	Policy.Id	get-bucket-policy	문자열	S3 버킷 정책의 ID	특정 ID가 있는 버킷 정책을 검색합니다. • policy.Policy.Id:"aaaa-bbbb-cccc-dddd"
policy.Policy.Statement.Action	Policy.Statement.Action	bucket-policy	문자열	S3 버킷 정책과 연결된 작업 목록(API 요청)	"put" 하위문자열 작업(`PutObject`, `PubBucketPolicy` 등)이 있는 버킷 정책을 검색합니다. • policy.Policy.Statement.Action: /s3:Put.*/

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
policy.Policy.Statement.Effect	Policy.Statement.Effect	GetBucketPolicy, bucket-policy	문자열	S3 버킷 정책과 연결된 정책 효과의 목록	명시적 "허용" 권한 부여가 있는 버킷 정책을 검색합니다. • policy.Policy.Statement.Effect: "Allow"
policy.Policy.Statement.NotPrincipal.AWS	Policy.Statement.NotPrincipal.AWS	GetBucketPolicy, bucket-policy	문자열	정책 규칙이 적용되는 보안 주체 예외	특정 계정이 NotPrincipal 섹션에 지정된 버킷 정책을 검색합니다. • policy.Policy.Statement.NotPrinci account-ID:role/ role-name"
policy.Policy.Statement.NotPrincipal.CanonicalUser	Policy.Statement.NotPrincipal.CanonicalUser	GetBucketPolicy, bucket-policy	문자열	정책의 NotPrincipal 표현식에 명시된 CanonicalUser.	특정 CanonicalUser가 NotPrincipal 섹션에 지정된 버킷 정책을 검색합니다. • policy.Policy.Statement.NotPrinci
policy.Policy.Statement.NotPrincipal.Federated	Policy.Statement.NotPrincipal.Federated	GetBucketPolicy, bucket-policy	문자열	정책의 NotPrincipal 표현식에 명시된 Federated 자격 증명.	특정 Federated 사용자가 NotPrincipal 섹션에 지정된 버킷 정책을 검색합니다. • policy.Policy.Statement.NotPrinci account-ID:saml- provider/provider- name"
policy.Policy.Statement.NotPrincipal.Service	Policy.Statement.NotPrincipal.Service	GetBucketPolicy, bucket-policy	문자열	정책의 NotPrincipal 표현식에 명시된 Service.	특정 Service가 NotPrincipal 섹션에 지정된 버킷 정책을 검색합니다. • policy.Policy.Statement.NotPrinci
policy.Policy.Statement.Principal.AWS	Policy.Statement.Principal.AWS	GetBucketPolicy, bucket-policy	문자열	AWS 표현식에 지정된 보안 주체.	모든 AWS 리소스에 대한 명시적 허용 권한 부여가 있는 버킷 정책을 검색합니다. • policy.Policy.Statement.Effect: Allow AND policy.Policy.Statement.Principal. \"*\"

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
policy.Policy.Statement.Principal.CanonicalUser	Policy.Statement.Principal.CanonicalUser	get-bucket-policy	문자열	정책의 보안 주체 표현식에 명시된 CanonicalUser	특정 CanonicalUser가 Principal 섹션에 지정된 버킷 정책을 검색합니다. • policy.Policy.Statement.Principal.
policy.Policy.Statement.Principal.Federated	Policy.Statement.Principal.Federated	get-bucket-policy	문자열	정책의 보안 주체 표현식에 명시된 Federated 자격 증명	특정 Federated 사용자가 NotPrincipal 섹션에 지정된 버킷 정책을 검색합니다. • policy.Policy.Statement.NotPrinci account-ID:saml-provider/provider-name"
policy.Policy.Statement.Principal.Service	Policy.Statement.Principal.Service	get-bucket-policy	문자열	정책의 보안 주체 표현식에 명시된 Service	특정 Service 사용자가 NotPrincipal 섹션에 지정된 버킷 정책을 검색합니다. • policy.Policy.Statement.NotPrinci
policy.Policy.Statement.Resource	Policy.Statement.Resource	get-bucket-policy	문자열	S3 버킷 정책이 적용되는 S3 리소스.	와일드카드를 포함하는 S3 버킷 정책을 검색합니다. • policy.Policy.Statement.Resource */
policy.Policy.Statement.Sid	Policy.Statement.Sid	get-bucket-policy	문자열	S3 버킷 정책의 Sid.	특정 Sid가 있는 버킷 정책을 검색합니다. • policy.Policy.Statement.Sid:"1"
policy.Policy.Version	Policy.Version	get-bucket-policy	문자열	S3 버킷 정책의 버전 번호	특정 버전이 있는 버킷 정책을 검색합니다. • policy.Policy.Statement.Version:"
tagging.TagSet.Key	TagSet.Key	get-bucket-tagging	문자열	S3 버킷 태그의 키	특정 태그 키가 있는 버킷 정책을 검색합니다. • tagging.TagSet.Key:"User"

