파트너 통합 가이드

AWS Security Hub

AWS Security Hub: 파트너 통합 가이드

Table of Contents

타사 통합 개요AWS Security Hub

이 가이드는 다음을 위한 것입니다.AWS파트너 네트워크 (APN) 와 통합을 만들고자 하는 파트너AWS Security Hub.

APN 파트너는 Security Hub와 통합할 수 있습니다.

- Security Hub로 결과 전송
- Security Hub에서 결과 사용
- 둘 다 검색 결과를 Security Hub에서 검색 결과를 보내고 사용합니다.
- Security Hub 관리형 보안 서비스 공급자 (MSSP) 오퍼링의 중심으로 사용
- 에 문의AWSSecurity Hub 배포 및 사용 방법에 대한 고객

이 온보딩 가이드는 Security Hub로 결과를 보내는 파트너에 주로 초점을 맞추고 있습니다.

주제

와 통합하는 이유AWS Security Hub?

AWS Security Hub에서는 Security Hub 계정의 우선순위가 높은 보안 알림과 보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub를 통해 파트너는 보안 검색 결과를 Security Hub에 전송하여 고객이 생성한 보안 결과에 대한 통찰력을 고객에게 제공할 수 있습니다.

Security Hub와의 통합은 다음과 같은 방법으로 가치를 더할 수 있습니다.

- Security Hub 통합을 요청한 고객을 만족시킵니다.
- 고객에게 단일 뷰를 제공합니다.AWSSecurity Finding
- 신규 고객이 특정 유형의 보안 이벤트와 관련된 결과를 제공하는 파트너를 찾을 때 솔루션을 찾을 수 있습니다.

Security Hub와의 통합을 구축하기 전에 통합 이유를 살펴보십시오. 고객이 제품과 Security Hub를 통합하려는 경우 통합이 성공할 가능성이 더 높습니다. 마케팅상의 이유로 또는 신규 고객을 확보하기 위해 통합을 구축할 수 있습니다. 그러나 현재 고객 입력 없이 통합을 빌드하고 고객의 요구 사항을 고려하지 않으면 통합으로 인해 예상되는 결과가 나오지 않을 수 있습니다.

에 결과를 보내려면 준비AWS Security Hub

APN 파트너는 Security Hub 팀에서 검색 서비스 제공업체로 지원할 때까지 고객을 위해 Security Hub 정보를 보낼 수 없습니다. 찾기 제공자로 활성화하려면 다음과 같은 온보딩 단계를 완료해야 합니다. 이렇게 하면 귀하와 귀사의 고객에게 Security Hub가 긍정적인 경험을 제공할 수 있습니다.

온보딩 단계를 완료할 때 의 가이드라인을 따라야 합니다.the section called “결과 생성 및 업데이트에 대한 교리”,the section called “ASFF 매핑 지침”, 및the section called “사용 지침BatchImportFindingsAPI”.

1. 보안 결과 매핑AWSASFF (보안 검색 형식).
2. 통합 아키텍처를 구축하여 결과를 올바른 Regional Security Hub 엔드포인트로 푸시합니다. 이렇게 하려면 검색 결과를 직접 전송할지 여부를 정의합니다.AWS계정 또는 고객 계정 내에서 사용할 수 있습니다.
3. 고객이 자신의 계정에 제품을 구독하도록 합니다. 이를 위해 콘솔이나 콘솔을 사용할 수 있습니다.`EnableImportFindingsForProduct`API 작업 단원을 참조하십시오.제품 통합 관리의AWS Security Hub사용 설명서.

   제품을 구독할 수도 있습니다. 이를 위해 교차 계정 역할을 사용하여`EnableImportFindingsForProduct`고객을 대신하여 API 작업

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

다음 블로그 게시물에서는 Security Hub와의 기존 파트너 통합에 대해 설명합니다.

- 클라우드 관리인 통합 발표AWS Security Hub
- 사용AWS Fargate에 대한 보안 구성 결과를 보내는 ProwlerAWSSecurity Hub
- 가져오기 방법AWS ConfigSecurity Hub에서 결과 로 규칙 평가

검색 결과 수신 준비AWS Security Hub

검색 결과를 수신하려면AWS Security Hub에서 다음 옵션 중 하나를 사용합니다.

- 고객이 모든 검색 결과를 자동으로 보내도록 합니다.CloudWatch이벤트. 고객이 특정 항목을 만들 수 있습니다.CloudWatchSIEM 또는 S3 버킷과 같은 특정 대상에 검색 결과를 전송하는 이벤트 규칙입니다.
- 고객이 Security Hub 콘솔에서 특정 검색 결과 또는 검색 결과 그룹을 선택한 다음 이에 대한 조치를 취하도록 합니다.

예를 들어 고객은 SIEM, 발권 시스템, 채팅 플랫폼 또는 문제 해결 워크플로우로 검색 결과를 보낼 수 있습니다. 이는 고객이 Security Hub 내에서 수행하는 경고 분류 워크플로의 일부입니다.

이를 사용자 지정 작업이라고 합니다. 사용자가 사용자 지정 작업을 수행하면CloudWatch이벤트는 이러한 특정 결과에 대해 생성됩니다. 파트너로서 이 기능을 활용하고 구축할 수 있습니다.CloudWatch 고객이 사용자 지정 작업의 일부로 사용할 이벤트 규칙 또는 대상 이 기능은 특정 유형이나 클래스의 모든 검색 결과를 자동으로 보내지는 않습니다.CloudWatch이벤트. 이 기능은 사용자가 특정 결과에 대해 조치를 취할 수 있도록 합니다.

