aws

파트너 통합 안내서

AWS Security Hub

AWS Security Hub: 파트너 통합 안내서

Table of Contents

와의 타사 통합 개요 AWS Security Hub

이 가이드는 통합을 생성하려는 AWS 파트너 네트워크(APN) 파트너를 위한 것입니다 AWS Security Hub.

APN 파트너는 다음 방법 중 하나 이상을 사용하여 Security Hub와 통합할 수 있습니다.

- Security Hub로 조사 결과 전송
- Security Hub에서 조사 결과 사용
- Security Hub로 결과를 전송하고 결과를 사용
- Security Hub를 관리형 보안 서비스 제공업체(MSSP) 서비스의 중심으로 사용
- Security Hub를 배포하고 사용하는 방법에 대해 AWS 고객과 상담

이 온보딩 안내서는 주로 Security Hub에 조사 결과를 보내는 파트너에 초점을 맞추고 있습니다.

주제

가와 통합되는 이유는 AWS Security Hub무엇입니까?

AWS Security Hub 는 Security Hub 계정 전반의 우선 순위가 높은 보안 알림 및 보안 상태에 대한 포괄적인 보기를 제공합니다. Security Hub를 사용하면 귀사와 같은 파트너가 조사 결과를 Security Hub에 전송하여 고객이 생성한 조사 결과에 대한 인사이트를 제공할 수 있습니다.

Security Hub와의 통합은 다음과 같은 방식으로 가치를 더할 수 있습니다.

- Security Hub 통합을 요청한 고객을 만족시킵니다.
- 고객에게 AWS 보안 관련 조사 결과에 대한 단일 보기 제공
- 신규 고객이 특정 유형의 보안 이벤트와 관련된 결과를 제공하는 파트너를 찾을 때 솔루션을 발견할 수 있습니다.

Security Hub와의 통합을 구축하기 전에 통합의 이유를 검토하세요. 고객이 Security Hub 제품과 통합하기를 원하는 경우 통합이 성공할 가능성이 더 높습니다. 순전히 마케팅 목적이나 신규 고객을 확보하기 위한 목적으로 통합을 구축할 수도 있습니다. 그러나 현재 고객의 의견을 전혀 반영하지 않고 고객의 요구 사항을 고려하지 않은 상태로 통합을 구축하면 통합이 예상한 결과를 얻지 못할 수 있습니다.

로 조사 결과 전송 준비 AWS Security Hub

Security Hub 팀에서 APN 파트너를 조사 결과 제공자로 사용하도록 설정하기 전까지 APN 파트너는 고객의 정보를 Security Hub로 보낼 수 없습니다. 조사 결과 제공자로 지정되려면 다음과 같은 온보딩 단계를 완료해야 합니다. 이렇게 하면 Security Hub가 여러분과 고객에게 긍정적인 경험을 제공할 수 있습니다.

온보딩 단계를 완료할 때, the section called “조사 결과 작성 및 업데이트 원칙”, the section called “ASFF 매핑 지침”, the section called “`BatchImportFindings` API 사용 지침”의 지침을 반드시 따르세요.

1. 보안 조사 결과를 AWS 보안 조사 결과 형식(ASFF)에 매핑합니다.
2. 통합 아키텍처를 구축하여 보안 결과를 알맞은 리전 Security Hub 엔드포인트로 푸시합니다. 이렇게 하려면 자신의 AWS 계정에서 조사 결과를 보낼지 아니면 고객 계정 내에서 조사 결과를 보낼지를 정의합니다.
3. 고객이 자체 계정에 제품을 구독하도록 합니다. 이를 위해 콘솔이나 `EnableImportFindingsForProduct` API 작업을 사용할 수 있습니다. AWS Security Hub 사용 설명서에서 Managing product integrations를 참조하세요.

   해당 제품을 구독할 수도 있습니다. 이렇게 하려면 고객 대신 교차 계정 역할을 사용하여 `EnableImportFindingsForProduct` API 작업에 액세스해야 합니다.

   이 단계는 해당 계정에 대해 해당 제품의 결과를 수락하는 데 필요한 리소스 정책을 설정합니다.

다음 블로그 게시물에서는 Security Hub와의 기존 파트너 통합 중 일부에 대해 설명합니다.

- 와의 Cloud Custodian 통합 발표 AWS Security Hub
- AWS Fargate 및 Prowler를 사용하여 AWS 서비스에 대한 보안 구성 조사 결과를 Security Hub로 전송
- How to import AWS Config rules evaluations as findings in Security Hub

에서 조사 결과를 수신할 준비 AWS Security Hub

결과를 수신하려면 다음 옵션 중 하나를 AWS Security Hub사용합니다.

- 고객이 모든 조사 결과를 자동으로 CloudWatch Events에 보내도록 합니다. 고객은 특정 CloudWatch 이벤트 규칙을 생성하여 SIEM 또는 S3 버킷과 같은 특정 대상으로 결과를 보낼 수 있습니다.
- 고객이 Security Hub 콘솔에서 특정 결과 또는 결과 그룹을 선택한 다음 그에 대한 조치를 취하도록 합니다.

예를 들어, 고객은 SIEM, 티켓 시스템, 채팅 플랫폼 또는 수정 워크플로우에 조사 결과를 보낼 수 있습니다. 이는 고객이 Security Hub 내에서 수행하는 알림 분류 워크플로우의 일부가 될 수 있습니다.

이를 사용자 지정 작업이라고 합니다. 사용자가 사용자 지정 작업을 수행하면 해당 특정 결과에 대한 CloudWatch 이벤트가 생성됩니다. 파트너는 이 기능을 활용하여 고객이 사용자 지정 작업의 일부로 사용할 CloudWatch 이벤트 규칙 또는 대상을 만들 수 있습니다. 이 기능이 특정 유형이나 클래스의 모든 결과를 CloudWatch Events에 자동 전송하지는 않습니다. 이 기능은 사용자가 특정 결과에 대해 조치를 취하기 위한 것입니다.

다음 블로그 게시물에서는 사용자 지정 작업을 위해 Security Hub 및 CloudWatch Events와의 통합을 사용하는 솔루션을 간략하게 설명합니다.

- How to Integrate AWS Security Hub Custom Actions with PagerDuty
- 에서 사용자 지정 작업을 활성화하는 방법 AWS Security Hub
- How to import AWS Config rules evaluations as findings in Security Hub

에 대해 알아보기 위한 리소스 AWS Security Hub

다음 자료는 AWS Security Hub 솔루션과 AWS 고객이 서비스를 사용하는 방법을 더 잘 이해하는 데 도움이 될 수 있습니다.

- Introduction to AWS Security Hub video
- Security Hub 사용 설명서
- Security Hub API 레퍼런스
- 온보딩 웹 세미나

또한 AWS 계정 중 하나에서 Security Hub를 활성화하고 서비스에 대한 실습 경험을 얻는 것이 좋습니다.

파트너 사전 조건

와의 통합을 시작하려면 다음 기준 중 하나를 충족해야 AWS Security Hub합니다.

- AWS Select Tier 파트너 이상입니다.
- AWS ISV 파트너 경로에 가입했으며 Security Hub 통합에 사용하는 제품이 AWS Foundational Technical Review(FTR)를 완료했습니다. 그런 다음 제품에 "검토자 AWS" 배지가 부여됩니다.

또한와 상호 비공개 계약을 체결해야 합니다 AWS.

통합 사용 사례 및 필수 권한

AWS Security Hub 를 통해 AWS 고객은 APN 파트너로부터 조사 결과를 받을 수 있습니다. 파트너의 제품은 고객 AWS 계정 내부 또는 외부에서 실행될 수 있습니다. 고객 계정의 권한 구성은 파트너 제품이 사용하는 모델에 따라 다릅니다.

Security Hub에서 고객은 항상 어떤 파트너가 고객 계정으로 조사 결과를 보낼 수 있는지 제어합니다. 고객은 언제든지 파트너의 권한을 취소할 수 있습니다.

파트너가 보안 결과를 자신의 계정으로 전송할 수 있도록 고객은 먼저 Security Hub의 파트너 제품을 구독합니다. 구독 단계는 아래에 설명된 모든 사용 사례에 필요합니다. 고객이 제품 통합을 관리하는 방법에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 Managing product integrations를 참조하세요.

고객이 파트너 제품을 구독하면 Security Hub는 관리형 리소스 정책을 자동으로 생성합니다. 이 정책은 파트너 제품에 `BatchImportFindings` API 작업을 사용하여 고객 계정의 Security Hub에 조사 결과를 보낼 수 있는 권한을 부여합니다.

Security Hub와 통합되는 파트너 제품의 일반적인 사례는 다음과 같습니다. 이 정보에는 각 사용 사례에 필요한 추가 권한이 포함됩니다.

파트너 호스팅: 파트너 계정에서 보낸 조사 결과

이 사용 사례에서는 자신의 AWS 계정에서 제품을 호스팅하는 파트너를 다룹니다. AWS 고객의 보안 조사 결과를 전송하기 위해 파트너는 파트너 제품 계정에서 `BatchImportFindings` API 작업을 호출합니다.

이 사용 사례의 경우 고객 계정에는 고객이 파트너 제품을 구독할 때 설정된 권한만 필요합니다.

파트너 계정에서 `BatchImportFindings` API 작업을 호출하는 IAM 주체는 해당 주체가 `BatchImportFindings`를 호출할 수 있도록 허용하는 IAM 정책을 가지고 있어야 합니다.

파트너 제품이 Security Hub에서 조사 결과를 고객에게 보낼 수 있도록 하려면 다음 두 단계를 거쳐야 합니다.

1. 고객이 Security Hub에서 파트너 제품을 구독합니다.
2. Security Hub는 고객의 확인을 바탕으로 올바른 관리형 리소스 정책을 생성합니다.

고객 계정과 관련된 보안 결과를 전송하기 위해 파트너 제품은 자체 자격 증명을 사용하여 BatchImportFindings API 작업을 호출합니다.

다음은 파트너 계정의 보안 주체에게 필요한 Security Hub 권한을 부여하는 IAM 정책의 예제입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:*:product-subscription/company-
name/product-name"
        }
    ]
}
```

파트너 호스팅: 고객 계정에서 보낸 조사 결과

이 사용 사례에서는 자신의 AWS 계정에서 제품을 호스팅하지만 교차 계정 역할을 사용하여 고객의 계정에 액세스하는 파트너를 다룹니다. 이들은 고객 계정에서 BatchImportFindings API 작업을 호출합니다.

이 사용 사례에서는 파트너 계정이 고객 계정에서 고객 관리형 IAM 역할을 맡아 BatchImportFindings API 작업을 호출합니다.

이 호출은 고객 계정에서 이루어집니다. 따라서 관리형 리소스 정책에서는 파트너 제품 계정의 제품 ARN을 호출에 사용할 수 있도록 허용해야 합니다. Security Hub 관리 리소스 정책은 파트너 제품 계정 및 파트너 제품 ARN에 대한 권한을 부여합니다. 제품 ARN은 제공자로서의 파트너의 고유 식별자입니다. 파트너 제품 계정에서 호출을 한 것이 아니므로 고객은 파트너 제품이 Security Hub에 조사 결과를 보낼 수 있도록 명시적으로 권한을 부여해야 합니다.

파트너 계정과 고객 계정 간의 교차 계정 역할에 대한 모범 사례는 파트너가 제공하는 외부 식별자를 사용하는 것입니다. 이 외부 식별자는 고객 계정의 교차 계정 정책 정의의 일부입니다. 파트너는 역할을 맡을 때 식별자를 제공해야 합니다. 외부 식별자는 파트너에게 AWS 계정 액세스 권한을 부여할 때 추가 보안 계층을 제공합니다. 고유 식별자를 사용하면 파트너가 올바른 고객 계정을 사용할 수 있습니다.

파트너 제품이 계정 간 역할을 사용하여 Security Hub의 고객에게 조사 결과를 보낼 수 있도록 하려면 다음 네 단계를 거쳐야 합니다.

1. 고객 또는 고객을 대신하여 상호 계정 역할을 사용하는 파트너가 Security Hub에서 제품 구독을 시작합니다.
2. Security Hub는 고객의 확인을 바탕으로 올바른 관리형 리소스 정책을 생성합니다.
3. 고객이 수동으로 또는를 사용하여 교차 계정 역할을 구성합니다 AWS CloudFormation. 교차 계정 역할에 대한 자세한 내용은 IAM 사용 설명서의 제3자가 소유한 AWS 계정에 대한 액세스 제공을 참조하세요.
4. 제품은 고객 역할과 외부 ID를 안전하게 저장합니다.

그런 다음 제품은 Security Hub로 결과를 보냅니다.

1. 제품은 AWS Security Token Service (AWS STS)를 호출하여 고객 역할을 수임합니다.
2. 제품은 수임된 역할의 임시 자격 증명을 사용하여 Security Hub에서 `BatchImportFindings` API 작업을 호출합니다.

다음은 파트너의 교차 계정 역할에 필요한 Security Hub 권한을 부여하는 IAM 정책의 예제입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-1:111122223333:product-
subscription/company-name/product-name"
        }
    ]
}
```

정책의 `Resource` 섹션에서는 특정 제품 구독을 식별합니다. 이렇게 하면 파트너가 고객이 구독한 파트너 제품에 대한 조사 결과만 보낼 수 있습니다.

고객 호스팅: 고객 계정에서 보낸 조사 결과

이 사용 사례는 고객 AWS 계정에 제품을 배포한 파트너를 대상으로 합니다. `BatchImportFindings` API는 고객 계정에서 실행되는 솔루션에서 호출됩니다.

이 사용 사례의 경우 파트너 제품에 BatchImportFindings API를 호출할 수 있는 추가 권한을 부여해야 합니다. 이 권한이 부여되는 방법은 파트너 솔루션과 고객 계정에서 해당 권한이 구성된 방식에 따라 다릅니다.

이 접근 방식의 예로는 고객 계정의 EC2 인스턴스에서 실행되는 파트너 제품이 있습니다. 이 EC2 인스턴스에는 해당 인스턴스에 BatchImportFindings API 작업을 호출할 수 있는 권한을 부여하는 EC2 인스턴스 역할이 연결되어 있어야 합니다. 그러면 EC2 인스턴스가 고객 계정으로 보안 조사 결과를 보낼 수 있습니다.

이 사용 사례는 고객이 소유한 제품에 대해 조사 결과를 계정에 로드하는 시나리오와 기능상 동일합니다.

고객은 파트너 제품이 고객 계정의 조사 결과를 Security Hub의 고객에게 보낼 수 있도록 합니다.

1. 고객은 AWS CloudFormation또는 다른 배포 도구를 사용하여 파트너 제품을 AWS 계정에 수동으로 배포합니다.
2. 고객은 Security Hub에 조사 결과를 전송할 때 파트너 제품이 사용할 필수 IAM 정책을 정의합니다.
3. 고객은 EC2 인스턴스, 컨테이너 또는 Lambda 함수와 같은 파트너 제품의 필수 구성 요소에 정책을 연결합니다.

이제 제품에서 Security Hub로 결과를 보낼 수 있습니다.

1. 파트너 제품은 AWS SDK 또는를 사용하여 Security Hub에서 BatchImportFindings API 작업을 AWS CLI 호출합니다. 이 작업은 정책이 연결된 고객 계정의 구성 요소에서 호출합니다.
2. BatchImportFindings API 호출 중에 호출이 성공하는 데 필요한 임시 자격 증명이 생성됩니다.