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
tagging.TagSet.Value	TagSet.Value	get-bucket-tagging	문자열	S3 버킷 태그의 값	특정 태그 값이 있는 버킷 정책을 검색합니다. • tagging.TagSet.Value:"johndoe"
versioning.MFADelete	MFADelete	get-bucket-versioning	문자열	버킷 버전 구성의 MFADelete(활성화/비활성화) 상태	버킷 버전 관리 구성에서 MFADelete가 활성화된 버킷을 검색합니다. • versioning.MFADelete:"enabled"
website.ErrorDocument.Key	ErrorDocument.Key	get-bucket-website	문자열	S3 정적 웹 사이트 호스팅의 일부로 구성된 오류 문서	정적 웹 사이트 호스팅을 위해 구성되고 오류 페이지가 404.html로 리디렉션되는 S3 버킷을 검색합니다. • website.ErrorDocument.Key: "404.html"
website.IndexDocument.Suffix	IndexDocument.Suffix	get-bucket-website	문자열	웹 사이트의 루트나 임의의 하위 폴더로 요청이 전달되는 경우에 Amazon S3가 반환하는 웹 페이지의 접미사	S3 정적 웹 사이트 호스팅의 일부로 구성되고 인덱스 페이지가 index.html로 리디렉션되는 인덱스 문서를 검색합니다. • website.IndexDocument.Key: "index.html"
• lifecycle_configuration.Rules.Expiration.Date • lifecycle_configuration.Rules.Expiration.Days • lifecycle_configuration.Rules.AbortIncompleteMultipartUpload.DaysAfterInitiation • lifecycle_configuration.Rules.Filter.Prefix • lifecycle_configuration.Rules.Filter.Tag.Key • lifecycle_configuration.Rules.Filter.Tag.Value • lifecycle_configuration.Rules.ID • lifecycle_configuration.Rules.NoncurrentVersionExpiration.NoncurrentDays • lifecycle_configuration.Rules.NoncurrentVersionTransitions.NoncurrentDays • lifecycle_configuration.Rules.NoncurrentVersionTransitions.StorageClass • lifecycle_configuration.Rules.Prefix • lifecycle_configuration.Rules.Status • lifecycle_configuration.Rules.Transitions.Date • lifecycle_configuration.Rules.Transitions.Days • lifecycle_configuration.Rules.Transitions.StorageClass	• Rules.Expiration.Date • Rules.Expiration.Days • Rules.AbortIncompleteMultipartUpload.DaysAfterInitiation • Rules.Filter.Prefix • Rules.Filter.And.Tag.Key • Rules.Filter.And.Tag.Value • Rules.ID • Rules.NoncurrentVersionExpiration.NoncurrentDays • Rules.NoncurrentVersionTransitions.NoncurrentDays • Rules.NoncurrentVersionTransitions.StorageClass • Rules.Prefix • Rules.Status • Rules.Transitions.Date • Rules.Transitions.Days • Rules.Transitions.StorageClass	get-bucket-lifecycle-configuration	• 날짜 • 정수 • 정수 • 문자열 • 문자열 • 문자열 • 문자열 • 정수 • 정수 • 문자열 • 문자열 • 문자열 • 날짜 • 정수 • 문자열	자세한 내용은 GET 버킷 수명 주기를 참조하십시오.	만료가 3일 미만인 수명 주기 구성 규칙이 있는 S3 버킷을 검색합니다. • lifecycle_configuration.Rules.Exp