다음 블로그 게시물에서는 Security Hub와의 통합을 사용하는 솔루션에 대해 설명합니다.CloudWatch 사용자 지정 작업에 대한 이벤트입니다.

- 통합 방법AWS Security Hub의 사용자 지정 작업PagerDuty
- 에서 사용자 지정 작업을 활성화하는 방법AWS Security Hub
- 가져오기 방법AWS ConfigSecurity Hub에서 결과 로 규칙 평가

에 대해 알아보는 리소스AWS Security Hub

다음 자료는 당신이 더 잘 이해하는 데 도움이 될 수 있습니다.AWS Security Hub솔루션 및 방법AWS 고객은 서비스를 사용할 수 있습니다.

- 소개AWS Security Hub비디오
- Security Hub
- Security Hub
- 온보딩 웨비나

또한 사용자 중 하나에서 Security Hub 활성화하는 것이 좋습니다.AWS계정을 만들고 서비스에 대한 실습 경험을 얻으십시오.

파트너 필수 조건

통합을 시작하기 전에AWS Security Hub다음 조건 중 하나를 충족해야 합니다.

- 당신은AWS티어 파트너 이상을 선택합니다.
- 에 가입했습니다.AWSISV 파트너 경로Security Hub 통합에 사용하는 제품이AWS기초 기술 검토 (FTR). 그런 다음 상품에 “검토 완료 자”가 부여됩니다.AWS“배지.

또한 다음과 같은 상호 기밀 유지 계약을 체결해야 합니다.AWS.

통합 사용 사례 및 필수 권한

AWS Security Hub허용합니다AWS고객이 APN 파트너로부터 결과를 수신할 수 있습니다. 파트너의 제품은 고객의 내부 또는 외부에서 실행될 수 있습니다.AWS계정. 고객 계정의 권한 구성은 파트너 제품이 사용하는 모델에 따라 다릅니다.

Security Hub에서 고객은 검색 결과를 고객 계정에 보낼 수 있는 파트너를 항상 제어합니다. 고객은 언제든지 파트너의 권한을 취소할 수 있습니다.

파트너가 보안 검색 결과를 자신의 계정에 보낼 수 있도록 하기 위해 고객은 먼저 Security Hub에서 파트너 제품을 구독합니다. 구독 단계는 아래에 설명된 모든 사용 사례에 필요합니다. 고객이 제품 통합을 관리하는 방법에 대한 자세한 내용은 단원을 참조하십시오.제품 통합 관리의AWS Security Hub사용 설명서.

고객이 파트너 제품을 구독하면 Security Hub에서 관리되는 리소스 정책을 자동으로 생성합니다. 정책은 파트너 제품에 사용 권한을 부여합니다.`BatchImportFindings`고객 계정의 Security Hub로 결과를 보내려면 API 작업입니다.

다음은 Security Hub와 통합되는 파트너 제품의 일반적인 사례입니다. 이 정보에는 각 사용 사례에 필요한 추가 권한이 포함됩니다.

파트너 호스팅: 파트너 계정에서 보낸 결과

이 사용 사례는 자체적으로 제품을 호스팅하는 파트너를 대상으로 합니다.AWS계정. 에 대한 보안 결과를 보내려면AWS고객, 파트너가`BatchImportFindings`파트너 제품 계정에서 API 작업을 수행합니다.

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

파트너 계정에서`BatchImportFindings`API 작업에는 보안 주체가 호출할 수 있도록 허용하는 IAM 정책이 있어야 합니다.`BatchImportFindings`.

Security Hub에서 파트너 제품이 검색 결과를 고객에게 보낼 수 있도록 설정하는 것은 2단계 프로세스입니다.

1. 고객은 Security Hub에서 파트너 제품에 대한 구독을 생성합니다.
2. Security Hub는 고객의 확인과 함께 올바른 관리형 리소스 정책을 생성합니다.

고객 계정과 관련된 보안 결과를 전송하기 위해 파트너 제품은 자체 자격 증명을 사용하여BatchImportFindingsAPI 작업.

다음은 파트너 계정의 보안 주체에 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-1:*:product-subscription/company-
name/product-name"
        }
    ]
}
```

파트너 호스팅: 고객 계정에서 보낸 결과

이 사용 사례는 자체적으로 제품을 호스팅하는 파트너를 대상으로 합니다.AWS계정을 사용하지만 교차 계정 역할을 사용하여 고객의 계정에 액세스합니다. 라고 부릅니다.BatchImportFindings고객 계정에서 API 작업을 수행합니다.

이 사용 사례의 경우BatchImportFindingsAPI 작업 시 파트너 계정은 고객 계정에서 고객 관리형 IAM 역할을 맡습니다.

이 전화는 고객의 계정에서 이루어집니다. 따라서 관리형 리소스 정책은 파트너 제품의 계정에 대한 제품 ARN이 호출에 사용될 수 있도록 허용해야 합니다. Security Hub 관리형 리소스 정책은 파트너 제품 계정 및 파트너 제품 ARN에 대한 권한을 부여합니다. 제품 ARN은 공급자로서 파트너의 고유 식별자입니다. 파트너 제품 계정에서 호출되지 않으므로 고객은 파트너 제품이 검색 결과를 Security Hub에 보낼 수 있는 권한을 명시적으로 부여해야 합니다.

파트너와 고객 계정 간의 교차 계정 역할의 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. 권한을 부여할 때 추가 보안 계층을 제공하는 외부 식별자AWS파트너에 대한 계정 액세스 권한 고유 식별자를 사용하면 파트너가 올바른 고객 계정을 사용할 수 있습니다.

파트너 제품이 교차 계정 역할로 Security Hub에서 고객에게 검색 결과를 보낼 수 있도록 설정하는 작업은 다음 네 단계로 이루어집니다.

1. 고객을 대신하여 작업하는 교차 계정 역할을 사용하는 고객 또는 파트너가 Security Hub에서 제품에 대한 구독을 시작합니다.
2. Security Hub는 고객의 확인과 함께 올바른 관리형 리소스 정책을 생성합니다.
3. 수동으로 또는 사용하여 교차 계정 역할을 구성한 경우AWS CloudFormation. 교차 계정 역할에 대한 자세한 내용은 단원을 참조하십시오.에 액세스 권한 제공AWS타사가 소유한 계정의IAM 사용 설명서.
4. 이 제품은 고객 역할과 외부 ID를 안전하게 저장합니다.

다음으로 제품은 Security Hub로 결과를 보냅니다.

1. 이 제품은AWS Security Token Service(AWS STS) 고객 역할을 맡습니다.
2. 이 제품은`BatchImportFindings`위임된 역할의 임시 자격 증명이 있는 Security Hub 허브에서 API 작업

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"
        }
    ]
}
```