다음은 고객 계정의 파트너 제품에 필요한 Security Hub 권한을 부여하는 IAM 정책의 예입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "securityhub:BatchImportFindings",
            "Resource": "arn:aws:securityhub:us-west-2:111122223333:product-
subscription/company-name/product-name"
        }
    ]
```

```
}
```

파트너 온보딩 프로세스

파트너는 온보딩 프로세스의 일환으로 몇 가지 상위 단계를 완료해야 합니다. 보안 조사 결과를 보내려면 먼저 다음 단계를 완료해야 합니다 AWS Security Hub.

1. APN 파트너 팀 또는 Security Hub 팀과 인게이지먼트를 시작하고 Security Hub의 파트너가 되는 데 관심을 표명합니다. Security Hub 커뮤니케이션 채널에 추가할 이메일 주소를 식별합니다.
2. AWS 는 Security Hub 파트너 온보딩 자료를 제공합니다.
3. 통합과 관련된 질문을 할 수 있는 Security Hub 파트너 Slack 채널에 초대받습니다.
4. 검토를 위해 APN 파트너 연락처에 제품 통합 매니페스트 초안을 제공합니다.

   제품 통합 매니페스트에는 와의 통합을 위한 파트너 제품 Amazon 리소스 이름(ARN)을 생성하는 데 사용되는 정보가 포함되어 있습니다 AWS Security Hub.

   Security Hub 콘솔의 파트너 제공업체 페이지에 표시되는 정보를 Security Hub 팀에 제공합니다. 이는 Security Hub 인사이트 라이브러리에 추가할 통합과 관련된 새로운 관리형 통찰력을 제안하는 데에도 사용됩니다.

   이 초기 버전의 제품 통합 매니페스트에는 전체 세부 정보가 포함되어 있지 않아도 됩니다. 하지만 최소한 사용 사례와 데이터 세트 정보는 포함되어 있어야 합니다.

   매니페스트와 필수 정보에 대한 자세한 내용은 제품 통합 매니페스트를 참조하세요.
5. Security Hub 팀에서 제품에 대한 제품 ARN을 제공합니다. ARN을 사용하여 찾기를 Security Hub로 보냅니다.
6. 조사 결과를 Security Hub로 보내거나 Security Hub에서 결과를 수신하도록 통합을 구축합니다.

   결과를 ASFF에 매핑하기

   조사 결과를 Security Hub로 보내려면 조사 결과를 AWS Security Finding Format(ASFF)에 매핑해야 합니다.

   ASFF는 AWS 보안 서비스, 파트너, 고객 보안 시스템 간에 공유할 수 있는 조사 결과에 대한 일관된 설명을 제공합니다. 이는 통합 노력을 줄이고 공통 언어를 장려하며 구현자를 위한 청사진을 제공합니다.

   ASFF는 AWS Security Hub에 결과를 전송하는 데 사용할 필수 유선 프로토콜 형식입니다. 조사 결과는 ASFF JSON 스키마 및 RFC-7493 I-JSON 메시지 형식을 준수하는 JSON 문서로 표

시됩니다. ASFF 스키마에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 AWS Security Finding Format (ASFF)을 참조하세요.

the section called “ASFF 매핑 지침” 섹션을 참조하세요.

통합 구축 및 테스트

소유한 AWS 계정을 사용하여 통합에 대한 모든 테스트를 완료할 수 있습니다. 이렇게 하면 Security Hub에 결과가 어떻게 표시되는지 완벽하게 파악할 수 있습니다. 또한 보안 결과에 대한 고객의 경험을 이해하는 데도 도움이 됩니다.

`BatchImportFindings` API 작업을 사용하여 새 조사 결과 및 업데이트된 결과를 Security Hub에 보낼 수 있습니다.

Security Hub 통합을 빌드하는 동안는 APN 파트너 연락처에 통합 진행 상황을 알리도록 AWS 권장합니다. 또한 통합 관련 질문에 대해 APN 파트너 연락처에 도움을 요청할 수도 있습니다.

the section called “`BatchImportFindings` API 사용 지침” 섹션을 참조하세요.

7. Security Hub 제품 팀에 통합을 시연합니다. 이 통합은 Security Hub 팀이 소유한 계정을 사용하여 시연해야 합니다.

   통합에 익숙해지면 Security Hub 팀이 귀하를 제공자로 등록하도록 승인합니다.
8. 검토할 최종 매니페스트 AWS 를 제공합니다.
9. Security Hub 팀은 Security Hub 콘솔에서 제공자 통합을 생성합니다. 그러면 고객이 통합을 검색하고 활성화할 수 있습니다.
10. (선택 사항) Security Hub 통합을 홍보하기 위해 추가 마케팅 활동에 참여합니다. 시장 진출 활동을 참조하세요.

    Security Hub는 최소한 다음과 같은 자산을 제공할 것을 권장합니다.
    - 작동 중인 통합 작업에 대한 데모 동영상(최대 3분) 비디오는 마케팅 목적으로 사용되며 AWS YouTube 채널에 게시됩니다.
    - Security Hub 퍼스트 콜 슬라이드 데크에 추가할 단일 슬라이드 아키텍처 다이어그램

시장 진출 활동

파트너는 AWS Security Hub 통합을 설명하고 홍보하는 데 도움이 되는 선택적 마케팅 활동에 참여할 수도 있습니다.

Security Hub와 관련된 마케팅 콘텐츠를 직접 만들려면 콘텐츠를 공개하기 전에 APN 파트너 관리자에게 초안을 보내 검토 및 승인을 받으세요. 이렇게 하면 모든 사람이 메시지에 대해 의견을 일치시킬 수 있습니다.

AWS 파트너 네트워크(APN) 파트너는 APN 파트너 마케팅 센트럴 및 시장 개발 자금(MDF) 프로그램을 사용하여 캠페인을 생성하고 자금 지원을 받을 수 있습니다. 이러한 프로그램에 대한 자세한 내용은 파트너 관리자에게 문의하세요.

Security Hub 파트너 페이지에 등록

Security Hub 파트너로 승인되면 AWS Security Hub 파트너 페이지에 솔루션을 표시할 수 있습니다.

이 페이지에 등록하려면 APN 파트너 연락처에 다음과 같은 세부 정보를 제공하세요. 파트너 개발 관리자(PDM), 파트너 솔루션 아키텍트(PSA) 또는 <securityhub-pms@amazon.com>으로 이메일을 보낼 수도 있습니다.

- 솔루션, Security Hub와의 통합, Security Hub와의 통합이 고객에게 제공하는 가치에 대한 간략한 설명. 이 설명은 공백을 포함하여 700자로 제한됩니다.
- 솔루션을 설명하는 페이지의 URL. 이 사이트는 AWS 통합, 특히 Security Hub 통합과 관련된 것이어야 합니다. 고객 경험과 고객이 통합을 사용하여 얻게 되는 가치에 초점을 맞춰야 합니다.
- 600x300픽셀 크기의 고해상도 로고 사본. 이 로고의 요구 사항에 대한 자세한 내용은 the section called “파트너 페이지 로고”를 참조하세요.

보도 자료

승인된 파트너인 경우 필요에 따라 웹 사이트 및 홍보 채널에 보도 자료를 게시할 수 있습니다. 보도 자료는의 승인을 받아야 합니다 AWS.

보도 자료를 게시하기 전에 APN 파트너 마케팅, Security Hub 리더십 및 AWS 외부 보안 서비스(ESS)의 검토를 AWS 위해에 제출해야 합니다. 보도 자료에는 ESS 담당 부사장을 위한 견적서 제안이 포함될 수 있습니다.

이 프로세스를 시작하려면 담당 PDM과 협력하세요. 보도 자료를 검토하는 데 필요한 서비스 수준에 관한 계약(SLA)은 영업일 기준 10일입니다.

AWS 파트너 네트워크(APN) 블로그

또한 작성하신 블로그 게시물을 APN 블로그에 게시하도록 도와드릴 수 있습니다. 블로그 게시물은 고객 스토리와 사용 사례에 초점을 맞춰야 합니다. 통합 출시 파트너라는 점만 강조해서는 안 됩니다.

관심이 있는 경우 PDM 또는 PSA에 문의하여 프로세스를 시작하세요. APN 블로그는 최종 승인 및 게시까지 8주 이상 걸릴 수 있습니다.

APN 블로그에 대해 알아야 할 주요 사항

블로그 게시물을 작성할 때는 다음 항목에 유의하세요.

블로그 게시물에는 어떤 내용이 담겨 있어야 합니까?

파트너 게시물은 교육적이어야 하며 AWS 고객과 관련된 주제에 대한 심층적인 전문 지식을 제공해야 합니다.

이상적인 길이는 1,500단어 이하입니다. 독자는 무엇이 가능한지 알려주는 심층적이고 교육적인 콘텐츠를 중요하게 생각합니다 AWS.

콘텐츠는 APN 블로그만의 독창적인 내용이어야 합니다. 기존 블로그 게시물이나 백서 등이 출처인 콘텐츠의 용도를 변경하여 사용하지 마세요.

APN 블로그에 게시할 때 적용되는 다른 제한 사항은 무엇입니까?

어드밴스드 또는 프리미어 티어 파트너만 APN 블로그에 게시할 수 있습니다. 서비스 제공과 같은 APN 프로그램 지정이 있는 일부 파트너에게는 예외가 있습니다.

각 파트너의 게시물은 연간 3회로 제한됩니다. 수만 개의 APN 파트너를 보유한 AWS 는 공평한 혜택을 제공해야 합니다.

각 게시물에는 솔루션 또는 사용 사례를 검증할 수 있는 기술 스폰서가 있어야 합니다.

블로그 게시물이 게시되기 전 편집은 얼마나 걸립니까?

블로그 게시물의 첫 번째 전체 길이 초안을 제출한 후 편집하는 데 4주에서 6주가 소요됩니다.

APN 블로그에 글을 쓰는 이유는 무엇입니까?

APN 블로그 게시물은 다음과 같은 이점을 제공합니다.

- 신뢰성 - APN 파트너의 경우에서 게시한 스토리가 전 세계 고객에게 영향을 미칠 AWS 수 있습니다.
- 가시성 - APN 블로그는 영향을 받는 트래픽을 포함하여 2019년에 179만 페이지 뷰 AWS 를 제공하는에서 가장 많이 읽은 블로그 중 하나입니다.
- 비즈니스 - APN 파트너 게시물에는 APN 고객 참여(ACE) 프로그램을 통해 잠재 고객을 생성할 수 있는 연결 버튼이 있습니다.

어떤 유형의 콘텐츠가 가장 적합합니까?

APN 블로그 게시물에 가장 적합한 콘텐츠 유형은 다음과 같습니다.

- 가장 인기 있는 유형의 스토리는 기술 관련 콘텐츠입니다. 여기에는 솔루션 스포트라이트 및 사용 방법 정보가 포함됩니다. 독자의 75% 이상이 이 기술 콘텐츠를 보고 있습니다.
- 고객은 AWS 에서 어떤 작업이 어떻게 진행되는지 또는 APN 파트너가 고객의 비즈니스 문제를 어떻게 해결했는지를 보여주는 200 레벨 이상의 스토리를 높이 평가합니다.
- 기술 전문가 또는 주제별 전문가가 작성한 게시물의 실적이 가장 우수합니다.

슬릭 시트 또는 마케팅 시트

슬릭 시트는 제품, 통합 아키텍처, 공동 고객 사용 사례를 요약한 한 페이지 분량의 문서입니다.

통합을 위한 슬릭 시트를 만들었다면, Security Hub 팀에 사본을 보내 주세요. 담당 팀이 파트너 페이지에 추가해 드립니다.

백서 또는 전자책

제품, 통합 아키텍처, 공동 고객 사용 사례를 요약한 백서 또는 전자책을 작성했다면 Security Hub 팀에 사본을 보내 주세요. 담당 팀이 Security Hub 파트너 페이지에 추가해 드립니다.

웹 세미나

통합에 대한 웹 세미나를 진행하는 경우 웹 세미나 녹화를 Security Hub 팀에 보내 주세요. 담당 팀이 파트너 페이지에 링크해 드립니다.

또한 웹 세미나에 참여할 Security Hub 주제 전문가를 주선해드릴 수도 있습니다.

데모 비디오

마케팅 목적으로 실제 통합의 데모 비디오를 제작할 수 있습니다. 비디오 플랫폼 계정에 비디오를 게시하면 Security Hub 팀이 파트너 페이지에서 해당 비디오로 연결해 드립니다.

제품 통합 매니페스트

모든 AWS Security Hub 통합 파트너는 제안된 통합에 필요한 세부 정보를 제공하는 제품 통합 매니페스트를 완료해야 합니다.

Security Hub 팀은 이 정보를 여러 가지 방법으로 사용합니다.

- 웹 사이트 목록 생성을 위해서.
- Security Hub 콘솔용 제품 카드 생성을 위해서.
- 제품 팀에 사용 사례를 알리기 위해서.

Security Hub 팀은 제안된 연동 서비스의 품질과 제공된 정보를 평가하기 위해 the section called “제품 준비 체크리스트”를 사용합니다. 이 체크리스트는 통합을 시작할 준비가 되었는지 여부를 결정합니다.

제공하는 모든 기술 정보는 설명서에도 반영되어야 합니다.

AWS Security Hub 파트너 페이지의 리소스 섹션에서 제품 통합 매니페스트의 PDF 버전을 다운로드할 수 있습니다. 중국(베이징) 및 중국(닝샤) 리전에서는 파트너 페이지를 사용할 수 없습니다.

내용

사용 사례 및 마케팅 정보

다음 사용 사례는 다양한 목적으로 AWS Security Hub 를 구성하는 데 도움이 될 수 있습니다.

공급자 및 소비자 사용 사례 찾기

독립 소프트웨어 개발 판매 회사(ISV)에 필요합니다.

와의 통합과 관련된 사용 사례를 설명하려면 다음 질문에 AWS Security Hub답하세요. 결과를 보내거나 받을 계획이 없다면 이 섹션의 내용을 참고하고 다음 섹션을 완료하세요.

설명서에는 다음과 같은 정보가 반영되어 있어야 합니다.

- 조사 결과를 보내시겠습니까, 받겠습니까, 아니면 둘 다 하시겠습니까?
- 조사 결과를 보낼 계획이라면 어떤 유형의 조사 결과를 보내시겠습니까? 모든 결과를 보내시겠습니까, 아니면 조사 결과의 특정 하위 집합을 보내시겠습니까?
- 조사 결과를 받을 계획이라면 해당 조사 결과를 어떻게 처리하겠습니까? 어떤 유형의 조사 결과를 받게 됩니까? 예를 들어, 모든 조사 결과 또는 특정 유형의 조사 결과를 받을 예정입니까, 아니면 고객이 선택한 특정 조사 결과만 받을 예정입니까?
- 조사 결과를 업데이트할 계획이십니까? 그렇다면 어떤 필드를 업데이트하시겠습니까? Security Hub는 항상 새 결과를 생성하는 대신 결과를 업데이트할 것을 권장합니다. 기존의 조사 결과를 업데이트하면 고객의 조사 결과 노이즈를 줄이는 데 도움이 됩니다.

  조사 결과를 업데이트하려면 이미 보낸 결과에 할당된 결과 ID로 결과를 보내면 됩니다.

사용 사례 및 데이터 세트에 대한 조기 피드백을 받으려면 APN 파트너 또는 Security Hub 팀에 문의하세요.

컨설팅 파트너(CP) 사용 사례

Security Hub 컨설팅 파트너인 경우 필수인 항목입니다.

Security Hub를 사용한 작업에 대한 두 가지 고객 사용 사례를 제공하세요. 이는 비공개 사용 사례일 수 있습니다. Security Hub 팀은 이를 어디에도 광고하지 않습니다. 다음 작업 중 하나 또는 모두를 설명해야 합니다.

- 고객이 Security Hub를 부트스트랩하도록 어떻게 지원합니까? 예를 들어 고객이 전문 서비스, Terraform 모듈 또는 AWS CloudFormation 템플릿을 사용하도록 도왔습니까?
- 고객이 Security Hub를 운영하고 확장하도록 어떻게 지원합니까? 예를 들어 응답 또는 수정 템플릿을 제공했거나, 맞춤형 통합을 구축했거나, 비즈니스 인텔리전스 도구를 사용하여 경영진 대시보드를 설정했습니까?

데이터세트

결과를 Security Hub로 보내는 경우 필요합니다.

Security Hub에 전송할 조사 결과에 대해서는 다음 정보를 제공하세요.

- JSON 또는 XML과 같은 기본 형식의 조사 결과
- 조사 결과를 AWS Security Finding Format(ASFF)으로 변환하는 방법의 예

통합을 지원하기 위해 ASFF에 대한 업데이트가 필요한 경우 Security Hub 팀에 알려주세요.

아키텍처

결과를 Security Hub로 보내거나 Security Hub에서 결과를 받는 경우 필수입니다.

Security Hub와 통합하는 방법을 설명해 주세요. 이 정보는 설명서에도 반영되어야 합니다.

아키텍처 다이어그램을 제공해야 합니다. 아키텍처 다이어그램을 준비할 때 다음을 고려하세요.

- 어떤 AWS 서비스, 운영 체제 에이전트 등을 사용하시겠습니까?
- 조사 결과를 Security Hub로 보내는 경우 고객 AWS 계정 또는 자신의 AWS 계정에서 조사 결과를 보내나요?
- 조사 결과를 받게 되면 CloudWatch Events 통합을 어떻게 사용할 계획입니까?
- 결과를 어떻게 ASFF로 변환할 것입니까?
- 결과를 어떻게 일괄 처리하고, 결과 상태를 추적하고, 병목 제한을 피할 것입니까?

구성

결과를 Security Hub로 보내거나 Security Hub에서 결과를 받는 경우 필수입니다.

고객이 Security Hub와의 통합을 어떻게 구성할지 설명하세요.

최소한 AWS CloudFormation 템플릿 또는 코드 템플릿과 같은 유사한 인프라를 사용해야 합니다. 일부 파트너는 원클릭 통합을 지원하는 사용자 인터페이스를 제공했습니다.

구성하는 데 걸리는 시간은 15분을 넘지 않아야 합니다. 제품 설명서에는 통합을 위한 구성 지침도 제공해야 합니다.

고객별 일일 평균 조사 결과

결과를 Security Hub로 보내는 경우 필요합니다.

고객 기반 전반에 걸쳐 Security Hub에 매월 몇 개의 결과 업데이트를 보낼 것으로 예상합니까(평균 및 최대)? 규모 추정치도 허용됩니다.

지연 시간

결과를 Security Hub로 보내는 경우 필요합니다.

조사 결과를 얼마나 빨리 일괄 처리하여 Security Hub로 전송하시겠습니까? 즉, 제품에서 결과가 생성된 시점부터 Security Hub로 전송될 때까지의 지연 시간은 얼마나 됩니까?

이 정보는 통합을 위한 제품 설명서에 반영되어야 합니다. 고객이 자주 묻는 질문입니다.

회사 및 제품 설명

Security Hub와의 모든 통합에 필요합니다.

Security Hub 통합의 성격을 구체적으로 강조하면서 회사와 제품을 간략하게 설명하세요. Security Hub 파트너 페이지에서 이 정보를 사용합니다.

여러 제품을 Security Hub와 통합하는 경우 각 제품에 대해 별도의 설명을 제공할 수 있지만 파트너 페이지에서는 해당 제품을 단일 항목으로 통합합니다.

각 설명은 공백을 포함하여 700자 이하여야 합니다.

파트너 웹 사이트 자산

Security Hub와의 모든 통합에 필요합니다.

최소한 Security Hub 파트너 페이지에서 자세히 알아보기 하이퍼링크에 사용할 URL을 제공해야 합니다. 제품과 Security Hub 간의 통합을 설명하는 마케팅 랜딩 페이지여야 합니다.

여러 제품을 Security Hub와 통합하는 경우 해당 제품에 대한 단일 랜딩 페이지를 만들 수 있습니다. Security Hub에서는 이 랜딩 페이지에 구성 지침에 대한 링크를 포함할 것을 권장합니다.

블로그, 웹 세미나, 데모 비디오 또는 백서와 같은 다른 리소스에 대한 링크를 제공할 수도 있습니다. Security Hub는 파트너 페이지에 있는 링크에도 연결됩니다.

파트너 페이지 로고

모든 Security Hub 통합에 필요합니다.

Security Hub 파트너 페이지에 표시할 로고의 URL을 제공하세요. 로고는 다음 조건을 충족해야 합니다.

- 크기: 600x300픽셀
- 크롭: 여백 없이 타이트하게 크롭할 것
- 배경: 투명
- 형식: PNG

Security Hub 콘솔용 로고

모든 통합에 필요합니다.

Security Hub 콘솔에 표시할 라이트 모드 및 다크 모드 로고의 URL을 제공하세요.

로고는 다음 조건을 충족해야 합니다.

- 형식: SVG
- 크기: 175x40픽셀 더 큰 경우 이미지가 해당 비율을 사용해야 합니다.
- 크롭: 여백 없이 타이트하게
- 배경: 투명

작은 로고에 대한 자세한 지침은 the section called “콘솔 로고 지침”을 참조하세요.

결과 유형

결과를 Security Hub로 보내는 경우 필요합니다.

사용하는 ASFF 형식의 조사 결과 유형과 이러한 유형이 기본 조사 결과 유형과 어떻게 일치하는지 문서화하는 표를 제공하세요. ASFF에서 유형을 찾는 방법에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 ASFF에 대한 유형 분류를 참조하세요.

또한 제품 설명서에 이 정보를 포함시키는 것이 좋습니다.

핫라인

Security Hub와의 모든 통합에 필요합니다.

기술 담당자에게 연락할 수 있는 이메일 주소와 전화번호 또는 페이저 번호를 제공하세요. 통합이 더 이상 작동하지 않는 경우와 같은 기술적인 문제가 발생하면 Security Hub에서 이 연락처로 연락을 드립니다.

또한 심각도가 높은 기술 문제에 대해서는 연중무휴 연락 창구를 제공하세요.

하트비트 검색

조사 결과를 Security Hub로 보내는 경우 권장됩니다.

Security Hub와의 통합이 작동 중임을 나타내는 '하트비트' 결과를 5분마다 Security Hub에 보낼 수 있습니까?

가능하다면 결과 유형 `Heartbeat`을 사용하여 결과를 보내세요.

AWS Security Hub 콘솔 정보

AWS Security Hub 팀에 다음 정보가 포함된 JSON 텍스트를 제공합니다. Security Hub는 이 정보를 사용하여 제품 ARN을 생성하고, 콘솔에 공급자 목록을 표시하고, 제안된 관리 인사이트를 Security Hub 인사이트 라이브러리에 포함시킵니다.

회사 정보

회사 정보는 회사에 대한 정보를 제공합니다. 다음은 그 예입니다.