Macie Classic에서 생성하는 S3 버킷 속성 데이터 필드

Macie Classic 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예
`@timestamp`	날짜	Macie Classic가 버킷을 마지막으로 분석한 시점의 타임스탬프.	최근 24시간 동안 Macie Classic가 분석한 S3 버킷을 검색합니다. • @timestamp:[now-1d TO now]
`accountId`	문자열	S3 버킷 소유자의 계정 ID.	지정된 계정에 속하지 않는 S3 버킷을 검색합니다. • NOT accountId: 110912345678
`bucket`	문자열	S3 버킷 이름	특정 S3 버킷을 이름으로 검색합니다. • bucket: "MyBucket"
`s3_world_readability`	문자열	S3 버킷을 전역적으로 읽을 수 있는지 여부를 나타내는 값: `true`, `false` 또는 `unknown`. `unknown` 값은 Macie Classic가 S3 버킷을 전역적으로 읽을 수 있는지 여부를 확인할 수 없음을 나타냅니다.	Amazon S3 ACL 또는 버킷 (IAM) 정책이 전역적으로 읽을 수 있는 S3 버킷을 검색합니다. • s3_world_readability: "true"
`s3_world_writability`	문자열	S3 버킷을 전역적으로 쓸 수 있는지 여부를 나타내는 값: `true`, `false` 또는 `unknown`. `unknown` 값은 Macie Classic가 S3 버킷을 전역적으로 쓸 수 있는지 여부를 확인할 수 없음을 나타냅니다.	Amazon S3 ACL 또는 버킷 (IAM) 정책이 전역적으로 쓸 수 있는 S3 버킷을 검색합니다. • s3_world_writability: "true"

S3 객체 데이터 조사

주제

S3 객체 검색 결과 분석

다음 단원에서는 Research(조사) 탭을 사용하여 Macie Classic에서 모니터링한 S3 객체를 조사할 경우 표시되는 검색 결과 항목에 대해 설명합니다.

Research(조사) 탭에서 다음 단계를 수행하십시오.

1. 첫 번째 필터 풀다운 목록에서 S3 objects(S3 객체)를 선택합니다.
2. 이 예제 절차를 위해 두 번째 필터 드롭다운 목록에서 Top 10(상위 10)을 선택합니다.

3. 이 예제 절차를 위해 세 번째 필터 드롭다운 목록에서 Past 90(지난 90)일을 선택합니다.
4. 돋보기 아이콘 버튼을 선택하여 검색을 시작합니다.

검색 결과에는 다음 항목이 포함됩니다.

- 선택한 시간 범위 동안의 S3 객체 검색과 일치하는 총 결과 수.
- 선택한 시간 범위 동안의 S3 객체 검색 결과의 그래픽 보기.

  Note

  데이터 세트가 매우 크고 시간 범위를 매우 광범위하게 지정하면 데이터가 제대로 렌더링 되지 않아서 검색 결과 항목 중 하나로 이 그래프가 표시되지 않을 수 있습니다.

  Important

  그래프를 사용하여 검색 범위를 더 좁히고, 앞 단계의 원래 건택을 통해 생성된 결과의 부분 집합을 생성하는 쿼리를 생성하여 실행할 수 있습니다. 그래프 결과를 두 번 클릭하면 선택 항목이 새 쿼리로 변환되어 쿼리 구문 분석기에 자동으로 표시되고 Research(조사) 탭이 이 새 쿼리의 결과로 새로 고쳐집니다.
- 검색 결과 요약 – 검색에서 가장 유의미한 필드 목록입니다. 첫 줄에는 각 필드의 상위(또는 하위) 3개 값이 들어 있습니다. 둘째 줄에는 각 필드의 상위(또는 하위) 10개 값이 들어 있습니다.