이`Resource`정책의 섹션은 특정 제품 구독을 식별합니다. 이렇게 하면 파트너가 고객이 가입한 파트너 제품에 대한 검색 결과만 보낼 수 있습니다.

고객 호스팅: 고객 계정에서 보낸 결과

이 사용 사례는 고객의 제품에 배포된 파트너를 대상으로 합니다.AWS계정.
이`BatchImportFindings`API는 고객 계정에서 실행되는 솔루션에서 호출됩니다.

이 사용 사례의 경우 파트너 제품에 호출할 수 있는 추가 권한이 부여되어야 합니다.BatchImportFindingsAPI. 이 권한이 부여되는 방식은 파트너 솔루션과 고객 계정에서 구성되는 방식에 따라 다릅니다.

이 접근 방식의 예로는 고객 계정의 EC2 인스턴스에서 실행되는 파트너 제품이 있습니다. 이 EC2 인스턴스에는 EC2 인스턴스 역할이 연결되어 있어야 해당 인스턴스에BatchImportFindingsAPI 작업. 이렇게 하면 EC2 인스턴스가 보안 검색 결과를 고객 계정에 보낼 수 있습니다.

이 사용 사례는 고객이 소유한 제품의 계정에 검색 결과를 로드하는 시나리오와 기능적으로 동일합니다.

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

1. 고객이 파트너 제품을 파트너에 배포합니다.AWS계정 수동 사용AWS CloudFormation또는 다른 배포 도구
2. 고객은 파트너 제품이 검색 결과를 Security Hub로 전송할 때 사용하는 데 필요한 IAM 정책을 정의합니다.
3. 고객은 EC2 인스턴스, 컨테이너 또는 Lambda 함수와 같은 파트너 제품의 필수 구성 요소에 정책을 연결합니다.

이제 Security Hub로 결과를 보낼 수 있습니다.

1. 파트너 제품은AWSSDK 또는AWS CLI를 호출하려면BatchImportFindingsSecurity Hub에서의 API 작업 정책이 연결된 고객 계정의 구성 요소에서 호출합니다.
2. API 호출 중에 필요한 임시 자격 증명이 생성되어BatchImportFindings를 호출합니다.

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 일부로 몇 가지 높은 수준의 단계를 완료할 수 있습니다. 보안 검색 결과를 다음으로 보내기 전에 다음 단계를 완료해야 합니다.AWS Security Hub.

1. APN 파트너 팀 또는 Security Hub 팀과 계약을 시작하고 보안 허브의 파트너가 되는 것에 대한 관심을 표명합니다. Security Hub 통신 채널에 추가할 이메일 주소를 식별합니다.
2. AWS에서는 Security Hub 파트너 온보딩 자료를 제공합니다.
3. Security Hub 파트너 Slack 채널에 초대되어 통합과 관련된 질문을 할 수 있습니다.
4. 검토를 위해 APN 파트너 담당자에게 초안 제품 통합 매니페스트를 제공합니다.

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

   Security Hub 팀에게 Security Hub 콘솔의 파트너 공급자 페이지에 표시되는 정보를 제공합니다. 또한 Security Hub 인사이트 라이브러리에 추가하기 위해 통합과 관련된 새로운 관리형 인사이트를 제안하는 데도 사용됩니다.

   이 초기 버전의 제품 통합 매니페스트에는 전체 세부 정보가 필요하지 않습니다. 그러나 적어도 사용 사례와 데이터세트 정보가 포함되어야 합니다.

   매니페스트 및 필요한 정보에 대한 자세한 내용은 단원을 참조하십시오.제품 통합 매니페스트.
5. Security Hub 팀은 제품에 대한 제품 ARN을 제공합니다. ARN을 사용하여 Security Hub로 결과를 전송합니다.
6. 검색 결과를 Security Hub로 보내거나 검색 결과를 수신하도록 통합을 구축할 수 있습니다.

   결과를 ASFF에 매핑

   검색 결과를 Security Hub로 보내려면 검색 결과를AWSASFF) Security Finding 형식

   ASFF는 서로 공유할 수 있는 결과에 대한 일관된 설명을 제공합니다.AWS보안 서비스, 파트너 및 고객 보안 시스템 이를 통해 통합 작업이 줄어들고 공통 언어를 장려하며 구현자에게 청사진을 제공합니다.

   ASFF는 검색 결과를 보내는 데 사용할 필수 와이어 프로토콜 형식입니다.AWS Security Hub. 결과는 ASFF JSON 스키마 및 RFC-7493 I-JSON 메시지 형식을 준수하는 JSON 문서로 표시됩니다. ASFF 스키마에 대한 자세한 내용은 단원을 참조하십시오.AWSASFF(Security Finding 형식)의AWS Security Hub사용 설명서.

the section called “ASFF 매핑 지침” 섹션을 참조하세요.