```
{
    "id": "example",
    "name": "Example Corp",
    "description": "Example Corp is a network security company that monitors your
 network for vulnerabilities.",
}
```

회사 정보에는 다음과 같은 필드가 포함됩니다.

필드	필수	설명
`id`	예	회사의 고유 식별자입니다. 회사 식별자는 회사 간에 고유해야 합니다. name과 같거나 비슷할 수 있습니다. 유형: 문자열 최소 길이: 5자 최대 길이: 24자 허용되는 문자: 소문자, 숫자, 하이픈 소문자로 시작해야 합니다. 소문자 또는 숫자로 끝나야 합니다.
`name`	예	Security Hub 콘솔에 표시되는 제공업체의 회사 이름입니다. 유형: 문자열 최대 길이: 16자
`description`	예	Security Hub 콘솔에 표시될 제공업체의 회사에 대한 설명입니다. 유형: 문자열 최대 길이: 200자

제품 정보

이 섹션에서는 제품에 대한 정보를 제공합니다. 다음은 그 예입니다.

```
{
    "IntegrationTypes": ["SEND_FINDINGS_TO_SECURITY_HUB"],
    "id": "example-corp-network-defender",
```

```
    "regionsNotSupported": "us-west-1",
    "commercialAccountNumber": "111122223333",
    "govcloudAccountNumber": "444455556666",
    "chinaAccountNumber": "777788889999",
    "name": "Example Corp Product",
    "description": "Example Corp Product is a managed threat detection service.",
    "importType": "BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT",
    "category": "Intrusion Detection Systems (IDS)",
    "marketplaceUrl": "marketplace_url",
    "configurationUrl": "configuration_url"
}
```

제품 정보에는 다음과 같은 필드가 포함됩니다.

필드	필수	설명
IntegrationType	예	제품이 조사 결과를 Security Hub로 보내는지, Security Hub로부터 조사 결과를 받는지, 아니면 조사 결과를 보내기도 하고 받기도 하는지 표시합니다. 컨설팅 파트너인 경우 이 필드를 비워 둡니다. 유형: 문자열 배열 유효한 값: SEND_FINDINGS_TO_SECURITY_HUB | RECEIVE_FINDINGS_FROM_SECURITY_HUB
id	예	제품의 고유 식별자입니다. 이는 회사 내에서 고유해야 합니다. 회사 간에는 고유하지 않아도 됩니다. name과 같거나 비슷할 수 있습니다. 유형: 문자열 최소 길이: 5자 최대 길이: 24자 허용되는 문자: 소문자, 숫자, 하이픈

필드	필수	설명
		소문자로 시작해야 합니다. 소문자 또는 숫자로 끝나야 합니다.
`regionsNotSupported`	예	다음 중 지원하지 않는 AWS 리전은 무엇입니까? 즉, Security Hub에서 Security Hub 콘솔의 파트너 페이지에 옵션으로 표시하지 말아야 하는 리전은 어디입니까? 유형: 문자열 리전 코드만 입력하세요. 예: `us-west-1` . 리전 목록은 AWS 일반 참조의 리전 엔드포인트를 참조하세요. 의 리전 코드는 `us-gov-west-1` (AWS GovCloud(미국 서부)) 및 `us-gov-east-1` (for AWS GovCloud(미국 동부)) AWS GovCloud (US) 입니다. 중국 리전의 리전 코드는 `cn-north-1` (중국(베이징)) 및 `cn-northwest-1` (중국(닝샤))입니다.

필드	필수	설명
`commercialAccountNumber`	예	AWS 리전의 제품에 대한 기본 AWS 계정 번호입니다. 조사 결과를 Security Hub로 보내는 경우 제공하는 계정은 조사 결과를 보내는 위치를 기반으로 합니다. • AWS 계정에서. 이 경우, 조사 결과를 제출할 때 사용하는 계정 번호를 제공하세요. • 고객 AWS 계정에서. 이 경우, Security Hub는 통합 테스트에 사용하는 기본 계정 번호를 제공할 것을 권장합니다. 모든 리전의 모든 제품에 동일한 계정을 사용하는 것이 가장 좋습니다. 이렇게 할 수 없는 경우 Security Hub 팀에 문의하세요. Security Hub에서 조사 결과만 받는 경우 이 계정 번호는 필요하지 않습니다. 유형: 문자열

필드	필수	설명
`govcloudAccountNumber`	아니요	AWS GovCloud (US) 리전용 제품의 기본 AWS 계정 번호입니다(제품을 사용할 수 있는 경우 AWS GovCloud (US)). 조사 결과를 Security Hub로 보내는 경우 제공하는 계정은 조사 결과를 보내는 위치를 기반으로 합니다. • AWS 계정에서. 이 경우, 조사 결과를 제출할 때 사용하는 계정 번호를 제공하세요. • 고객 AWS 계정에서. 이 경우, Security Hub는 통합 테스트에 사용하는 기본 계정 번호를 제공할 것을 권장합니다. 모든 AWS GovCloud (US) 리전의 모든 제품에 동일한 계정을 사용하는 것이 이상적입니다. 이렇게 할 수 없는 경우 Security Hub 팀에 문의하세요. Security Hub에서 조사 결과만 받는 경우 이 계정 번호는 필요하지 않습니다. 유형: 문자열

필드	필수	설명
`chinaAccountNumber`	아니요	중국 리전용 제품의 기본 AWS 계정 번호입니다(중국 리전에서 제품을 사용할 수 있는 경우). 조사 결과를 Security Hub로 보내는 경우 제공하는 계정은 조사 결과를 보내는 위치를 기반으로 합니다. • AWS 계정에서. 이 경우, 조사 결과를 제출할 때 사용하는 계정 번호를 제공하세요. • 고객 AWS 계정에서. 이 경우, Security Hub는 통합 테스트에 사용하는 기본 계정 번호를 제공할 것을 권장합니다. 모든 중국 리전의 모든 제품에 동일한 계정을 사용하는 것이 이상적입니다. 이렇게 할 수 없는 경우 Security Hub 팀에 문의하세요. Security Hub에서만 조사 결과를 받는 경우에는 중국 리전에서 소유하고 있는 모든 계정이 될 수 있습니다. 유형: 문자열
`name`	예	Security Hub 콘솔에 표시할 제공업체 제품 이름입니다. 유형: 문자열 최대 길이: 24자
`description`	예	Security Hub 콘솔에 표시할 제공업체 제품에 대한 설명입니다. 유형: 문자열 최대 길이: 200자

필드	필수	설명
importType	예	파트너의 리소스 정책 유형입니다. 파트너 온보딩 프로세스 중에 다음 리소스 정책 중 하나를 지정하거나 NEITHER로 지정할 수 있습니다. • BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT 를 사용하면 제품 ARN에 등록된 계정에서만 Security Hub에 조사 결과를 보낼 수 있습니다. • BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT 를 사용하면 구독한 고객 계정의 조사 결과만 보낼 수 있습니다. 유형: 문자열 유효한 값: BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT | BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT | NEITHER

필드	필수	설명
`category`	예	제품을 정의하는 카테고리입니다. 선택 내용은 Security Hub 콘솔에 표시됩니다. 카테고리는 최대 3개까지 선택할 수 있습니다. 사용자 지정 선택은 허용되지 않습니다. 카테고리가 누락되었다고 생각되면 Security Hub 팀에 문의하세요. 유형: 배열 사용 가능한 카테고리: • `API Firewall` • `Asset Management` • `AV Scanning and Sandboxing` • `Backup and Disaster Recovery` • `Breach and Attack Simulation` • `Bug Bounty Platform` • `Certificate Management` • `Cloud Access Security Broker` • `Cloud Security Posture Management` • `Configuration and Patch Management` • `Configuration Management Database (CMDB)` • `Consulting Partner` • `Container Security` • `Cyber Range` • `Data Access Management` • `Data Classification` • `Data Loss Prevention`