  Important

  검색 결과 요약의 필드를 사용하여 검색 범위를 더 좁히고, 앞 단계의 원래 건택을 통해 생성된 결과의 부분 집합을 생성하는 쿼리를 생성하여 실행할 수 있습니다. 결과 첫째 줄이나 둘째 줄의 필드를 선택하고 확장된 결과 항목에서 결과 옆에 있는 돋보기 아이콘을 선택합니다. 선택 항목이 새 쿼리로 변환되어 쿼리 구문 분석기에 자동으로 표시되고 Research(조사) 탭이 이 새 쿼리의 결과로 새로 고쳐집니다.
- 검색 조건과 일치하는 S3 객체의 목록. S3 객체를 선택하여 확장하고 자세한 내용을 확인합니다.

S3 객체 데이터 필드 및 샘플 쿼리

다음 표에는 S3 객체 검색의 결과에 나타날 수 있는 필드가 나와 있습니다.

- 첫 번째 표에는 Macie Classic가 Amazon S3 객체 API 메타데이터에서 추출하는 필드가 나와 있습니다. 이러한 필드는 S3 API 메타데이터에도 있는 필드입니다. 예를 들어 `filesystem_metadata.ETag`는 체크섬 또는 콘텐츠의 해시를 기반으로 S3 객체의 엔터티 태그를 설명합니다.
- 두 번째 표에는 검사한 S3 객체 콘텐츠 및 메타데이터를 기반으로 추가 보안 인텔리전스 및 컨텍스트를 제공하도록 Macie Classic에서 생성하는 필드가 나와 있습니다. 예를 들어 `dlp_risk`는 S3 객체 메타데이터 및 콘텐츠의 위험 프로필을 설명하는 가중치 기반 점수를 나타내며, `pii_types`는 S3 객체에 포함된 개인 식별 정보를 설명합니다.

Macie Classic에서 추출하는 S3 객체 데이터 필드

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
`key`	`key`	`get-bucket (listObjects)`	문자열	S3 객체 키 경로	키워드 'myobject'가 있는 문서 이름을 검색합니다. • key: /.*myobject.*/

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
`accountId`	없음	없음	문자열	S3 객체를 소유하는 AWS 계정 ID.	특정 계정 ID가 소유한 S3 객체를 검색합니다. • accountId:"110912345678"
`filesystem_metadata.bucket`	없음	없음	문자열	S3 객체를 보유한 S3 버킷 이름	특정 S3 버킷의 S3 객체를 검색합니다. • filesystem_metadata.bucket:"MyB

`filesystem_metadata.first_prefix`	없음
	Note
	Macie Classic는 S3 키 필드를 사용하며 버킷 이름을 제외하고 첫 번째 '/' 앞의 모든 문자를 구문 분석합니다.
		`prefix`
		`bucket`
		(`listObjects`)
			문자열	S3 객체가 포함된 첫 번째 폴더의 이름	폴더 이름이 `AWSLogs`인 첫 번째 폴더 이름에 포함된 S3 객체를 검색합니다.
					• filesystem_metadata.first_prefix:"

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
filesystem_metadata.ETag	ETag	get-bucket (listBuckets)	문자열	RFC 2616에 정의된 엔터티 태그	특정 eTag를 검색합니다. • filesystem_metadata.ETag:""8b7
filesystem_metadata.bucket_owner.id	ID	get-bucket-acl	문자열	S3 버킷 소유자의 고유한 ID	특정 소유자 ID에 속한 S3 객체를 검색합니다. • filesystem_metadata.bucket_own "447fba12b05da301df359096ff54
filesystem_metadata.bucket_owner.name	Owner	get-bucket-acl	문자열	S3 버킷 소유자의 이름	John Doe가 소유한 S3 객체를 검색합니다. • filesystem_metadata.bucket_own "JohnDoe"
filesystem_metadata.last_modified	LastModified	get-bucket (list-buckets)	날짜	S3 객체가 마지막으로 수정된 시점의 타임스탬프	최근 24시간 동안 수정된 S3 객체를 검색합니다. • filesystem_metadata.last_modifie [now-1d TO now]
filesystem_metadata.server_encryption	ServerSideEncryption	get-object	문자열	S3 객체를 암호화하는 데 사용되는 서버 측 암호화	AES256 표준으로 암호화되지 않은 객체를 검색합니다. • NOT filesystem.metadata.server_encry "AES256"
filesystem_metadata.size	Size	get-bucket (list-buckets)	정수	S3 객체의 콘텐츠 크기(바이트)	1MB보다 큰 S3 객체를 검색합니다. • filesystem.metadata.size: > 1024000
filesystem_metadata.sse_kms_key_id	SSEKMSKeyId	get-object	문자열	S3 객체의 서버 측 암호화에 사용되는 마스터 키의 고유한 식별자(ARN)	지정된 키 ID로 암호화된 S3 객체를 모두 검색합니다. • filesystem_metadata.sse_kms_ke "arn:aws:kms:us-west-2: 110912345678:key/06f8b4fa-3f5 b60a56a9a1f2"