통합 구축 및 테스트

다음을 사용하여 통합에 대한 모든 테스트를 완료할 수 있습니다.AWS소유한 계정. 이렇게 하면 검색 결과가 Security Hub에 어떻게 표시되는지 완벽하게 파악할 수 있습니다. 또한 보안 결과에 대한 고객의 경험을 이해하는 데 도움이 됩니다.

이BatchImportFindingsSecurity Hub로 새로운 결과 및 업데이트된 결과를 전송하기 위한 API 작업

Security Hub 통합 구축 전반에 걸쳐,AWS는 APN 파트너 담당자에게 통합 진행 상황에 대한 정보를 계속 알려줄 것을 권장합니다. 또한 APN 파트너 담당자에게 통합 질문에 대한 도움을 요청할 수도 있습니다.

the section called “사용 지침BatchImportFindingsAPI” 섹션을 참조하세요.

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

   통합에 익숙하다면 Security Hub 팀은 앞으로 나아가 공급자로 등록할 수 있는 승인을 제공합니다.
8. 사용자가 제공합니다.AWS검토를 위한 최종 매니페스트가 있습니다.
9. Security Hub 팀은 Security Hub 콘솔에서 제공자 통합을 생성합니다. 그런 다음 고객은 통합을 발견하고 활성화할 수 있습니다.
10. (선택 사항) Security Hub 통합을 홍보하기 위해 추가 마케팅 활동에 참여합니다. Go-to-market활동 섹션을 참조하세요.

    최소한 Security Hub에서는 다음과 같은 자산을 제공하는 것이 좋습니다.
    - 작업 통합의 데모 비디오 (최대 3분). 동영상은 마케팅 목적으로 사용되며AWS YouTube채널.
    - Security Hub 첫 번째 통화 슬라이드 데크에 추가할 수 있는 원 슬라이드 아키텍처 다이어그램입니다.

Go-to-market활동

파트너는 또한 선택적 마케팅 활동에 참여하여 설명하고 홍보할 수 있습니다.AWS Security Hub를 통합

Security Hub와 관련된 자체 마케팅 콘텐츠를 생성하려는 경우 콘텐츠를 릴리스하기 전에 검토 및 승인을 위해 APN 파트너 관리자에게 초안을 보냅니다. 이렇게 하면 모든 사람이 메시징에 맞게 조정됩니다.

AWS파트너 네트워크 (APN) 파트너는 APN 파트너 마케팅 센트럴 및 MDF (시장 개발 기금) 프로그램을 사용하여 캠페인을 만들고 자금 지원을 받을 수 있습니다. 이러한 프로그램에 대한 자세한 내용은 파트너 관리자에게 문의하십시오.

Security Hub 파트너 페이지의 항목

Security Hub 파트너로 승인된 후 솔루션을AWS Security Hub파트너 페이지.

이 페이지에 리스팅하려면 APN 파트너 연락처에 다음 세부 정보를 제공하십시오. 파트너 개발 관리자 (PDM), 파트너 솔루션 설계자 (PSA) 또는 이메일<securityhub-pms@amazon.com>.

- 솔루션에 대한 간략한 설명, Security Hub와의 통합 및 Security Hub와의 통합이 고객에게 제공하는 가치에 대해 설명합니다. 이 설명은 공백을 포함하여 700자로 제한됩니다.
- 솔루션을 설명하는 페이지의 URL입니다. 이 사이트는 귀하의 특정 사이트여야 합니다.AWS통합 및 보다 구체적으로 Security Hub 통합 고객 경험과 고객이 통합을 사용할 때 받는 가치에 중점을 두어야 합니다.
- 600 x 300 픽셀인 로고의 고해상도 복사본입니다. 이 로고의 요구 사항에 대한 자세한 내용은the section called “파트너 페이지 로고”.

보도 자료

승인된 파트너로서 웹 사이트 및 홍보 채널에 보도 자료를 선택적으로 게시할 수 있습니다. 보도 자료는 의 승인을 받아야 합니다.AWS.

보도 자료를 게시하기 전에 다음 주소로 제출해야 합니다.AWSAPN 파트너 마케팅, Security Hub 리더십 및AWS외부 보안 서비스 (ESS). 보도 자료에는 ESS 부사장에 대한 제안된 견적이 포함될 수 있습니다.

이 프로세스를 시작하려면 PDM과 함께 작업하십시오. 당사는 보도 자료를 검토하기 위해 영업일 기준 10일의 서비스 수준 계약 (SLA) 을 보유하고 있습니다.

AWS파트너 네트워크 (APN) 블로그

또한 APN 블로그에 작성한 블로그 항목을 게시하는 데 도움을 줄 수 있습니다. 블로그 항목은 고객 스토리와 사용 사례에 중점을 두어야 합니다. 통합 출시 파트너로만 포지셔닝할 수는 없습니다.

관심이 있으시면 PDM 또는 PSA에 문의하여 프로세스를 시작하십시오. APN 블로그를 최종 승인 및 게시하는 데 8주 이상이 걸릴 수 있습니다.

APN 블로그에 대해 알아야 할 주요 사항

블로그 게시물을 만들 경우 다음 항목에 유의해야 합니다.

블로그 게시물에는 무엇이 들어가나요?

- 파트너 게시물은 교육적이어야 하며 관련 주제에 대한 심층적인 전문 지식을 제공해야 합니다.AWS고객
- 이상적인 길이는 1,500 단어를 넘지 않습니다. 독자는 가능한 것을 가르쳐주는 깊고 교육적인 콘텐츠를 소중히 여깁니다.AWS.
- 콘텐츠는 APN 블로그의 원본이어야 합니다. 기존 블로그 게시물이나 백서와 같은 소스의 콘텐츠의 용도를 변경하지 마십시오.