필드	필수	설명
		• Data Masking and Tokenization • Database Activity Monitoring • DDoS Protection • Deception • Device Control • Dynamic Application Security Testing • Data Encryption • Email Gateway • Encrypted Search • Endpoint Detection and Response (EDR) • Endpoint Forensics • Forensics Toolkit • Fraud Detection • Governance, Risk, and Compliance (GRC) • Host-based Intrusion Detection (HIDs) • Human Resources Information System • Interactive Application Security Testing (IAST) • Instant Messaging • IoT Security • IT Security Training • IT Ticketing and Incident Management • Managed Security Service Provider (MSSP)

필드	필수	설명
		• Micro-Segmentation • Multi-Cloud Management • Multi-Factor Authentication • Network Access Control (NAC) • Network Firewall • Network Forensics • Network Intrusion Detection Systems (IDS) • Network Intrusion Prevention Systems (IPS) • Phishing Simulation and Training • Privacy Operations • Privileged Access Management • Rogue Device Detection • Runtime Application Self-Protection (RASP) • Secure Web Gateway
marketplaceUrl	아니요	제품 AWS Marketplace 대상의 URL입니다. URL은 Security Hub 콘솔에 표시됩니다. 유형: 문자열 URL이어야 합니다 AWS Marketplace . AWS Marketplace 목록이 없는 경우이 필드를 비워 둡니다.

필드	필수	설명
`configurationUrl`	예	Security Hub와의 통합에 대한 제품 설명서의 URL입니다. 이 콘텐츠는 웹 사이트 또는 관리자가 관리하는 웹 페이지(예: GitHub 페이지)에서 호스팅됩니다. 유형: 문자열 설명서에는 다음 정보가 포함되어야 합니다. • 구성 지침 • AWS CloudFormation 템플릿에 대한 링크(필요한 경우) • 통합 사용 사례에 대한 정보 • 지연 시간 • ASFF 매핑 • 포함된 결과 유형 • 아키텍처

지침 및 체크리스트

AWS Security Hub 통합에 필요한 자료를 준비할 때 다음 지침을 사용합니다.

준비 체크리스트는 Security Hub 고객에게 통합 기능을 제공하기 전에 통합을 최종 검토하는 데 사용됩니다.

주제

AWS Security Hub 콘솔에 표시할 로고에 대한 지침

AWS Security Hub 콘솔에 로고를 표시하려면 다음 지침을 따르세요.

라이트 모드와 다크 모드

로고의 라이트 모드와 다크 모드 버전을 모두 제공해야 합니다.

형식

SVG 파일 형식

배경색

투명

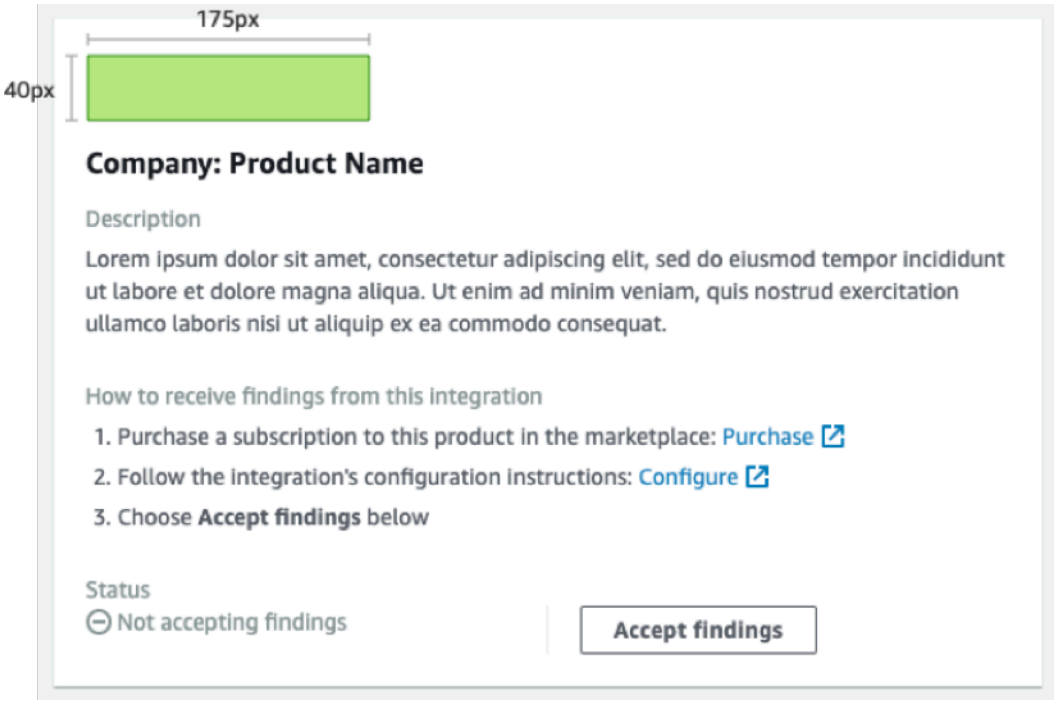
크기

이상적인 비율은 너비 175픽셀, 높이 40픽셀입니다.

최소 높이는 40픽셀입니다.

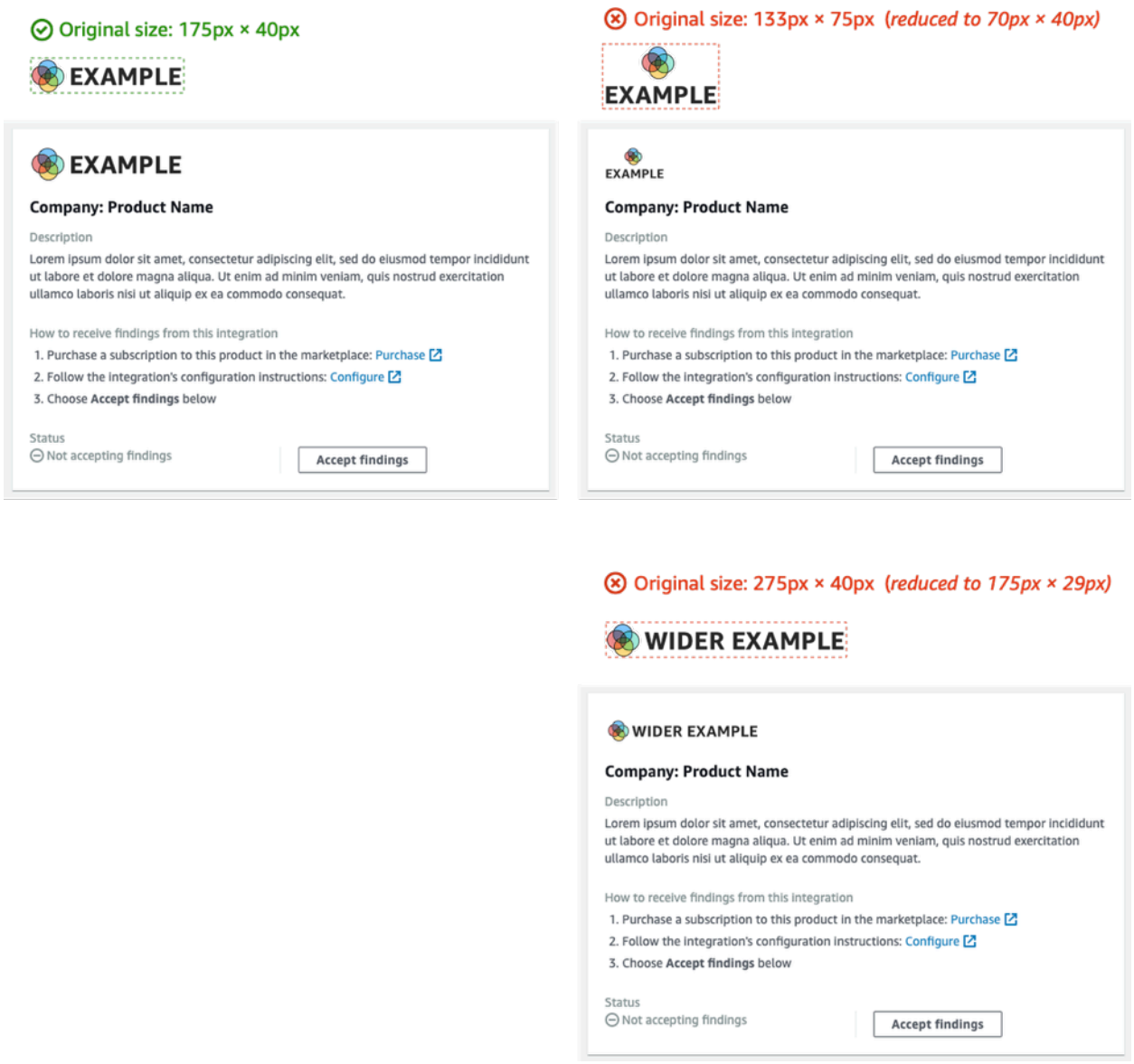
직사각형 로고가 가장 적합합니다.

다음 이미지는 Security Hub 콘솔에 이상적인 로고가 어떻게 표시되는지를 보여줍니다.



로고가 이 크기와 일치하지 않는 경우 Security Hub는 크기를 최대 높이 40픽셀, 최대 너비 175픽셀로 줄입니다. 이는 Security Hub 콘솔에 로고가 표시되는 방식에 영향을 줍니다.

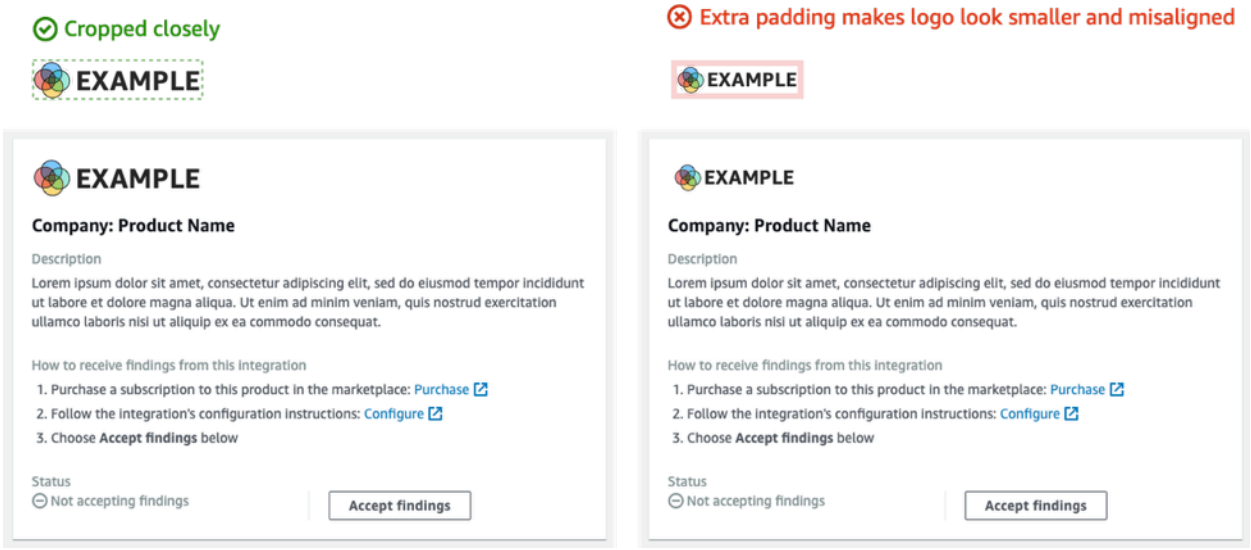
다음 이미지는 이상적인 크기를 사용한 로고와 더 넓거나 더 큰 로고의 표시를 비교한 것입니다.



크롭

로고 이미지는 최대한 가깝게 크롭하세요. 추가 여백을 제공하지 마세요.

다음 이미지는 가깝게 크롭한 로고와 추가 여백이 있는 로고의 차이를 보여줍니다.



조사 결과 작성 및 업데이트 원칙

결과를 생성하고 업데이트하는 방법을 계획할 때 AWS Security Hub다음 원칙을 염두에 두세요.

조사 결과를 구체적으로 작성하여 고객이 쉽게 조치를 취할 수 있도록 하세요.

고객은 대응 및 개선 조치를 자동화하고 조사 결과를 다른 조사 결과와 연관시키기를 원합니다. 이를 뒷받침하려면 결과가 다음과 같은 특성을 가져야 합니다.

- 일반적으로 단일 또는 기본 리소스를 다루어야 합니다.
- 검색 유형은 하나여야 합니다.
- 단일 보안 이벤트를 처리해야 합니다.

조사 결과에 여러 보안 이벤트에 대한 데이터가 포함되어 있으면 고객이 해당 결과에 대해 조치를 취하기가 더 어려워집니다.

모든 결과 필드를 AWS Security Finding Format(ASFF)에 매핑합니다. 고객이 Security Hub를 신뢰할 수 있는 소스로 사용할 수 있도록 하세요.

고객은 기본 검색 형식의 모든 필드가 Security Hub ASFF에도 표시되기를 기대합니다.

고객은 Security Hub 버전의 조사 결과에 모든 데이터가 표시되기를 원합니다. 데이터가 누락되면 보안 정보의 중심 소스인 Security Hub에 대한 신뢰를 잃게 됩니다.

조사 결과의 중복성을 최소화합니다. 고객에게 너무 많은 양의 조사 결과를 제공하지 마세요.

Security Hub는 일반적인 로그 관리 도구가 아닙니다. 실행 가능성이 높고 고객이 다른 조사 결과에 직접 대응하거나 문제를 해결하거나 상호 연관시킬 수 있는 조사 결과를 Security Hub에 보내야 합니다.

조사 결과에 사소한 변경 사항만 있는 경우 새 조사 결과를 만드는 대신 조사 결과를 업데이트하세요.

심각도 점수나 리소스 식별자와 같이 조사 결과에 중대한 변경 사항이 있는 경우 새 조사 결과를 생성하세요.

예를 들어, 개별 포트 스캔에 대한 조사 결과를 실시간으로 생성하는 것은 실행 가능성이 거의 없습니다. 포트 스캔은 지속적으로 이루어질 수 있기 때문에 대량의 조사 결과를 생성할 수 있습니다. TOR 노드에서 MongoDB 포트의 포트 스캔에 대한 단일 검색으로 마지막 스캔 시간과 스캔 수를 한 번만 업데이트하는 것이 훨씬 더 매력적이고 정확합니다.

고객이 조사 결과를 사용자 지정하여 더 의미 있게 만들 수 있도록 합니다.

고객은 특정 조사 결과 필드를 조정하여 자신의 환경이나 요구사항에 더 적합하게 만들 수 있기를 원합니다.

예를 들어, 고객은 계정 유형이나 조사 결과가 연결된 리소스 유형에 따라 메모, 태그를 추가하고 심각도 점수를 조정할 수 있기를 원합니다.

결과를 AWS Security Finding Format(ASFF)에 매핑하기 위한 지침

다음 지침을 사용하여 조사 결과를 ASFF에 매핑하세요. 각 ASFF 필드 및 객체에 대한 자세한 설명은 AWS 사용 설명서의 AWS Security Hub Security Finding Format (ASFF)을 참조하세요.

식별 정보

`SchemaVersion`은 항상 `2018-10-08`입니다.

`ProductArn`는가 AWS Security Hub 할당하는 ARN입니다.

`Id`는 Security Hub에서 조사 결과를 인덱싱하는 데 사용하는 값입니다. 조사 결과 식별자는 다른 조사 결과를 덮어쓰지 않도록 고유해야 합니다. 조사 결과를 업데이트하려면 동일한 식별자를 사용하여 조사 결과를 다시 제출하세요.

`GeneratorId`는 `Id`와 동일할 수도 있고, Amazon GuardDuty 탐지기 ID, AWS Config 레코더 ID 또는 IAM Access Analyzer ID와 같은 개별 로직 단위를 참조할 수도 있습니다.

Title 및 Description

Title에는 영향을 받는 리소스에 대한 몇 가지 정보가 포함되어야 합니다. Title은 공백을 포함하여 256자로 제한됩니다.

Description에 더 자세한 정보를 추가하세요. Description은 공백을 포함하여 1024자로 제한됩니다. 설명에 잘라내기를 추가하는 것도 고려해 볼 수 있습니다. 다음은 예시입니다.