Macie Classic 필드 이름	Amazon S3 API 필드 이름	Amazon S3API 작업	Macie Classic 필드 유형	설명	검색 쿼리 예
`object_acl.Grants.Grantee.DisplayName`	Grants.Grantee.DisplayName	`get-object-acl`	문자열	ACL 피부여자 이름	John Doe에게 부여된 S3 객체 ACL 권한을 검색합니다. • object_acl.Grants.Grantee.Displa "JohnDoe"
`object_acl.Grants.Grantee.ID`	Grants.Grantee.ID	`get-object-acl`	문자열	ACL 피부여자의 고유한 ID	특정 피부여자 ID가 있는 S3 객체 ACL 권한을 검색합니다. • object_acl.Grants.Grantee.ID:"75
`object_acl.Grants.Grantee.Type`	Grants.Grantee.Type	`get-object-acl`	문자열	ACL 피부여자의 유형입니다(예: `CanonicalUser` 또는 `Group`).	사용자 또는 그룹에 부여된 S3 객체 ACL을 모두 검색합니다. • object_acl.Grants.Grantee.Type: • object_acl.Grants.Grantee.Type:
`object_acl.Grants.Grantee.URI`	Grants.Grantee.URI	`get-object-acl`	문자열	ACL 피부여자 URI	`AllUsers` 권한 부여가 있는 S3 객체 ACL을 검색합니다. • object_acl.Grants.Grantee.URI: "http://acs.amazonaws.com/groups/global/AllUsers"
`object_acl.Grants.Permission`	Grants.Permission	`get-object-acl`	문자열	ACL 피부여자 권한	모든 제어 권한을 부여하는 S3 객체 ACL을 검색합니다. • object_acl.Grants.Permission: "FULL_CONTROL"
`object_acl.Owner.DisplayName`	Owner.DisplayName	`get-object-acl`	문자열	ACL 소유자 이름	John Doe가 소유한 S3 객체를 검색합니다. • object_acl.Owner.DisplayName: "JohnDoe"
`object_acl.Owner.ID`	Owner.ID	`get-object-acl`	문자열	ACL 소유자 ID	특정 소유자 ID에 속한 S3 객체를 검색합니다. • object_acl.Owner.ID: "447fba12b05da301df359096ff54