APN 블로그에 게시할 때 다른 제한은 무엇입니까?

- 어드밴스 또는 프리미어 티어 파트너만 APN 블로그에 게시할 수 있습니다. 서비스 제공과 같이 APN 프로그램 지정이 있는 Select 파트너에는 예외가 있습니다.
- 각 파트너는 매년 세 개의 게시물로 제한됩니다. 수만 개의 APN 파트너와 함께AWS해당 범위에서 공평해야 합니다.
- 각 게시물에는 솔루션 또는 사용 사례를 검증할 수 있는 기술 후원자가 있어야 합니다.

블로그 게시물을 게시하기 전에 편집하는 데 얼마나 걸립니까?

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

APN 블로그를 작성해야 하는 이유는 무엇입니까?

APN 블로그 게시물은 다음과 같은 이점을 제공할 수 있습니다.

- 신뢰성— APN 파트너의 경우, 에 의해 게시된 스토리AWS전 세계 고객에게 영향을 미칠 수 있습니다
- 표시 여부— APN 블로그는 가장 많이 읽은 블로그 중 하나입니다.AWS영향을 받는 트래픽을 포함하여 2019년 1,770만 페이지 조회수를 제공합니다.
- 비즈니스— APN 파트너 게시물에는 APN 고객 참여 (ACE) 프로그램을 통해 잠재 고객을 생성할 수 있는 연결 버튼이 있습니다.

어떤 유형의 콘텐츠가 가장 적합합니까?

다음 유형의 컨텐츠는 APN 블로그 게시물에 가장 적합합니다.

- 테크니컬 콘텐츠는 가장 인기 있는 스토리 유형입니다. 여기에는 솔루션 스포트라이트 및 사용 방법 정보가 포함됩니다. 75% 이상의 독자가 이 기술 콘텐츠를 살펴봅니다.
- 고객은 무언가가 어떻게 작동하는지 보여주는 200급 이상의 스토리를 소중히 여깁니다.AWS또는 APN 파트너가 고객의 비즈니스 문제를 어떻게 해결했는지 확인할 수 있습니다.
- 기술 전문가 또는 주제 전문가가 작성한 게시물은 지금까지 최선을 다합니다.

슬릭 시트 또는 마케팅 시트

매끄러운 시트는 제품, 통합 아키텍처 및 공동 고객 사용 사례를 간략하게 설명하는 한 페이지짜리 문서입니다.

통합을 위한 매끄러운 시트를 만드는 경우 Security Hub 팀에 사본을 보냅니다. 파트너 페이지에 추가됩니다.

백서 또는 eBook

제품, 통합 아키텍처 및 공동 고객 사용 사례를 간략하게 설명하는 백서 또는 eBook을 만드는 경우 Security Hub 팀에 사본을 보냅니다. Security Hub 파트너 페이지에 추가됩니다.

웨비나

통합에 대한 웨비나를 진행하는 경우 웹 세미나 녹화를 Security Hub 팀에 보냅니다. 팀은 파트너 페이지에서 해당 팀으로 연결됩니다.

또한 Security Hub 주제 전문가를 제공하여 웹 세미나에 참여할 수 있습니다.

데모 비디오

마케팅 목적으로 작업 통합에 대한 데모 비디오를 제작할 수 있습니다. 이러한 비디오를 비디오 플랫폼 계정에 게시하면 Security Hub 팀이 파트너 페이지에서 해당 동영상을 링크합니다.

제품 통합 매니페스트

모든AWS Security Hub 통합 파트너는 제안된 통합에 필요한 세부 정보를 제공하는 제품 통합 매니페스트를 작성해야 합니다.

Security Hub 팀은 다음과 같은 여러 가지 방법으로 이 정보를 사용합니다.

- 웹사이트 목록을 만들려면
- Security Hub 콘솔용 제품 카드를 만들려면
- 제품 팀에 사용 사례를 알리기 위해서입니다.

제안된 통합 및 제공된 정보의 품질을 평가하기 위해 Security Hub 팀은 를 사용합니다the section called “제품 준비 체크리스트”. 이 체크리스트는 연동을 시작할 준비가 되었는지 여부를 결정합니다.

제공하는 모든 기술 정보도 문서에 반영되어야 합니다.

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

목차

사용 사례 및 마케팅 정보

다음 사용 사례는 다양한AWS Security Hub 목적으로 구성하는 데 도움이 될 수 있습니다.

공급업체 및 소비자 사용 사례 찾기

독립 소프트웨어 공급업체 (ISV) 에 필요합니다.

와의 통합과 관련된AWS Security Hub 사용 사례를 설명하려면 다음 질문에 답하세요. 결과를 보내거나 받지 않으려는 경우 이 섹션에서 해당 내용을 메모하고 다음 섹션을 완료하십시오.

다음 정보는 문서에 반영되어야 합니다.

- 결과를 보내시겠습니까, 결과를 받으시겠습니까, 아니면 둘 다 보내시겠습니까?
- 조사 결과를 보낼 계획이라면 어떤 유형의 조사 결과를 보내시겠습니까? 모든 조사 결과를 보내시겠습니까, 아니면 조사 결과의 특정 하위 집합을 보내시겠습니까?
- 연구 결과를 받아볼 계획이라면 그 결과를 가지고 무엇을 할 계획입니까? 어떤 유형의 연구 결과를 받게 되나요? 예를 들어 모든 검색 결과, 특정 유형의 결과 또는 고객이 선택한 특정 검색 결과만 받을 수 있습니까?
- 결과를 업데이트할 계획입니까? 그렇다면 어떤 필드를 업데이트하시겠습니까? Security Hub Hub에서는 항상 새 결과를 생성하는 대신 결과를 업데이트할 것을 권장합니다. 기존 결과를 업데이트하면 고객의 검색 결과 잡음을 줄이는 데 도움이 됩니다.