```
"Title": "Instance i-12345678901 is vulnerable to CVE-2019-1234",
"Description": "Instance i-12345678901 is vulnerable to CVE-2019-1234. This
 vulnerability affects version 1.0.1 of widget-1 and earlier, and can lead to buffer
 overflow when someone sends a ping.",
```

결과 유형

FindingProviderFields.Types에서 결과 유형 정보를 제공합니다.

Types은 ASFF의 유형 분류와 일치해야 합니다.

필요한 경우 사용자 지정 분류자(세 번째 네임스페이스)를 지정할 수 있습니다.

타임스탬프

ASFF 형식에는 몇 가지 다른 타임스탬프가 포함됩니다.

CreatedAt 및 UpdatedAt

각 결과에 대해 BatchImportFindings를 호출할 때마다 CreatedAt 및 UpdatedAt을 제출해야 합니다.

값은 Python 3.8의 ISO8601 형식과 일치해야 합니다.

```
datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()
```

FirstObservedAt 및 LastObservedAt

FirstObservedAt과 LastObservedAt은 시스템에서 결과를 관찰한 시점과 일치해야 합니다. 이 정보를 기록하지 않으면 이러한 타임스탬프를 제출할 필요가 없습니다.

값은 Python 3.8의 ISO8601 형식과 일치합니다.