Macie Classic에서 생성하는 S3 객체 데이터 필드

Macie Classic 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예
`@timestamp`	날짜	S3 객체가 마지막으로 수정된 시점의 타임스탬프	최근 24시간 동안 Macie Classic가 분류한 S3 객체를 검색합니다. • @timestamp:[now-1d TO now]
`content_type`	문자열	S3 객체 콘텐츠 및 인코딩 유형 **Note** 이 값은 Macie Classic 콘솔의 설정 페이지에서 Content types(콘텐츠 유형) 섹션에 있는 특정 콘텐츠 유형의 이름 필드에서 찾을 수 있습니다.	하드 코딩된 AWS 자격 증명이 포함된 java 소스 코드를 검색합니다. • content_type:"text/x-java-source" AND regex_themes: "aws_access_key" • content_type:"text/x-java-source" AND regex_themes: "aws_access_key"
`dlp_risk`	정수	Macie Classic가 모니터링하는 객체에는 자동 분류 방법을 통해 각 콘텐츠 유형, 파일 확장명, 주제, regex 및 할당되는 SVM 아티팩트를 기반으로 위험 수준이 할당됩니다. 객체의 종합(최종) 위험 수준은 할당된 위험 수준(`dlp_risk`)의 가장 높은 값으로 설정됩니다. **Note** 지원되는 각 데이터 분류자의 위험 수준은 Macie Classic 콘솔의 설정 페이지에서 찾을 수 있습니다.	종합(최종) 위험 수준이 5 이상인 전역적으로 액세스할 수 있는 (읽기 또는 쓰기) 객체를 검색합니다. • object_acl.Grants.Grantee.URI: "http://acs.amazonaws.com/groups/global/AllUsers" AND dlp_risk>5
`encoding`	문자열	S3 객체 콘텐츠를 분석할 때 식별되는 인코딩 체계	유니코드 텍스트 문서를 검색합니다. • encoding: "utf-8"
`filetype_risk`	정수	파일 확장명을 기반으로 S3 객체에 할당되는 위험 수준 **Note** 지원되는 각 데이터 분류자의 위험 수준은 Macie Classic 콘솔의 설정 페이지에서 찾을 수 있습니다.	할당된 파일 확장명 위험이 6보다 큰 문서를 검색합니다. • filetype_risk: > 6

Macie Classic 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예
`filetypes`	문자열	확장명에 기반한 파일 유형 **Note** 이 값은 Macie Classic 콘솔의 설정 페이지의 File extensions(파일 확장명) 섹션에 있는 특정 파일 유형의 이름 및 설명 필드에서 찾을 수 있습니다.	확장명이 .pdf인 파일을 검색합니다. • filetypes: "Adobe PDF (.pdf)"
`keyword_themes`	문자열	S3 객체에 할당된 주제. 지원되는 주제는 Macie Classic 콘솔의 설정 페이지에서 찾을 수 있습니다.	사회 보장과 관련된 콘텐츠가 포함된 S3 객체를 검색합니다. • keyword_themes: "Social Security Keywords"
`language_code`	문자열	S3 객체의 콘텐츠를 분석할 때 찾을 수 있는 언어 코드	독일어 키워드가 포함된 S3 객체를 검색합니다. • language_code: "de"
`last_crawl_time`	날짜	Macie Classic가 S3 객체를 마지막으로 분석한 시점의 타임스탬프.	최근 24시간 동안 Macie Classic가 분석한 S3 객체를 검색합니다. • last_crawl_time: [now-1d/d TO now]
`mimetype_risk`	정수	S3 객체 콘텐츠/MIME 유형에 기반한 위험 수준.	위험도가 높은 콘텐츠와 관련된 MIME 유형이 포함된 S3 객체를 검색합니다. • mimetype_risk: > 5
`mimetypes`	문자열	S3 객체의 MIME 유형입니다.	AWS 보안 키가 포함된 일반 텍스트 문서를 검색합니다. • mimetypes: "Plain Text (text/plain)" AND themes: aws_secret_key
`pii_impact`	문자열	S3 객체의 Macie Classic 지정 PII 심각도 영향.	매우 중요한 개인 식별 정보가 포함된 S3 객체를 검색합니다. • pii_impact: "high"
`pii_types`	문자열	S3 객체에서 찾을 수 있는 특정 유형의 PII	이메일이 포함된 S3 객체를 검색합니다. • pii_types: "email"

Macie Classic 필드 이름	Macie Classic 필드 유형	설명	검색 쿼리 예
`regex_risk`	정수	S3 객체의 Macie Classic 지정 regex에 기반한 위험 수준.	regex 기반 위험 수준이 5보다 큰 S3 객체를 검색합니다. • regex_risk: > 5
`regex_themes`	문자열	S3 객체의 regex 주제	RSA 프라이빗 키가 포함된 S3 객체를 검색합니다. • regex_themes: "RSA Private Key"
`theme_risk`	문자열	S3 객체의 Macie Classic 지정 테마에 기반한 위험 수준.	주제 기반 위험 수준이 5보다 큰 S3 객체를 검색합니다. • theme_risk: > 5
`themes`	문자열	S3 객체의 결합 주제	RSA 프라이빗 키가 포함된 S3 객체를 검색합니다. • themes: "RSA Private Key"