  검색 결과를 업데이트하려면 이미 보낸 검색 결과에 할당된 검색 결과 ID와 함께 검색 결과를 전송합니다.

사용 사례 및 데이터세트에 대한 피드백을 빨리 받으려면 APN 파트너 또는 Security Hub 팀에 문의하십시오.

컨설팅 파트너 (CP) 사용 사례

Security Hub 컨설팅 파트너인 경우 필수입니다.

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

- 고객이 Security Hub 부트스트랩하도록 어떻게 지원합니까? 예를 들어 고객이 전문 서비스, Terraform 모듈 또는AWS CloudFormation 템플릿을 사용하도록 지원한 적이 있습니까?
- 고객이 Security Hub를 운영하고 확장하도록 어떻게 지원합니까? 예를 들어, 대응 또는 문제 해결 템플릿을 제공했거나, 사용자 지정 통합을 구축했거나, 비즈니스 인텔리전스 도구를 사용하여 경영진 대시보드를 설정한 적이 있습니까?

데이터 세트

에서 결과를 전송하는 경우 Security Hub.

Security Hub에 보낼 결과를 보려면 다음 정보를 제공하십시오.

- JSON 또는 XML과 같은 기본 형식의 결과
- 결과를AWS Security Ffding 형식 (ASFF) 으로 변환하는 방법의 예

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

아키텍처

에서 결과를 전송하거나 에서 결과를 받는 경우 Security Hub.

Security Hub 허브와 통합하는 방법을 설명해 주세요. 이 정보는 문서에도 반영되어야 합니다.

아키텍처 다이어그램을 제공해야 합니다. 아키텍처 다이어그램을 준비할 때 다음 항목을 고려하세요.

- 어떤AWS 서비스, 운영 체제 에이전트 등을 사용할 예정입니까?
- 검색 결과를 Security Hub로 보내려면 고객AWS 계정에서 결과를 보내시겠습니까, 아니면 자체 AWS 계정에서 보내시겠습니까?
- 조사 결과를 받게 되면 CloudWatch Events 연동을 어떻게 사용할 계획입니까?
- 결과를 ASFF로 어떻게 변환하시겠습니까?
- 결과를 일괄 처리하고, 결과 상태를 추적하고, 스로틀링 제한을 피하려면 어떻게 해야 할까요?

구성

에서 결과를 전송하거나 에서 결과를 받는 경우 Security Hub.

고객이 Security Hub와의 통합을 구성하는 방법을 설명하십시오.

최소한AWS CloudFormation 템플릿이나 코드 템플릿과 같은 유사한 인프라를 사용해야 합니다. 일부 파트너는 원클릭 통합을 지원하는 사용자 인터페이스를 제공합니다.

구성은 15분 이상 걸리지 않아합니다. 제품 설명서에는 통합을 위한 구성 지침도 제공해야 합니다.

고객당 일일 평균 검색 결과

에서 결과를 전송하는 경우 Security Hub.

고객 기반의 Security Hub에 매달 얼마나 많은 검색 업데이트를 보낼 것으로 예상하십니까 (평균 및 최대)? 몇 배나 되는 추정치를 사용할 수 있습니다.

Latency

에서 결과를 전송하는 경우 Security Hub.

결과를 얼마나 빨리 Security Hub로 보낼 예정입니까? 즉, 제품에서 검색 결과가 생성된 시점부터 Security Hub로 전송될 때까지의 지연 시간은 얼마입니까?

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

회사 및 제품 설명

Security Hub 허브와의 모든 통합에 필요합니다.

Security Hub 통합의 특성에 특히 중점을 두고 회사 및 제품을 간략하게 설명하십시오. 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 하나의 항목으로 통합합니다.

각 설명은 700자를 넘어서는 안 됩니다.

파트너 웹사이트 자산

Security Hub 허브와의 모든 통합에 필요합니다.

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

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

블로그, 웨비나, 데모 비디오 또는 백서와 같은 다른 리소스에 대한 링크를 제공할 수도 있습니다. Security Hub Hub는 파트너 페이지의 링크도 제공합니다.

파트너 페이지 로고

모든 Security Hub 통합에 필요합니다.

Security Hub 파트너 페이지에 표시할 로고 URL을 입력합니다. 로고는 다음 기준을 충족해야 합니다.

- 크기: 600 x 300픽셀
- 크롭: 패딩 없이 타이트하게
- 백그라운드: 투명
- 포맷: PNG

Security Hub 콘솔용 로고

모든 통합에 필요합니다.

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

로고는 다음 기준을 충족해야 합니다.

- 형식: SVG
- 크기: 175 x 40픽셀. 이미지가 더 크면 해당 비율을 사용해야 합니다.
- 크롭: 타이트한 패딩 없음
- 백그라운드: 투명

작은 로고에 대한 자세한 지침은 을 참조하십시오the section called “콘솔 로고 가이드라인”.

유형 찾기

에서 결과를 전송하는 경우 Security Hub.

사용하는 ASFF 형식의 검색 결과 유형과 기본 검색 결과 유형에 맞게 정렬되는 방식을 설명하는 표를 제공하십시오. ASFF에서 유형을 찾는 방법에 대한 자세한 내용은 AWS Security Hub사용 설명서의 ASFF용 유형 분류를 참조하십시오.