```
datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()
```

Severity

다음 필드가 포함된 FindingProviderFields.Severity 객체에서 심각도 정보를 제공합니다.

Original

시스템의 심각도 값입니다. Original은 사용하는 시스템에 맞게 어떤 문자열이든 사용할 수 있습니다.

Label

결과 심각도에 대한 필수 Security Hub 표시기입니다. 허용되는 값은 다음과 같습니다.

- INFORMATIONAL - 문제를 찾을 수 없습니다.
- LOW - 자체적으로 조치가 필요하지 않은 문제입니다.
- MEDIUM - 해결해야 하지만 긴급하지는 않은 문제입니다.
- HIGH - 우선적으로 해결해야 할 문제입니다.
- CRITICAL - 추가 피해를 방지하기 위해 즉시 해결해야 하는 문제입니다.

규정을 준수하는 결과는 항상 Label이 INFORMATIONAL로 설정되어 있어야 합니다. INFORMATIONAL 조사 결과의 예로는 통과한 보안 검사 결과와 해결된 AWS Firewall Manager 조사 결과가 있습니다.

고객은 보안 운영 팀에 할 일 목록을 제공하기 위해 심각도별로 조사 결과를 정렬하는 경우가 많습니다. 결과 심각도를 HIGH 또는 CRITICAL로 설정할 때는 보수적으로 설정하세요.

통합 문서에는 매핑 근거가 포함되어야 합니다.

Remediation

Remediation에는 두 가지 요소가 있습니다. 이러한 요소는 Security Hub 콘솔에 결합되어 있습니다.

Remediation.Recommendation.Text는 결과 세부 정보의 문제 해결 섹션에 나타납니다. Remediation.Recommendation.Url 값에 하이퍼링크되어 있습니다.

현재는 Security Hub 표준, IAM Access Analyzer 및 Firewall Manager의 결과에만 결과를 교정하는 방법에 대한 문서에 대한 하이퍼링크가 표시됩니다.

SourceUrl

특정 결과에 대해 콘솔에 딥링크 URL을 제공할 수 있는 경우에만 `SourceUrl`을 사용하세요. 그렇지 않으면 매핑에서 생략하세요.

Security Hub는 이 필드의 하이퍼링크를 지원하지 않지만 Security Hub 콘솔에는 표시됩니다.

Malware, Network, Process, ThreatIntelIndicators

해당하는 경우, `Malware`, `Network`, `Process` 또는 `ThreatIntelIndicators`를 사용하세요. 이러한 각 객체는 Security Hub 콘솔에 표시됩니다. 전송 중인 조사 결과의 맥락에서 이러한 객체를 사용하세요.

예를 들어, 알려진 명령 및 제어 노드에 대한 아웃바운드 연결을 만드는 악성 코드를 탐지하는 경우 `Resource.Details.AwsEc2Instance`에 EC2 인스턴스에 대한 세부 정보를 제공하세요. 해당 EC2 인스턴스에 대한 관련 `Malware`, `Network`, `ThreatIntelIndicator` 객체를 제공하세요.

Malware

`Malware`는 최대 5개의 멀웨어 정보 배열을 허용하는 목록입니다. 리소스 및 결과와 관련된 멀웨어 항목을 만드세요.

각 항목에는 다음과 같은 필드가 있습니다.

`Name`

멀웨어의 이름입니다. 값은 최대 64자의 문자열입니다.

`Name`은 검증된 위협 인텔리전스 또는 연구원 소스에서 나온 것이어야 합니다.

`Path`

멀웨어의 경로입니다. 값은 최대 512자의 문자열입니다. `Path`는 다음 경우를 제외하고 Linux 또는 Windows 시스템 파일 경로여야 합니다.

- YARA 규칙에 따라 S3 버킷 또는 EFS 공유의 객체를 스캔하는 경우 `Path`는 S3://또는 HTTPS 객체 경로입니다.
- Git 리포지토리의 파일을 스캔하는 경우 `Path`는 Git URL 또는 클론 경로입니다.

`State`

멀웨어의 상태입니다. 허용 값은 `OBSERVED` | `REMOVAL_FAILED` | `REMOVED`입니다.

결과 제목과 설명에 멀웨어가 발생한 상황에 대한 컨텍스트를 제공해야 합니다.

예를 들어 Malware.State가 REMOVED인 경우 조사 결과 제목과 설명에 제품이 경로에 있는 멀웨어를 제거했음을 반영해야 합니다.

Malware.State가 OBSERVED인 경우 조사 결과 제목과 설명에 제품이 경로에 있는 이 멀웨어를 발견했음을 반영해야 합니다.

Type

멀웨어 유형을 나타냅니다. 허용되는 값은 ADWARE | BLENDED_THREAT | BOTNET_AGENT | COIN_MINER | EXPLOIT_KIT | KEYLOGGER | MACRO | POTENTIALLY_UNWANTED | SPYWARE | RANSOMWARE | REMOTE_ACCESS | ROOTKIT | TROJAN | VIRUS | WORM입니다.

Type에 대한 추가 값이 필요한 경우 Security Hub 팀에 문의하세요.

Network

Network는 단일 객체입니다. 네트워크 관련 세부 정보는 여러 개 추가할 수 없습니다. 필드를 매핑할 때는 다음 지침을 사용하세요.

대상 및 소스 정보

대상과 소스는 TCP, VPC 흐름 로그 또는 WAF 로그를 쉽게 매핑할 수 있습니다. 공격에 대한 탐지 결과를 얻기 위해 네트워크 정보를 설명할 때는 사용하기가 더 어렵습니다.

일반적으로 소스는 공격이 시작된 위치이지만 아래에 나열된 것과 같은 다른 소스가 있을 수 있습니다. 문서에서 소스를 설명하고 조사 결과 제목 및 설명에도 소스를 설명해야 합니다.

- EC2 인스턴스에 대한 DDoS 공격의 경우 소스는 공격자이지만 실제 DDoS 공격은 수백만 개의 호스트를 사용할 수 있습니다. 대상은 EC2 인스턴스의 퍼블릭 IPv4 주소입니다. Direction은 IN입니다.
- EC2 인스턴스에서 알려진 명령 및 제어 노드로 통신하는 것으로 관찰된 멀웨어의 경우 소스는 EC2 인스턴스의 IPV4 주소입니다. 대상은 명령 및 제어 노드입니다. Direction은 OUT입니다. 또한 Malware 및 ThreatIntelIndicators도 제공합니다.

Protocol

특정 프로토콜을 제공할 수 없는 경우 Protocol은 항상 IANA(Internet Assigned Numbers Authority) 등록 이름에 매핑됩니다. 항상 이를 사용하고 포트 정보를 제공해야 합니다.

Protocol은 소스 및 대상 정보와 독립적입니다. 적절한 경우에만 제공하세요.

`Direction`

`Direction`는 항상 AWS 네트워크 경계를 기준으로 합니다.

- `IN`는 입력 중임을 의미합니다 AWS (VPC, 서비스).
- `OUT`는 AWS 네트워크 경계를 벗어남을 의미합니다.

Process

`Process`는 단일 객체입니다. 프로세스 관련 세부 정보는 여러 개 추가할 수 없습니다. 필드를 매핑할 때는 다음 지침을 사용하세요.

`Name`

`Name`은 실행 파일의 이름과 일치해야 합니다. 최대 64자까지 허용됩니다.

`Path`

`Path`는 프로세스 실행 파일의 시스템 경로입니다. 최대 512자까지 허용됩니다.

`Pid`, **`ParentPid`**

`Pid` 및 `ParentPid`는 Linux PID(프로세스 식별자) 또는 Windows 이벤트 ID와 일치해야 합니다. 차별화하려면 EC2 Amazon Machine Image(AMI)를 사용하여 정보를 제공하세요. 고객은 아마도 Windows와 Linux를 구별할 수 있을 것입니다.

타임스탬프(**`LaunchedAt`** 및 **`TerminatedAt`**)

이 정보를 안정적으로 검색할 수 없고 밀리초 단위까지 정확하지 않은 경우에는 제공하지 마세요.

포렌식 조사를 위해 타임스탬프를 사용하는 고객의 경우 타임스탬프가 없는 것이 잘못된 타임스탬프를 입력하는 것보다 낫습니다.

ThreatIntelIndicators

`ThreatIntelIndicators`는 최대 5개의 위협 인텔리전스 객체로 구성된 배열을 허용합니다.

각 항목에 대해 `Type`은 특정 위협의 맥락을 따릅니다. 허용되는 값은 `DOMAIN` | `EMAIL_ADDRESS` | `HASH_MD5` | `HASH_SHA1` | `HASH_SHA256` | `HASH_SHA512` | `IPV4_ADDRESS` | `IPV6_ADDRESS` | `MUTEX` | `PROCESS` | `URL`입니다.

다음은 위협 인텔리전스 지표를 매핑하는 방법의 몇 가지 예입니다.

- Cobalt Strike와 관련된 것으로 알고 있는 프로세스를 발견했습니다. FireEye의 블로그에서 이 내용을 배웠습니다.

  `Type`를 `PROCESS`으로 설정합니다. 프로세스에 사용할 `Process` 객체도 만듭니다.
- 메일 필터에서 누군가가 알려진 악성 도메인에서 잘 알려진 해시 패키지를 보내는 것을 발견했습니다.

  두 개의 `ThreatIntelIndicator` 객체를 만듭니다. 한 객체는 `DOMAIN`용입니다. 다른 하나는 `HASH_SHA1`용입니다.
- Yara 규칙(Loki, Fenrir, Awss3VirusScan, BinaryAlert)이 포함된 멀웨어를 발견했습니다.

  두 개의 `ThreatIntelIndicator` 객체를 만듭니다. 하나는 멀웨어를 위한 것입니다. 다른 하나는 `HASH_SHA1`용입니다.

Resources

`Resources`의 경우 가능하면 제공된 리소스 유형과 세부 정보 필드를 사용하세요. Security Hub는 ASFF에 지속적으로 새로운 리소스를 추가하고 있습니다. ASFF 변경 사항에 대한 월간 로그를 받으려면 <securityhub-partners@amazon.com>에 문의해 주세요.

모델링된 리소스 유형에 대한 세부 정보 필드의 정보를 맞출 수 없는 경우 나머지 세부 정보를 `Details.Other`에 매핑하세요.

ASFF에서 모델링되지 않은 리소스의 경우 `Type`을 `Other`로 설정합니다. 자세한 정보를 보려면 `Details.Other`를 사용하세요.

조사AWS 결과가 아닌 `Other` 리소스 유형을 사용할 수도 있습니다.

ProductFields

`ThreatIntelIndicators`, `Network` 또는 `Malware`와 같은 설명 객체 또는 `Resources`에 대해 다른 큐레이트된 필드를 사용할 수 없는 경우에만 `ProductFields`를 사용하세요.

`ProductFields`를 사용할 경우 이 결정에 대한 엄격한 근거를 제시해야 합니다.

Compliance

결과가 규정 준수와 관련된 경우에만 `Compliance`를 사용하세요.

Security Hub는 제어를 기반으로 생성된 결과에 대해 `Compliance`를 사용합니다.

Firewall Manager는 규정 준수와 관련된 결과이므로 `Compliance`를 사용합니다.

제한되는 필드

이 필드는 고객이 조사 결과에 대한 조사 내용을 추적할 수 있도록 하기 위한 것입니다.

이러한 필드나 개체에 매핑하지 마세요.

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

이러한 필드의 경우 `FindingProviderFields` 객체에 있는 필드에 매핑하세요. 최상위 필드에 매핑하지 마세요.

- `Confidence` - 서비스가 유사한 기능을 제공하거나 조사 결과를 100% 신뢰할 수 있는 경우에만 신뢰도 점수(0~99)를 포함합니다.
- `Criticality` - 중요도 점수(0~99)는 결과와 관련된 리소스의 중요성을 표현하기 위한 것입니다.
- `RelatedFindings` - 동일한 리소스 또는 결과 유형과 관련된 결과를 추적할 수 있는 경우에만 관련 결과를 제공합니다. 관련 조사 결과를 식별하려면 이미 Security Hub에 있는 결과의 결과 식별자를 참조해야 합니다.

`BatchImportFindings` API 사용 지침

`BatchImportFindings` API 작업을 사용하여 결과를 보낼 때는 다음 지침을 AWS Security Hub사용합니다.

- 조사 결과와 관련된 계정을 사용하여 `BatchImportFindings`를 호출해야 합니다. 관련 계정의 식별자는 결과에 대한 `AwsAccountId` 속성의 값입니다.
- 가능한 가장 큰 배치를 보내세요. Security Hub는 검색결과를 배치당 최대 100개, 검색당 최대 240KB, 배치당 최대 6MB까지 허용합니다.
- 조절 속도 제한은 리전별 계정당 10TPS이며 버스트는 30TPS입니다.
- 제한 또는 네트워크 문제가 있는 경우 조사 결과를 유지할 수 있는 메커니즘을 구현해야 합니다. 또한 조사 결과가 규정을 준수하거나 위반할 때 조사 결과 업데이트를 제출할 수 있도록 조사 결과 상태도 필요합니다.

- 문자열의 최대 길이 및 기타 제한 사항에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 AWS Security Finding Format (ASFF)을 참조하세요.

제품 준비 체크리스트

AWS Security Hub 및 APN 파트너 팀은이 체크리스트를 사용하여 통합을 시작할 준비가 되었는지 확인합니다.

ASFF 매핑

이러한 질문은 조사 결과를 AWS Security Finding Format(ASFF)에 매핑하는 것과 관련이 있습니다.

파트너의 모든 조사 결과 데이터가 ASFF에 매핑되어 있습니까?

모든 결과를 어떤 식으로든 ASFF에 매핑하세요.

모델링된 리소스 유형, `Network`, `Malware` 또는 `ThreatIntelIndicators`와 같은 큐레이트된 필드를 사용하세요.

그 외의 다른 모든 항목은 `Resource.Details.Other` 또는 `ProductFields`에 적절히 매핑하세요.

파트너가 **`AwsEc2instance`**, **`AwsS3Bucket`**, **`Container`**와 같은 **`Resource.Details`** 필드를 사용합니까? 파트너가 **`Resource.Details.Other`**를 사용하여 ASFF에서 모델링되지 않은 리소스 세부 정보를 정의합니까?

가능하면 EC2 인스턴스, S3 버킷, 보안 그룹과 같이 큐레이트된 리소스에 대해 제공된 필드를 결과에서 사용하세요.

리소스와 관련된 기타 정보는 직접 일치하는 항목이 없는 경우에만 `Resource.Details.Other`에 매핑하세요.

파트너가 값을 **`UserDefinedFields`**에 매핑합니까?

`UserDefinedFields`는 사용하지 마세요.

`Resource.Details.Other` 또는`ProductFields`와 같이 큐레이트된 다른 필드를 사용해 보세요.

파트너가 다른 ASFF 필드에 매핑할 수 있는 정보를 **`ProductFields`** 필드에 매핑합니까?

버전 관리 정보, 제품별 심각도 결과 또는 큐레이트된 필드나 `Resources.Details.Other`에 매핑할 수 없는 기타 정보와 같은 제품별 정보에만 `ProductFields` 필드를 사용하세요.

파트너가 **FirstObservedAt**에 대한 자체 타임스탬프를 가져옵니까?

FirstObservedAt 타임스탬프는 제품에서 조사 결과가 관찰된 시간을 기록하기 위한 것입니다. 가능하면 이 필드를 매핑하세요.

파트너는 업데이트하려는 결과를 제외하고 각 조사 결과 식별자에 대해 생성된 고유한 값을 제공합니까?

Security Hub의 모든 조사 결과는 결과 식별자(Id 속성)에 인덱싱됩니다. 이 값은 조사 결과가 실수로 업데이트되지 않도록 항상 고유해야 합니다.

또한 조사 결과를 업데이트하기 위해 조사 결과 식별자 상태를 유지해야 합니다.

파트너가 결과를 생성기 ID에 매핑하는 값을 제공합니까?

GeneratorID는 결과 ID와 같은 값을 가져서는 안 됩니다.

GeneratorID는 결과를 생성한 항목에 따라 결과를 논리적으로 연결할 수 있어야 합니다.

이는 제품 내의 하위 구성 요소(제품 A - 취약성 대 제품 A - EDR) 또는 이와 유사한 것일 수 있습니다.

파트너가 제품과 관련된 방식으로 필수 검색 유형 네임스페이스를 사용합니까? 파트너가 결과 유형에 권장 결과 유형 카테고리 또는 분류자를 사용합니까?

조사 결과 분류법은 제품에서 생성되는 결과와 밀접하게 매핑되어야 합니다.

AWS 보안 조사 결과 형식에 설명된 첫 번째 수준 네임스페이스가 필요합니다.

2단계 및 3단계 네임스페이스(카테고리 또는 분류자)에 사용자 정의 값을 사용할 수 있습니다.

파트너가 네트워크 데이터가 있는 경우 **Network** 필드에서 네트워크 흐름 정보를 캡처합니까?

제품이 NetFlow 정보를 캡처하는 경우 해당 정보를 Network 필드에 매핑하세요.

파트너가 프로세스 데이터가 있는 경우 **Process** 필드에서 프로세스(PID) 정보를 캡처합니까?

제품이 프로세스 정보를 캡처하는 경우 Process 필드에 매핑하세요.

파트너에게 멀웨어 데이터가 있는 경우 **Malware** 필드에서 멀웨어 정보를 캡처합니까?

제품이 멀웨어 정보를 캡처하는 경우 해당 정보를 Malware 필드에 매핑하세요.

파트너가 위협 인텔리전스 데이터를 가지고 있는 경우 **ThreatIntelIndicators** 필드에서 위협 인텔리전스 정보를 캡처합니까?

제품이 위협 인텔리전스 정보를 캡처하는 경우 해당 정보를 ThreatIntelIndicators 필드에 매핑하세요.

파트너가 결과에 대한 신뢰도 등급을 제공합니까? 제공한다면 그 근거를 제공합니까?

이 필드를 사용할 때마다 설명서와 매니페스트에 근거를 제시하세요.

파트너가 조사 결과의 리소스 ID로 표준 ID 또는 ARN을 사용합니까?

AWS 리소스를 식별할 때 ARN을 사용하는 것이 가장 좋습니다. ARN을 사용할 수 없는 경우 표준 리소스 ID를 사용하세요.

통합 설정 및 기능

이러한 질문은 통합의 설정 및 일상적인 기능과 관련이 있습니다.

파트너가 Terraform과 같은 Security Hub와의 통합을 배포하기 위해 infrastructure-as-code(IaC) 템플릿을 제공합니까 AWS CloudFormation, 아니면 AWS 클라우드 개발 키트 (AWS CDK)

고객 계정에서 결과를 보내거나 CloudWatch Events를 사용하여 결과를 소비하는 통합의 경우 특정 형태의 IaC 템플릿이 필요합니다.

AWS CloudFormation 가 선호되지만 AWS CDK 또는 Terraform도 사용할 수 있습니다.

파트너 제품의 콘솔에 Security Hub와의 통합을 위한 원클릭 설정 기능이 있습니까?