Amazon Macie Classic 비활성화 및 수집한 메타데이터 삭제

Amazon Macie Classic 계정을 비활성화하기 전에 선택적으로 기존 데이터 분류 결과를 S3 버킷으로 내보낼 수 있습니다. 새로운 Amazon Macie로 이전하는 경우 Macie Classic을 비활성화하고 새로운 Amazon Macie로 이전하기 전에 이 작업을 수행하는 것이 좋습니다. 자세한 방법은 새로운 Amazon Macie로 이전 (p. 3) 단원을 참조하십시오.

이 항목에서는 데이터 분류 결과를 내보내지 않고 Macie Classic을 비활성화하는 방법을 설명합니다.

> **Important**
>
> 마스터 계정만 Macie Classic을 비활성화할 수 있습니다. 멤버 계정에 대해 Macie Classic를 비활성화하려면 먼저 마스터 계정에서 해당 멤버 계정을 연결 해제해야 합니다.

Macie Classic를 비활성화하면 마스터 계정 및 모든 멤버 계정에서 리소스에 더 이상 액세스할 수 없습니다. 또한 Macie Classic을 다시 활성화할 수 없습니다. Macie Classic 계정을 비활성화한 후 다시 Amazon Macie 사용을 시작하려면 계정에 대해 새 Amazon Macie를 활성화합니다. 이를 위한 자세한 방법은 Amazon Macie User Guide 단원을 참조하십시오.

Macie Classic를 비활성화하면 마스터 계정 및 모든 멤버 계정에서 리소스 처리가 중지됩니다. Macie Classic가 비활성화되면 Macie Classic가 마스터 및 멤버 계정에서 데이터를 모니터링하는 동안 수집한 메타데이터가 삭제됩니다. Macie Classic을 비활성화한 후 90일 이내에 이 메타데이터가 모두 Macie Classic 시스템 백업에서 만료됩니다.

> **Important**
>
> Macie Classic를 비활성화해도 AWS 계정 내의 다른 데이터가 삭제된다는 메시지는 표시되지 않습니다. Macie Classic를 비활성화하면 Macie Classic가 계정을 모니터링하는 동안 수집한 메타데이터만 삭제됩니다.

1. https://console.aws.amazon.com/macie/에서 Amazon Macie 콘솔을 엽니다.
2. 탐색 창에서 Macie Classic을 선택합니다.
3. 로그인한 이름 옆의 아래쪽 화살표를 선택하여 Macie Classic 일반 설정 페이지로 이동합니다.
4. Macie Classic 일반 설정 페이지에서 다음 확인란을 검토하고 선택합니다.
   - I understand that if I disable Macie Classic, the service will no longer have access to the resources in the master account and all member accounts. You must add member accounts again if you decide to re-enable Macie Classic.
   - I understand that if I disable Macie Classic, the service will stop processing the resources in the master account and all member accounts. All metadata that Macie Classic collected while monitoring the data in these accounts will be deleted.
5. Amazon Macie Classic 비활성화를 선택합니다.

Amazon CloudWatch Events로 Amazon Macie Classic 알림 모니터링

Amazon Macie Classic에서는 Macie Classic 알림이 변경되면 CloudWatch 이벤트를 기반으로 알림을 보냅니다. 여기에는 새롭게 생성된 알림과 기존 알림에 대한 업데이트가 포함됩니다. 예측 알림 및 기본 알림을 비롯한 모든 알림 유형(관리형 및 사용자 지정)에 대해 알림이 전송됩니다. 알림 유형에 대한 자세한 내용은 Amazon Macie Classic 알림 (p. 48) 단원을 참조하십시오.

Macie Classic는 마스터 및 멤버 Macie Classic 계정 모두에서 생성된 알림에 대해 CloudWatch 이벤트를 기반으로 알림을 보냅니다. 그러나 마스터 Macie Classic 계정만 CloudWatch 이벤트에서 생성된 이벤트에 액세스할 수 있습니다. 마스터 및 멤버 계정에 대한 자세한 내용은 개념 및 용어 (p. 10) 단원을 참조하십시오.