제품 설명서에도 이 정보를 포함시키는 것이 좋습니다.

핫라인

Security Hub 허브와의 모든 통합에 필요합니다.

기술 담당자를 위한 이메일 주소와 전화번호 또는 호출기 번호를 제공하십시오. Security Hub Hub는 통합이 더 이상 작동하지 않는 경우와 같은 기술적 문제에 대해 이 담당자와 통신합니다.

또한 심각도가 높은 기술 문제에 대해서는 연중무휴 24시간 연락 창구를 제공합니다.

하트비트 파인딩

에서 결과를 전송하는 경우 Security Hub.

5분마다 Security Hub와의 통합이 제대로 작동하고 있음을 나타내는 “하트비트” 결과를 Security Hub에 보낼 수 있습니까?

가능하면 검색 유형을 사용하여 이 작업을 수행하십시오`Heartbeat`.

AWS Security Hub콘솔 정보

다음 정보가 포함된 JSON 텍스트를 제공합니다.AWS Security Hub Security Hub는 이 정보를 사용하여 제품 ARN을 생성하고, 콘솔에 공급업체 목록을 표시하고, 제안된 관리형 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 다음 필드가 포함됩니다.

필드	필수	설명
`id`	예	회사의 고유 식별자입니다. 회사 식별자는 회사 간에 고유해야 합니다. 이것은 같거나 비슷할 수name 있습니다. 유형: String 최소 길이: 5자 최대 길이: 24자 허용되는 문자: 소문자, 하이픈 및 하이픈 소문자로 시작해야 합니다. 소문자나 숫자로 끝나야 합니다.
`name`	예	Security Hub 콘솔에 표시될 제공자의 회사 이름입니다. 유형: String 최대 길이: 16자
`description`	예	제공자의 회사에 대한 설명이 Security Hub 콘솔에 표시됩니다. 유형: String 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 다음 필드가 포함됩니다.

필드	필수	설명
`IntegrationType`	예	제품에서 검색 결과를 Security Hub로 전송할지, Security Hub에서 결과를 수신할지, 아니면 둘 다 결과를 보내고 받는지를 나타냅니다. 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. 이러한 항목은 회사 내에서 고유해야 합니다. 회사 간에 고유하지 않아도 됩니다. 이것은 아마도 같거나 비슷할name 것입니다. 유형: String 최소 길이: 5자 최대 길이: 24자 허용되는 문자: 소문자, 하이픈 및 하이픈

필드	필수	설명
		소문자로 시작해야 합니다. 소문자나 숫자로 끝나야 합니다.
`regionsNotSupported`	예	다음AWS 지역 중 지원하지 않는 지역은 무엇입니까? 다시 말해, Security Hub가 Security Hub 콘솔의 파트너 페이지에 옵션으로 표시하지 않아야 하는 지역은 어디입니까? 유형: String 지역 코드만 입력하세요. 예: `us-west-1` . 지역 목록은 의 리전 엔드포인트를 참조하십시오 AWS 일반 참조. 의 지역AWS GovCloud (US) 코드는`us-gov-west-1` AWS GovCloud (미국 서부)) 및`us-gov-east-1` AWS GovCloud (미국 동부)) 입니다. 중국 지역의 지역 코드는 (중국`cn-north-1` (베이징)) 및`cn-northwest-1` (중국 (닝샤)) 입니다.

필드	필수	설명
`commercialAccountNumber`	예	해당AWS 지역의 제품에 대한 기본AWS 계정 번호입니다. 검색 결과를 Security Hub로 보내는 경우 제공하는 계정은 검색 결과를 보낸 위치를 기반으로 합니다. • 내AWS 계정에서 이 경우 조사 결과를 제출할 때 사용하는 계좌 번호를 입력하십시오. • 고객AWS 계정에서 이 경우 Security Hub는 통합을 테스트하는 데 사용하는 기본 계정 번호를 제공할 것을 권장합니다. 이상적으로는 모든 지역의 모든 제품에 동일한 계정을 사용하는 것이 좋습니다. 가능하지 않은 경우 Security Hub 팀에 문의하세요. Security Hub로부터 조사 결과만 받는 경우에는 이 계정 번호가 필요하지 않습니다. 유형: String

필드	필수	설명
`govcloudAccountNumber`	아니요	AWS GovCloud (US)지역용 제품의 기본AWS 계정 번호 (제품이 에서 사용 가능한 경우AWS GovCloud (US)). 검색 결과를 Security Hub로 보내는 경우 제공하는 계정은 검색 결과를 보낸 위치를 기반으로 합니다. • 내AWS 계정에서 이 경우 조사 결과를 제출할 때 사용하는 계좌 번호를 입력하십시오. • 고객AWS 계정에서 이 경우 Security Hub는 통합을 테스트하는 데 사용하는 기본 계정 번호를 제공할 것을 권장합니다. 이상적으로는 모든AWS GovCloud (US) 지역의 모든 제품에 동일한 계정을 사용하는 것이 좋습니다. 가능하지 않은 경우 Security Hub 팀에 문의하세요. Security Hub로부터 조사 결과만 받는 경우에는 이 계정 번호가 필요하지 않습니다. 유형: String