일부 파트너 제품은 제품에 토글 또는 유사한 메커니즘을 사용하여 통합을 활성화합니다. 여기에는 리소스와 권한이 자동으로 프로비저닝되어야 할 수도 있습니다. 제품 계정에서 결과를 보내는 경우 원클릭 설정이 선호됩니다.

파트너는 가치 있는 결과만 보냅니까?

일반적으로 보안 가치가 있는 조사 결과만 Security Hub 고객에게 보내야 합니다.

Security Hub는 일반적인 로그 관리 도구가 아닙니다. 가능한 모든 로그를 Security Hub에 전송해서는 안 됩니다.

파트너가 고객당 하루에 전송할 조사 결과 수와 빈도(평균 및 버스트)에 대한 예상 결과를 제공했습니까?

Security Hub의 부하를 계산하기 위해 고유한 조사 결과 수가 사용됩니다. 고유한 결과는 다른 결과와 다른 ASFF 매핑을 사용한 결과로 정의됩니다.

예를 들어, 한 결과가 `ThreatIntelIndicators`만 채우고 다른 결과가 `Resources.Details.AWSEc2Instance`만 채우는 경우, 이는 두 개의 고유한 결과입니다.

파트너가 제한되지 않고 모든 결과를 나중에 전송할 수 있도록 4xx 및 5xx 오류를 정상적으로 처리하는 방법이 있습니까?

현재 BatchImportFindings API 작업의 버스트 속도는 30~50TPS입니다. 4xx 또는 5xx 오류가 반환되는 경우 나중에 완전히 재시도할 수 있도록 실패한 결과의 상태를 보존해야 합니다. 배달 못한 편지 대기열이나 Amazon SNS 또는 Amazon SQS와 같은 다른 AWS 메시징 서비스를 통해이 작업을 수행할 수 있습니다.

파트너가 더 이상 존재하지 않는 조사 결과를 보관할 수 있도록 조사 결과의 상태를 유지합니까?

원래 결과 ID를 덮어쓰는 방식으로 결과를 업데이트하려는 경우, 올바른 결과에 대해 올바른 정보가 업데이트될 수 있도록 상태를 유지하는 메커니즘이 있어야 합니다.

조사 결과를 제공하는 경우 BatchUpdateFindings 작업을 사용하여 결과를 업데이트하지 마세요. 이 작업은 고객만 사용해야 합니다. 결과를 조사하고 결과에 대한 조치를 취할 때만 BatchUpdateFindings를 사용하세요.

파트너가 이전에 전송된 성공적인 결과를 손상시키지 않는 방식으로 재시도를 처리합니까?

오류 발생 시 원래의 검색어 ID를 유지하는 메커니즘이 있어야 성공적인 검색어를 오류로 복제하거나 덮어쓰지 않을 수 있습니다.

파트너가 기존 조사 결과의 조사 결과 ID로 **BatchImportFindings** 작업을 호출하여 결과를 업데이트합니까?

결과를 업데이트하려면 동일한 조사 결과 ID를 제출하여 기존 결과를 덮어써야 합니다.

BatchUpdateFindings 작업은 고객만 사용해야 합니다.

파트너가 **BatchUpdateFindings** API를 사용하여 결과를 업데이트합니까?

조사 결과에 대해 조치를 취하면 BatchUpdateFindings 작업을 사용하여 특정 필드를 업데이트할 수 있습니다.

파트너가 발견이 생성된 시점과 해당 발견이 제품에서 Security Hub로 전송되는 시점 사이의 지연 시간에 대한 정보를 제공합니까?

고객이 Security Hub에서 가능한 한 빨리 결과를 볼 수 있도록 지연 시간을 최소화해야 합니다.

이 정보는 매니페스트에 필요합니다.

파트너의 아키텍처가 고객 계정에서 Security Hub로 결과를 전송하는 경우, 파트너가 이를 성공적으로 시연했습니까? 파트너의 아키텍처가 자체 계정에서 Security Hub로 결과를 전송하는 경우, 이를 성공적으로 시연했습니까?

테스트 중에는 제품 ARN에 제공된 계정과 다른 계정을 소유하고 있는 계정에서 결과를 성공적으로 전송해야 합니다.

제품 ARN 소유자 계정에서 조사 결과를 보내면 API 작업의 특정 오류 예외를 우회할 수 있습니다.

파트너가 Security Hub에 하트비트 조사 결과를 제공합니까?

통합이 제대로 작동하는지 확인하려면 하트비트 조사 결과를 보내야 합니다. 하트비트 조사 결과는 5분마다 전송되며 결과 유형 `Heartbeat`를 사용합니다.

이는 제품 계정에서 결과를 전송할 때 중요합니다.

테스트 중에 파트너가 Security Hub 제품 팀의 계정과 통합되었습니까?

사전 프로덕션 검증 중에 조사 결과 예시를 Security Hub 제품 팀의 AWS 계정으로 보내야 합니다. 이러한 예는 결과가 올바르게 전송되고 매핑되었음을 보여줍니다.

설명서

이러한 질문은 제공하는 통합 설명서와 관련이 있습니다.

파트너가 전용 웹 사이트에서 설명서를 호스팅합니까?

문서는 정적 웹 페이지, 위키, Read the Docs, 또는 기타 전용 형식으로 웹 사이트에 호스팅되어야 합니다.

GitHub의 호스팅 문서는 전용 웹 사이트 요구 사항을 충족하지 않습니다.

파트너 문서에서 Security Hub 통합을 설정하는 방법에 대한 지침을 제공합니까?

IaC 템플릿이나 콘솔 기반의 '원클릭' 통합을 사용하여 통합을 설정할 수 있습니다.

파트너 설명서에 해당 사용 사례에 대한 설명이 제공됩니까?

매니페스트에서 제공하는 사용 사례는 설명서에도 설명되어 있어야 합니다.

파트너 설명서가 파트너가 보내는 조사 결과에 대한 근거를 제공합니까?

보내는 조사 결과 유형에 대한 근거를 제시해야 합니다.

예를 들어, 제품에서 취약성, 멀웨어 및 바이러스 백신 조사 결과를 생성하지만 취약성 및 멀웨어 탐지 결과만 Security Hub에 보낼 수 있습니다. 이 경우 바이러스 백신 조사 결과를 보내지 않는 이유에 대한 근거를 제공해야 합니다.

파트너 설명서에 파트너가 조사 결과를 ASFF에 매핑하는 방법에 대한 근거가 나와 있습니까?

제품의 고유 결과를 ASFF에 매핑하는 근거를 제시해야 합니다. 고객은 특정 제품 정보를 어디서 찾아야 하는지 알고 싶어합니다.

파트너 설명서에 파트너가 조사 결과를 업데이트할 경우 조사 결과를 업데이트하는 방법에 대한 지침이 제공됩니까?

상태를 유지하고, 멱등성을 보장하고, 결과를 최신 정보로 덮어쓰는 방법에 대한 정보를 고객에게 제공하세요.

파트너 설명서에 지연 시간 조사 결과에 대한 설명이 있습니까?

고객이 Security Hub에서 결과를 최대한 빨리 볼 수 있도록 지연 시간을 최소화하세요.

이 정보는 매니페스트에 필요합니다.

파트너 문서에 파트너의 심각도 점수가 ASFF 심각도 점수와 어떻게 매핑되는지 설명되어 있습니까?

`Severity.Original`을 `Severity.Label`에 매핑하는 방법에 대한 정보를 제공하세요.

예를 들어 심각도 값이 문자 등급(A, B, C)인 경우 문자 등급을 심각도 레이블에 매핑하는 방법에 대한 정보를 제공해야 합니다.

파트너 설명서에 신뢰 등급의 근거가 나와 있습니까?

신뢰도 점수를 제공할 경우 해당 점수의 순위를 매겨야 합니다.

정적으로 채워진 신뢰 점수 또는 인공 지능 또는 기계 학습에서 파생된 매핑을 사용하는 경우 추가 컨텍스트를 제공해야 합니다.

파트너 문서에 파트너가 지원하는 리전과 지원하지 않는 리전이 나와 있습니까?

고객이 통합을 시도하지 말아야 할 리전을 알 수 있도록 지원하는 리전 또는 지원하지 않는 리전을 기재하세요.

제품 카드 정보

이러한 질문은 Security Hub 콘솔의 통합 페이지에 표시되는 제품 카드와 관련이 있습니다.

제공된 AWS 계정 ID가 유효하고 12자리를 포함하나요?

계정 식별자의 길이는 12자리입니다. 계정 ID가 12자리 미만인 경우 제품 ARN은 유효하지 않습니다.

제품 설명이 200자 이하로 작성되어 있습니까?

매니페스트 내 JSON에 제공된 제품 설명은 공백을 포함하여 200자를 넘지 않아야 합니다.

구성 링크가 통합 설명서로 연결됩니까?

구성 링크는 온라인 설명서로 연결되어야 합니다. 기본 웹 사이트나 마케팅 페이지로 연결되어서는 안 됩니다.

구매 링크(제공된 경우)가 제품 AWS Marketplace 목록으로 연결되나요?

구매 링크를 제공하는 경우, AWS Marketplace 항목을 위한 링크여야 합니다. Security Hub는 AWS에서 호스팅되지 않은 구매 링크를 허용하지 않습니다.

제품 카테고리가 제품을 정확하게 설명합니까?

매니페스트에는 최대 3개의 상품 카테고리를 제공할 수 있습니다. 이는 JSON과 일치해야 하며 사용자 정의할 수 없습니다. 제품 카테고리는 3개 이상 제공할 수 없습니다.

회사 및 제품 이름이 유효하고 정확합니까?

회사 이름은 16자 이하여야 합니다.

제품 이름은 24자 이하여야 합니다.

제품 카드 JSON의 제품 이름은 매니페스트의 이름과 일치해야 합니다.

마케팅 정보

이 질문은 통합을 위한 마케팅과 관련된 질문입니다.

Security Hub 파트너 페이지의 제품 설명은 공백을 포함하여 700자 이내입니까?

Security Hub 파트너 페이지에는 공백을 포함하여 최대 700자까지만 입력할 수 있습니다.

그보다 더 긴 설명은 팀에서 편집할 것입니다.

Security Hub 파트너 페이지 로고가 600x300픽셀 이하입니까?

회사 로고를 600x300픽셀보다 크지 않은 PNG 또는 JPG로 된 공개적으로 액세스할 수 있는 URL 형식으로 제공하세요.

Security Hub 파트너 페이지의 자세히 알아보기 하이퍼링크를 클릭하면 통합에 대한 파트너의 전용 웹 페이지로 연결됩니까?

자세히 알아보기 링크는 파트너의 기본 웹 사이트 또는 설명서 정보로 연결되지 않아야 합니다.

이 링크는 항상 통합에 대한 마케팅 정보가 있는 전용 웹 페이지로 연결되어야 합니다.

파트너가 통합 서비스 사용 방법에 대한 데모 또는 교육용 동영상을 제공합니까?

데모 또는 통합 안내 동영상은 선택 사항이지만 권장됩니다.

AWS 파트너 및 파트너 개발 관리자 또는 파트너 개발 담당자와 함께 파트너 네트워크 블로그 게시물이 릴리스됩니까?

AWS 파트너 네트워크 블로그 게시물은 파트너 개발 관리자 또는 파트너 개발 담당자와 미리 조정해야 합니다.

이 게시물은 직접 작성하는 블로그 게시물과는 별도입니다.

4~6주의 리드 타임을 허용하세요. 이 작업은 비공개 제품 ARN으로 테스트를 완료한 후에 시작해야 합니다.

파트너가 주도하는 보도 자료가 발표되고 있습니까?

파트너 개발 관리자 또는 파트너 개발 담당자와 협력하여 외부 보안 서비스 담당 부사장으로부터 견적을 받을 수 있습니다. 보도 자료에 이 인용문을 사용할 수 있습니다.

파트너가 주도하는 블로그 게시물이 공개됩니까?

AWS 파트너 네트워크 블로그 외부에서 통합을 소개하는 자체 블로그 게시물을 작성할 수 있습니다.

파트너 주도 웹 세미나가 공개됩니까?

자체 웹 세미나를 생성하여 통합을 소개할 수 있습니다.

Security Hub 팀의 지원이 필요한 경우 비공개 제품 ARN으로 테스트를 완료한 후 제품 팀과 협력하세요.

파트너가에 소셜 미디어 지원을 요청했습니까 AWS?

릴리스 후 AWS 보안 마케팅 책임자와 협력하여 공식 소셜 미디어 채널을 사용하여 AWS 웨비나에 대한 세부 정보를 공유할 수 있습니다.

AWS Security Hub 파트너 FAQ

다음은 AWS Security Hub와의 통합 설정 및 유지 관리에 대한 일반적인 질문입니다.

1. Security Hub 통합의 이점은 무엇입니까?
   - 고객 만족 - Security Hub와 통합해야 하는 가장 큰 이유는 고객의 요청이 있기 때문입니다.

     Security Hub는 AWS 고객을 위한 보안 및 규정 준수 센터입니다. 보안 및 규정 준수 전문가가 AWS 보안 및 규정 준수 상태를 파악하기 위해 매일 이동하는 첫 번째 지점으로 설계되었습니다.

     고객의 의견을 들어보세요. Security Hub에서 발견한 결과를 보고 싶은지 고객이 알려줄 것입니다.
   - 발견 기회 - Security Hub 콘솔 내에서 AWS Marketplace 목록에 대한 링크를 포함하여 인증된 통합 기능을 갖춘 파트너를 홍보합니다. 이는 고객이 새로운 보안 제품을 발견할 수 있는 좋은 방법입니다.
   - 마케팅 기회 - 통합이 승인된 공급업체는 웨비나에 참여하고, 보도 자료를 발행하고, 슬릭 시트를 만들고, AWS 고객에게 통합을 시연할 수 있습니다.
2. 어떤 유형의 파트너가 있습니까?
   - Security Hub로 조사 결과를 전송하는 파트너
   - Security Hub로부터 조사 결과를 수신하는 파트너
   - 조사 결과를 전송하기도 하고 수신하기도 하는 파트너
   - 고객이 자신의 환경에서 Security Hub를 설치, 사용자 지정 및 사용할 수 있도록 지원하는 컨설팅 파트너
3. Security Hub와의 파트너 통합은 상위 수준에서 어떻게 작동합니까?

   고객 계정 또는 자체 AWS 계정에서 조사 결과를 수집하고 조사 결과 형식을 AWS Security Finding Format(ASFF)으로 변환합니다. 그런 다음 해당 결과를 적절한 Security Hub 리전 엔드포인트로 푸시합니다.

   CloudWatch Events를 사용하여 Security Hub에서 조사 결과를 받을 수도 있습니다.
4. Security Hub와의 통합을 완료하기 위한 기본 단계는 무엇입니까?

   a. 파트너 매니페스트 정보를 제출하세요.

   b. Security Hub로 조사 결과를 전송할 경우 Security Hub에서 사용할 제품 ARN을 받으세요.

   c. 결과를 ASFF에 매핑하세요. the section called “ASFF 매핑 지침”을 참조하세요.

d. Security Hub로 결과를 전송하고 수신하는 아키텍처를 정의하세요. the section called “조사 결과 작성 및 업데이트 원칙”에 설명된 원칙을 따르세요.

e. 고객을 위한 배포 프레임워크를 만드세요. 예를 들어 AWS CloudFormation 스크립트는이 목적을 제공할 수 있습니다.

f. 설정을 문서화하고 고객을 위한 구성 지침을 제공하세요.

g. 고객이 제품에 사용할 수 있는 사용자 지정 인사이트(상관 관계 규칙)를 정의하세요.

h. Security Hub 팀에 통합을 시연하세요.

i. 승인을 위해 마케팅 정보(웹 사이트 언어, 보도 자료, 아키텍처 슬라이드, 동영상, 슬릭 시트)를 제출하세요.

5. 파트너 매니페스트를 제출하는 절차는 어떻게 됩니까? 그리고 AWS 서비스에서 Security Hub로 조사 결과를 보내려면 어떻게 해야 합니까?

   매니페스트 정보를 Security Hub 팀에 제출하려면 <securityhub-partners@amazon.com>을 이용하세요.

   역일 기준 7일 이내에 제품 ARN이 발급됩니다.

6. Security Hub에 어떤 유형의 조사 결과를 보내야 합니까?

   Security Hub 요금은 수집된 조사 결과의 수에 따라 부분적으로 책정됩니다. 따라서 고객에게 가치를 제공하지 않는 조사 결과는 보내지 않는 것이 좋습니다.

   예를 들어, 일부 취약성 관리 공급업체는 CVSS(공통 취약성 평가 시스템) 점수가 10점 만점에 3점 이상인 조사 결과만 전송합니다.

7. Security Hub에 조사 결과를 보내는 방법에는 어떤 것이 있습니까?

   주요 접근 방식은 다음과 같습니다.

   - `BatchImportFindings` 작업을 AWS 사용하여 지정된 계정에서 조사 결과를 보냅니다.
   - 고객 계정 내에서 `BatchImportFindings` 작업을 사용하여 결과를 보냅니다. 역할 가정 접근 방식을 사용할 수도 있지만 이러한 접근 방식이 반드시 필요한 것은 아닙니다.

   `BatchImportFindings` 사용에 대한 전체 지침은 the section called “`BatchImportFindings` API 사용 지침”를 참조하세요.

8. 조사 결과를 수집하여 Security Hub 리전 엔드포인트로 푸시하려면 어떻게 해야 합니까?

   이 작업은 솔루션의 아키텍처에 따라 크게 달라지기 때문에 파트너마다 다른 접근 방식을 사용합니다.

예를 들어 일부 파트너는 AWS CloudFormation 스크립트로 배포할 수 있는 Python 앱을 빌드합니다. 이 스크립트는 고객 환경에서 파트너의 조사 결과를 수집하여 ASFF로 변환한 다음 Security Hub 리전 엔드포인트로 전송합니다.

고객이 클릭 한 번으로 조사 결과를 Security Hub로 푸시할 수 있는 전체 마법사를 구축한 파트너도 있습니다.

9. 조사 결과를 Security Hub로 보내기 시작하는 시점을 어떻게 알 수 있습니까?

   Security Hub는 모든 고객을 위해 모든 조사 결과를 Security Hub로 보낼 수 있도록 `BatchImportFindings` API 작업에 대한 부분 일괄 승인을 지원합니다.

   일부 고객이 아직 Security Hub를 구독하지 않은 경우 Security Hub는 해당 결과를 수집하지 않습니다. 일괄 처리 중인 승인된 조사 결과만 수집합니다.

10. 조사 결과를 고객의 Security Hub 인스턴스로 보내려면 어떤 단계를 완료해야 합니까?

    a. 올바른 IAM 정책이 마련되어 있는지 확인하세요.

    b. 계정에 대한 제품 구독(리소스 정책)을 사용 설정하세요. 제품에 대한 `EnableImportFindingsForProduct` API 작업 또는 통합 페이지를 사용하세요. 고객이 이 작업을 수행할 수도 있고, 교차 계정 역할을 사용하여 고객을 대신할 수도 있습니다.

    c. 조사 결과의 `ProductArn`이 제품의 공개 ARN인지 확인하세요.

    d. 조사 결과의 `AwsAccountId`가 고객의 계정 ID인지 확인하세요.

    e. 조사 결과에 AWS 보안 조사 결과 형식(ASFF)에 따라 잘못된 형식의 데이터가 없는지 확인합니다. 예를 들어 필수 필드가 채워져 있고 유효하지 않은 값이 없는지 확인하세요.

    f. 올바른 리전 엔드포인트로 발견 결과를 일괄적으로 전송하세요.

11. 결과를 보내려면 어떤 IAM 권한이 있어야 합니까?

    `BatchImportFindings` 또는 기타 API 호출을 호출하는 IAM 사용자 또는 역할에 대한 IAM 정책이 구성되어 있어야 합니다.

    가장 쉬운 테스트는 관리자 계정에서 이 작업을 수행하는 것입니다. 이를 `action: 'securityhub:BatchImportFindings'` 및 `resource: <productArn and/or productSubscriptionArn>`로 제한할 수 있습니다.

    동일한 계정의 리소스는 리소스 정책 없이도 IAM 정책으로 구성할 수 있습니다.

    `BatchImportFindings`호출자의 IAM 정책 문제를 배제하려면 호출자에 대한 IAM 정책을 다음과 같이 설정하세요.