이벤트 형식

CloudWatch 이벤트의 Macie Classic에 대한 이벤트에는 다음과 같은 형식이 있습니다. 가상의 계정 ID `111122223333`은 마스터 Macie Classic 계정의 ID를 나타냅니다.

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Macie Alert",
  "source": "aws.macie",
  "account": "111122223333",
  "time": "2017-04-24T22:28:49Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:macie:us-east-1:111122223333:trigger/trigger_id/alert/alert_id",
    "arn:aws:macie:us-east-1:111122223333:trigger/trigger_id"
  ],
  "detail": {
    "notification-type": "ALERT_CREATED",
    "name": "Scanning bucket policies",
    "tags": [
      "Custom_Alert",
      "Insider"
    ],
    "url": "https://lb00.us-east-1.macie.aws.amazon.com/111122223333/posts/alert_id",
    "alert-arn": "arn:aws:macie:us-east-1:111122223333:trigger/trigger_id/alert/alert_id",
    "risk-score": 8,
    "trigger": {
      "rule-arn": "arn:aws:macie:us-east-1:111122223333:trigger/trigger_id",
      "alert-type": "basic",
      "created-at": "2017-01-02 19:54:00.644000",
      "description": "Alerting on failed enumeration of large number of bucket policies",
      "risk": 8
    },
    "created-at": "2017-04-18T00:21:12.059000",
    "actor": "555566667777:assumed-role:superawesome:aroaidpldc7nsesfnheji",
    "summary": {ALERT_DETAILS_JSON}
  }
}
```

CloudWatch 이벤트 구성

다음 절차를 완료하여 CloudWatch 이벤트에서 Macie Classic 이벤트를 받고 이러한 이벤트를 Amazon Simple Queue Service(Amazon SQS) 대기열로 추가하도록 마스터 Macie Classic 계정을 구성할 수 있습니다.

사전 조건

Macie Classic에서 이벤트에 대한 Amazon SQS 대기열을 생성합니다. 자세한 내용은 자습서: Amazon SQS 대기열 생성을 참조하십시오.

마스터 Macie Classic 계정에 대한 CloudWatch 이벤트를 구성하려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 이벤트, 규칙을 선택한 후 규칙 생성을 선택합니다.
3. 편집을 선택한 후 Macie Classic 이벤트에 대해 다음 이벤트 패턴을 입력합니다.

```
{
   "source": [
       "aws.macie"
   ]
}
```

4. 대상 창에서 대상 추가를 선택하고 대상 드롭다운 메뉴에서 SQS 대기열을 선택한 후 Macie Classic에서 이벤트에 대한 대기열을 지정합니다.

Amazon Macie Classic 문서 기록

다음 표에서는 Amazon Macie Classic 설명서에서 변경된 중요 사항에 대해 설명합니다.

update-history-change	update-history-description	update-history-date
새 콘텐츠 (p. 91)	새로운 버전의 Amazon Macie로 이전하는 방법을 설명하는 내용을 추가했습니다. 또한 이 설명서의 이름을 Amazon Macie Classic 사용 설명서로 변경했습니다.	May 13, 2020
새로운 기능 (p. 91)	Macie Classic에서 이제 `AWSServiceRoleForAmazonMacie`라는 서비스 연결 역할을 사용할 수 있습니다. Macie Classic는 이를 통해 사용자를 대신하여 AWS의 민감한 데이터를 검색, 분류 및 보호할 수 있습니다.	June 28, 2018
새 콘텐츠 (p. 91)	데이터 검색 결과에 나타날 수 있는 데이터 필드에 대한 설명을 추가했습니다. 자세한 내용은 CloudTrail 데이터 필드, S3 버킷 속성 데이터 필드 및 S3 객체 데이터 필드를 참조하십시오.	May 4, 2018
최초 릴리스 (p. 91)	이 사용 설명서를 최초로 릴리스했습니다.	August 14, 2017