```
{
    Action: 'securityhub:*',
    Effect: 'Allow',
    Resource: '*'
}
```

호출자에 대한 Deny 정책이 없는지 확인하세요. 이 기능을 사용하도록 설정한 후에는 정책을 다음과 같이 제한할 수 있습니다.

```
{
    Action: 'securityhub:BatchImportFindings',
    Effect: 'Allow',
    Resource: 'arn:aws:securityhub:<region>:<account>:product/mycompany/myproduct'
},
{
    Action: 'securityhub:BatchImportFindings',
    Effect: 'Allow',
    Resource: 'arn:aws:securityhub:<region>:*:product-subscription/mycompany/
myproduct'
}
```

12제품 구독이란 무엇입니까?

특정 파트너 제품으로부터 조사 결과를 받으려면 고객(또는 고객을 대신하여 계정 간 역할을 담당하는 파트너)이 제품 구독을 설정해야 합니다. 콘솔에서 이 작업을 수행하려면 통합 페이지를 사용합니다. API에서 이 작업을 수행하려면 `EnableImportFindingsForProduct` API 작업을 사용합니다.

제품 구독은 파트너의 조사 결과를 고객이 받거나 보낼 수 있도록 승인하는 리소스 정책을 생성합니다. 세부 정보는 사용 사례 및 권한을 참조하세요.

Security Hub에는 파트너를 위한 다음과 같은 유형의 리소스 정책이 있습니다.

- `BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`
- `BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT`

파트너 온보딩 프로세스 중에 하나 또는 두 가지 유형의 정책을 모두 요청할 수 있습니다.

`BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT`를 사용하면 제품 ARN에 등록된 계정에서만 Security Hub에 조사 결과를 보낼 수 있습니다.

BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT를 사용하면 구독한 고객 계정의 조사 결과만 보낼 수 있습니다.

13. 고객이 관리자 계정을 만들고 멤버 계정을 몇 개 추가했다고 가정해 보겠습니다. 각각의 멤버 계정이 저를 구독하도록 해야 합니까? 아니면 고객이 관리자 계정으로만 구독하면 제가 모든 멤버 계정의 리소스에 대해 조사 결과를 보낼 수 있습니까?

    이 질문은 관리자 계정 등록을 기준으로 모든 멤버 계정에 대한 권한이 생성되는지 여부를 묻는 질문입니다.

    고객은 각 계정에 대해 제품 구독을 설정해야 합니다. API를 통해 프로그래밍 방식으로 이 작업을 수행할 수 있습니다.

14. 내 제품 ARN은 무엇입니까?

    제품 ARN은 Security Hub에서 생성하여 조사 결과를 제출하는 데 사용하는 고유 식별자입니다. Security Hub와 통합하는 각 제품에 대해 제품 ARN을 받게 됩니다. Security Hub로 보내는 모든 조사 결과에는 올바른 제품 ARN이 포함되어야 합니다. 제품 ARN이 없는 조사 결과는 삭제됩니다. 제품 ARN은 다음 형식을 사용합니다.

    `arn:aws:securityhub:[region code]:[account ID]:product/[company name]/[product name]`

    예:

    `arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro`

    Security Hub가 배포된 각 리전에 대해 제품 ARN이 제공됩니다. 계정 ID, 회사 및 제품 이름은 파트너 매니페스트 제출에 따라 결정됩니다. 리전 코드를 제외하고는 제품 ARN과 관련된 어떤 정보도 변경할 수 없습니다. 리전 코드는 조사 결과를 제출하는 리전과 일치해야 합니다.

    흔히 하는 실수는 현재 작업 중인 계정과 일치하도록 계정 ID를 변경하는 것입니다. 계정 ID는 변경되지 않습니다. 매니페스트 제출의 일부로 '홈' 계정 ID를 제출합니다. 이 계정 ID는 제품 ARN에 고정되어 있습니다.

    Security Hub가 새 리전에 출시되면 표준 리전 코드를 사용하여 해당 리전에 대한 제품 ARN을 자동으로 생성합니다.

    또한 모든 계정에는 비공개 제품 ARN이 자동으로 프로비저닝됩니다. 이 ARN을 사용하여 공식 공개 제품 ARN을 받기 전에 자체 개발 계정 내에서 결과를 가져오는 것을 테스트할 수 있습니다.

15. Security Hub로 조사 결과를 전송하려면 어떤 형식을 사용해야 합니까?

조사 결과는 AWS 보안 조사 결과 형식(ASFF)으로 제공해야 합니다. 자세한 내용은 AWS Security Hub 사용 설명서에서 AWS Security Finding Format (ASFF)을 참조하세요.

기본 조사 결과에 있는 모든 정보가 ASFF에 완전히 반영될 것으로 예상됩니다. `ProductFields` 및 `Resource.Details.Other`와 같은 사용자 지정 필드를 사용하면 사전 정의된 필드에 잘 맞지 않는 데이터를 매핑할 수 있습니다.

16.사용할 올바른 리전 엔드포인트는 무엇입니까?

고객 계정과 연결된 Security Hub 리전 엔드포인트로 조사 결과를 보내야 합니다.

17.리전 엔드포인트 목록은 어디에서 찾을 수 있습니까?

Security Hub 엔드포인트 목록을 참조하세요.

18.리전 간 조사 결과를 제출할 수 있습니까?

Security Hub는 Amazon GuardDuty, Amazon Macie, Amazon Inspector와 같은 네이티브 AWS 서비스에 대한 리전 간 조사 결과 제출을 아직 지원하지 않습니다. 고객이 허용하는 경우 Security Hub는 다른 리전의 조사 결과를 제출하는 것을 막지 않습니다.

따라서 어디서든 리전 엔드포인트를 호출할 수 있으며, ASFF의 리소스 정보가 엔드포인트의 리전과 일치하지 않아도 됩니다. 하지만 `ProductArn`은 엔드포인트의 리전과 일치해야 합니다.

19.조사 결과 일괄 전송에 대한 규칙과 지침은 무엇입니까?

`BatchImportFindings`를 한 번 호출할 때 최대 100개 또는 240KB의 결과를 일괄 전송할 수 있습니다. 이 한도까지 가능한 한 많은 조사 결과를 대기열에 넣고 일괄 처리하세요.

여러 계정의 조사 결과 집합을 일괄 처리할 수 있습니다. 그러나 배치에 포함된 계정 중 하나라도 Security Hub를 구독하지 않은 계정이 있으면 전체 배치가 실패합니다. 이는 API 게이트웨이 기준 인증 모델의 제한 사항입니다.

the section called “`BatchImportFindings` API 사용 지침” 섹션을 참조하세요.

20.내가 만든 조사 결과에 대한 업데이트를 보낼 수 있습니까?

예. 동일한 제품 ARN과 동일한 조사 결과 ID로 검색 결과를 제출하면 해당 조사 결과에 대한 이전 데이터를 덮어씁니다. 모든 데이터를 덮어쓰므로 전체 조사 결과를 제출해야 합니다.

고객에게는 새로운 조사 결과와 조사 결과 업데이트 모두에 대해 요금이 청구됩니다.

21.다른 사람이 만든 조사 결과에 대한 업데이트를 보낼 수 있습니까?

예. 고객이 `BatchUpdateFindings` API 작업에 대한 액세스 권한을 부여하면 해당 작업을 사용하여 특정 필드를 업데이트할 수 있습니다. 이 작업은 고객, SIEM, 티켓팅 시스템 및 SOAR(보안 오케스트레이션, 자동화 및 대응) 플랫폼에서 사용하도록 설계되었습니다.

22 조사 결과의 유효 기간은 어떻게 됩니까?

Security Hub는 마지막 업데이트 날짜로부터 90일 후에 조사 결과의 유효 기간을 만료시킵니다. 이 시간이 지나면 오래된 조사 결과는 Security Hub OpenSearch 클러스터에서 제거됩니다.

동일한 조사 결과 ID로 조사 결과를 업데이트했는데 조사 결과가 만료된 경우 Security Hub에 새 조사 결과가 생성됩니다.

고객은 CloudWatch Events를 사용하여 조사 결과를 Security Hub 외부로 옮길 수 있습니다. 이렇게 하면 모든 결과를 고객이 선택한 대상으로 보낼 수 있습니다.

일반적으로 Security Hub는 90일마다 새로운 조사 결과를 생성하고 조사 결과를 영구적으로 업데이트하지 말 것을 권장합니다.

23 Security Hub에는 어떤 제한이 적용됩니까?

Security Hub가 조사 정보에 액세스하기 위한 권장 접근 방식은 CloudWatch Events를 사용하는 것이므로 `GetFindings` API 호출을 제한합니다.

Security Hub는 API Gateway 및 Lambda 호출에 의해 적용되는 것 외에는 내부 서비스, 파트너 또는 고객에 대한 다른 제한을 구현하지 않습니다.

24 소스 서비스에서 Security Hub로 전송되는 결과에 대한 적시성 또는 지연 시간 SLA 또는 기대치는 무엇입니까?

목표는 초기 조사 결과와 결과 업데이트 모두를 가능한 한 실시간에 가깝게 만드는 것입니다. 조사 결과는 생성된 후 5분 이내에 Security Hub로 보내야 합니다.

25 Security Hub에서 조사 결과를 받으려면 어떻게 해야 합니까?

조사 결과를 받으려면 다음 방법 중 하나를 사용하세요.

- 모든 조사 결과는 자동으로 CloudWatch Events로 전송됩니다. 고객은 특정 CloudWatch Events 규칙을 생성하여 SIEM 또는 S3 버킷과 같은 특정 대상으로 결과를 보낼 수 있습니다. 이 기능은 기존의 `GetFindings` API 작업을 대체합니다.
- CloudWatch Events를 사용하여 사용자 지정 작업을 수행할 수 있습니다. Security Hub를 사용하면 고객이 콘솔 내에서 특정 조사 결과 또는 조사 결과 그룹을 선택하고 조치를 취할 수 있습니다. 예를 들어 SIEM, 티켓 시스템, 채팅 플랫폼 또는 문제 해결 워크플로에 조사 결과를 보낼 수 있습

니다. 이는 고객이 Security Hub 내에서 수행하는 알림 분류 워크플로우의 일부가 될 수 있습니다. 이를 사용자 지정 작업이라고 합니다.

사용자가 사용자 지정 작업을 선택하면 해당 특정 조사 결과에 대한 CloudWatch 이벤트가 생성됩니다. 이 기능을 활용하여 고객이 사용자 지정 작업의 일부로 사용할 CloudWatch Events 규칙 및 대상을 구축할 수 있습니다. 이 기능은 특정 유형이나 클래스의 모든 결과를 CloudWatch Events에 자동으로 전송하는 데 사용되지는 않으며, 사용자가 특정 결과에 대해 조치를 취하기 위한 것입니다.

와 같은 사용자 지정 작업 API 작업을 사용하여 제품에 사용할 수 있는 작업(예: AWS CloudFormation 템플릿 사용)`CreateActionTarget`을 자동으로 생성할 수 있습니다. 또한 CloudWatch Events 규칙 API 작업을 사용하여 사용자 지정 작업과 관련된 해당 CloudWatch Events 규칙을 생성할 수 있습니다. AWS CloudFormation 템플릿을 사용하여 CloudWatch Events 규칙을 생성하여 Security Hub에서 모든 조사 결과 또는 특정 특성을 가진 모든 조사 결과를 자동으로 수집할 수도 있습니다.

26.관리형 보안 서비스 제공업체(MSSP)가 Security Hub 파트너가 되기 위한 요건은 무엇입니까?

고객에게 서비스를 제공하는 과정에서 Security Hub가 어떻게 사용되는지 보여 주어야 합니다.

Security Hub 사용을 설명하는 사용자 설명서가 있어야 합니다.

MSSP가 결과 공급자인 경우 Security Hub에 조사 결과를 보내는 것을 입증해야 합니다.

MSSP가 Security Hub의 조사 결과만 수신하는 경우, 최소한 적절한 CloudWatch Events 규칙을 설정할 수 있는 AWS CloudFormation 템플릿이 있어야 합니다.

27.MSSP가 아닌 APN 컨설팅 파트너가 Security Hub 파트너가 되기 위한 요건은 무엇입니까?

APN 컨설팅 파트너인 경우 Security Hub 파트너가 될 수 있습니다. 특정 고객이 다음을 수행하도록 지원한 방법에 대한 비공개 사례 연구 2개를 제출해야 합니다.

- 고객이 필요로 하는 IAM 권한으로 Security Hub를 설정하세요.
- 콘솔의 파트너 페이지에 있는 구성 지침을 사용하여 이미 통합된 독립 소프트웨어 개발 판매 회사(ISV) 솔루션을 Security Hub에 연결하도록 지원하세요.
- 맞춤형 제품 통합으로 고객을 지원하세요.
- 고객의 요구 사항 및 데이터 세트와 관련된 사용자 지정 인사이트를 구축하세요.
- 사용자 지정 작업을 구축하세요.
- 문제 해결 플레이북을 구축하세요.

- Security Hub 규정 준수 표준에 부합하는 Quickstarts를 구축하세요. 이는 Security Hub 팀의 검증을 거쳐야 합니다.

사례 연구를 공개적으로 공유할 필요는 없습니다.

28.Security Hub와의 통합을 고객에게 배포하는 방법과 관련된 요구 사항은 무엇입니까?

Security Hub와 파트너 제품 간의 통합 아키텍처는 파트너 솔루션 운영 방식에 따라 파트너마다 다릅니다. 통합을 위한 설정 프로세스가 15분을 넘지 않도록 해야 합니다.

통합 소프트웨어를 고객 AWS 환경에 배포하는 경우 AWS CloudFormation 템플릿을 활용하여 통합을 간소화해야 합니다. 일부 파트너는 원클릭 통합을 만들었으며, 이를 적극 권장합니다.

29.설명서에 대한 요구 사항은 무엇입니까?

AWS CloudFormation 템플릿 사용을 포함하여 제품과 Security Hub 간의 통합 및 설정 프로세스를 설명하는 설명서 링크를 제공해야 합니다.

이 설명서에는 ASFF 사용에 대한 정보도 포함되어야 합니다. 특히, 여기에는 다양한 결과에 사용하는 ASFF 조사 결과 유형이 나열되어야 합니다. 기본 인사이트 정의가 있는 경우 여기에도 포함하는 것이 좋습니다.

다음과 같은 기타 잠재적 정보를 포함하는 것을 고려해 보세요.

- Security Hub와의 통합을 위한 사용 사례
- 평균 조사 결과 전송량
- 통합 아키텍처
- 지원하는 리전과 지원하지 않는 리전
- 조사 결과가 생성된 시점과 Security Hub로 전송되는 시점 사이의 지연
- 조사 결과 업데이트 여부

30.사용자 지정 인사이트란 무엇입니까?

결과에 대한 사용자 지정 인사이트를 정의하는 것이 좋습니다. 인사이트는 간단한 상관 관계 규칙으로, 고객이 가장 주의를 기울이고 조치를 취해야 하는 결과 및 리소스의 우선 순위를 정하는 데 도움이 됩니다.

Security Hub에는 `CreateInsight` API 오퍼레이션이 있습니다. AWS CloudFormation 템플릿의 일부로 고객 계정 내에서 사용자 지정 인사이트를 생성할 수 있습니다. 이러한 인사이트는 고객 콘솔에 표시됩니다.

31.대시보드 위젯을 제출할 수 있습니까?

아니요, 현재는 지원되지 않습니다. 관리형 인사이트만 만들 수 있습니다.

32.요금 모델은 어떻게 됩니까?

Security Hub 요금 정보를 참조하세요.

33.통합에 대한 최종 승인 절차의 일부로 Security Hub 데모 계정에 조사 결과를 제출하려면 어떻게 해야 합니까?

제공된 제품 ARN을 사용하여 Security Hub 데모 계정으로 결과를 보내세요. 리전은 `us-west-2`를 사용합니다. 조사 결과에는 ASFF `AwsAccountId` 필드의 데모 계정 번호가 포함되어야 합니다. 데모 계정 번호를 얻으려면 Security Hub 팀에 문의하세요.

민감한 데이터나 개인 식별 정보는 보내지 마세요. 이 데이터는 공개 데모에 사용됩니다. 이 데이터를 보내면 데모에 사용할 수 있는 권한을 당사에 부여하는 것으로 간주됩니다.

34.**`BatchImportFindings`**는 어떤 오류 또는 성공 메시지를 제공합니까?

Security Hub는 권한 부여에 대한 응답과 `BatchImportFindings`에 대한 응답을 제공합니다. 보다 명확한 성공, 실패 및 오류 메시지는 개발 중입니다.

35.소스 서비스는 어떤 오류 처리를 담당합니까?

소스 서비스는 모든 오류 처리를 담당합니다. 오류 메시지, 재시도, 제한, 알람을 처리해야 합니다. 또한 Security Hub 피드백 메커니즘을 통해 전송된 피드백 또는 오류 메시지도 처리해야 합니다.

36.일반적인 문제의 해결 방법에는 어떤 것이 있습니까?

`AuthorizerConfigurationException`은 잘못된 `AwsAccountId` 또는 `ProductArn`으로 인해 발생합니다.

테스트 시 다음 사항에 유의하세요.

- `AwsAccountId`는 정확히 12자리여야 합니다.
- `ProductArn`은 다음과 같은 형식이어야 합니다. arn:aws:securityhub:*<us-west-2 or us-east-1>*:*<accountId>*:product/*<company-id>*/*<product-id>*

  계정 ID는 Security Hub 팀이 제공한 제품 ARN에 포함된 계정 ID에서 변경되지 않습니다.

잘못된 계정으로 또는 잘못된 계정에서 조사 결과가 전송되었거나 계정에 `ProductSubscription`이 없는 경우 `AccessDeniedException`이 발생합니다. 오류 메시지에는 리소스 유형이 `product` 또는 `product-subscription`인 ARN이 포함됩니다. 이 오류는 계정 간 호출 중에만 발생합니다. `AwsAccountId` 및 `ProductArn`에서 동일한 계정에 대

해 자신의 계정으로 BatchImportFindings를 호출하는 경우 이 작업은 IAM 정책을 사용하며 ProductSubscriptions과는 아무 관련이 없습니다.

사용하는 고객 계정과 제품 계정이 실제 등록된 계정인지 확인하세요. 일부 파트너는 제품 ARN의 제품 계정 번호를 사용했지만 완전히 다른 계정을 사용하여 BatchImportFindings를 호출하려고 시도합니다. 다른 고객 계정이나 심지어 자신의 제품 계정에 대한 ProductSubscriptions을 만드는 경우도 있습니다. 해당 경우에서는 조사 결과를 가져오려고 시도한 고객 계정에 대한 ProductSubscriptions을 만들지 않았습니다.

37. 질문, 의견, 버그는 어디로 보내야 합니까?

    <securityhub-partners@amazon.com>

38. 글로벌 AWS 서비스와 관련된 항목에 대한 조사 결과는 어느 리전으로 보내야 합니까? 예를 들어, IAM 관련 조사 결과는 어디로 보내야 합니까?

    조사 결과가 발견된 동일한 리전으로 조사 결과를 보내세요. IAM과 같은 서비스의 경우, 솔루션에서 여러 리전에서 동일한 IAM 문제를 발견할 수 있습니다. 이 경우, 문제가 발견된 모든 리전으로 조사 결과가 전송됩니다.

    고객이 3개 리전에서 Security Hub를 실행하고 있고 3개 리전 모두에서 동일한 IAM 문제가 감지되었다면 3개 리전 모두에 결과를 보내세요.

    문제가 해결되면 조사 결과에 대한 업데이트를 원래 결과를 보낸 모든 리전으로 보내세요.

파트너 통합 안내서 문서 기록

다음 표는 이 안내서에 대한 문서 변경 사항을 설명합니다.

변경 사항	설명	날짜
콘솔 로고 요구 사항 업데이트	파트너가 Security Hub 콘솔에 표시할 로고의 라이트 모드 및 다크 모드 버전을 모두 제공해야 한다는 것을 명시하기 위해 파트너 매니페스트 및 로고 지침을 업데이트했습니다. 로고는 SVG 형식이어야 합니다.	2021년 5월 10일
새 통합 파트너의 사전 조건 업데이트	Security Hub는 이제 AWS ISV 파트너 경로에 가입하고 AWS 기본 기술 검토(FTR)를 완료한 통합 제품을 사용하는 파트너도 허용합니다. 이전에는 모든 통합 파트너가 AWS Select Tier 파트너여야 했습니다.	2021년 4월 29일
ASFF의 새로운 `FindingProviderFields` 객체	결과를 ASFF에 매핑하는 방법에 대한 정보가 업데이트되었습니다. `Confidence`, `Criticality`, `RelatedFindings`, `Severity`, `Types` 유형의 경우 파트너는 해당 값을 `FindingProviderFields` 의 필드에 매핑합니다.	2021년 3월 18일
결과 작성 및 업데이트에 대한 새로운 원칙	Security Hub에서 새로운 결과를 생성하고 기존 결과를 업데이트하기 위한 새로운 지침이 추가되었습니다.	2020년 12월 4일

본 안내서 최초 공개	이 파트너 통합 안내서는 와의 통합을 설정하는 방법에 대한 정보를 AWS 파트너에게 제공합니다 AWS Security Hub.	2020년 6월 23일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.