필드	필수	설명
`chinaAccountNumber`	아니요	중국 지역용 제품의 기본AWS 계정 번호입니다(중국 지역에서 제품을 사용할 수 있는 경우). 검색 결과를 Security Hub로 보내는 경우 제공하는 계정은 검색 결과를 보낸 위치를 기반으로 합니다. • 내AWS 계정에서 이 경우 조사 결과를 제출할 때 사용하는 계좌 번호를 입력하십시오. • 고객AWS 계정에서 이 경우 Security Hub는 제품 통합을 테스트하는 데 사용하는 기본 계정 번호를 제공할 것을 권장합니다. 이상적으로는 모든 중국 지역의 모든 제품에 동일한 계정을 사용하는 것이 좋습니다. 가능하지 않은 경우 Security Hub 팀에 문의하세요. Security Hub로부터 조사 결과만 받는 경우 중국 지역에서 소유하고 있는 모든 계정일 수 있습니다. 유형: String
`name`	예	Security Hub 콘솔에 표시할 제공자의 제품 이름입니다. 유형: String 최대 길이: 24자
`description`	예	Security Hub 콘솔에 표시할 공급자 제품에 대한 설명입니다. 유형: String 최대 길이: 200자

필드	필수	설명
importType	예	파트너의 리소스 정책 유형 파트너 온보딩 프로세스 중에 다음 리소스 정책 중 하나를 지정하거나 지정할 수 있습니다NEITHER. • 를 사용하면 제품 ARN에 나열된 계정에서만 검색 결과를 Security Hub로 보낼 수 있습니다.BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT • BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT 를 사용하면 구독한 고객 계정에서만 검색 결과를 보낼 수 있습니다. 유형: String 유효한 값: BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT |BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT | NEITHER

필드	필수	설명
`category`	예	상품을 정의하는 카테고리 선택한 항목이 Security Hub 콘솔에 표시됩니다. 최대 세 가지 범주를 선택합니다. 사용자 지정 선택은 허용되지 않습니다. 카테고리가 누락되었다고 생각되면 Security Hub 팀에 문의하세요. 형식: 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	제품AWS Marketplace 목적지의 URL입니다. URL은 Security Hub 콘솔에 표시됩니다. 유형: String AWS MarketplaceURL이어야 합니다. AWS Marketplace리스팅이 없는 경우 이 필드를 비워 둡니다.

필드	필수	설명
`configurationUrl`	예	Security Hub와의 통합에 대한 제품 설명서의 URL입니다. 이 콘텐츠는 웹 사이트 또는 사용자가 관리하는 웹 페이지 (예: GitHub 페이지) 에서 호스팅됩니다. 유형: String 문서에는 다음 정보가 포함되어야 합니다. • 구성 지침 • AWS CloudFormation템플릿 링크 (필요한 경우) • 통합을 위한 사용 사례에 대한 정보 • Latency • ASFFFF매핑 • 결과의 유형 포함 • 아키텍처

지침 및 체크리스트

필요한 자료를 준비 할 때AWS Security Hub통합, 다음 지침을 사용하십시오.

준비 체크리스트는 Security Hub 고객이 Security Hub를 사용할 수 있도록 하기 전에 통합에 대한 최종 검토를 수행하는 데 사용됩니다.

주제

에 표시할 로고에 대한 지침AWS Security Hub콘솔

로고가 표시되는 경우AWS Security Hub콘솔에서 다음 지침을 따릅니다.

밝은 모드 및 다크 모드

라이트 모드와 다크 모드 버전의 로고를 모두 제공해야 합니다.

형식

SVG 파일 형식

Background color(배경색)

Transparent

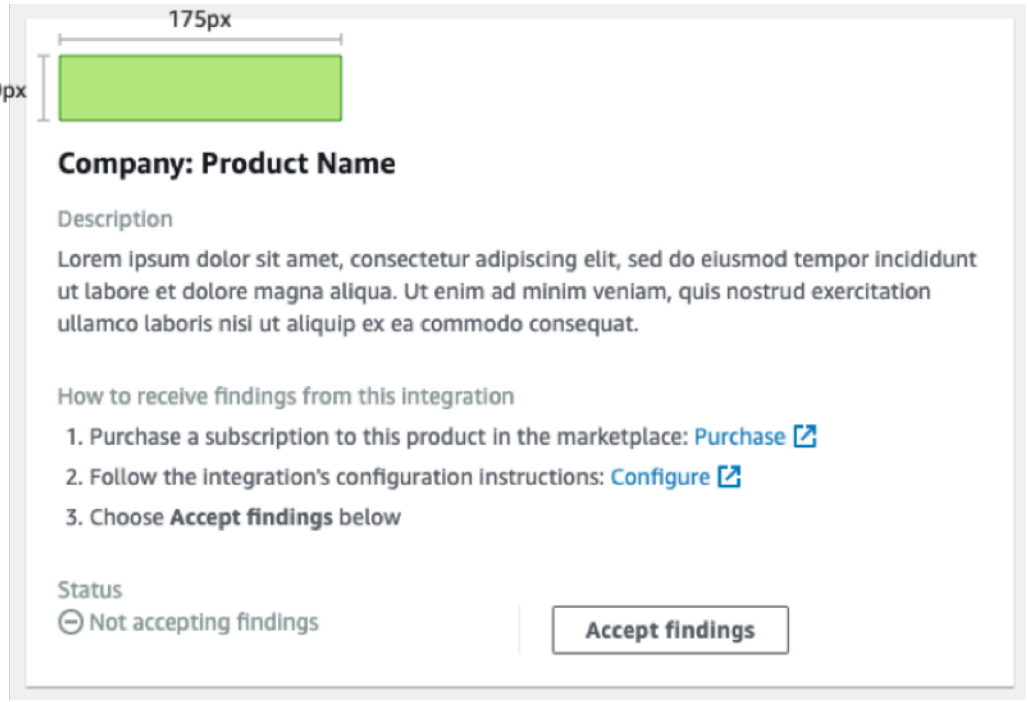
Size

이상적인 비율은 폭 175px x 40px 높이입니다.

최소 높이는 40px입니다.

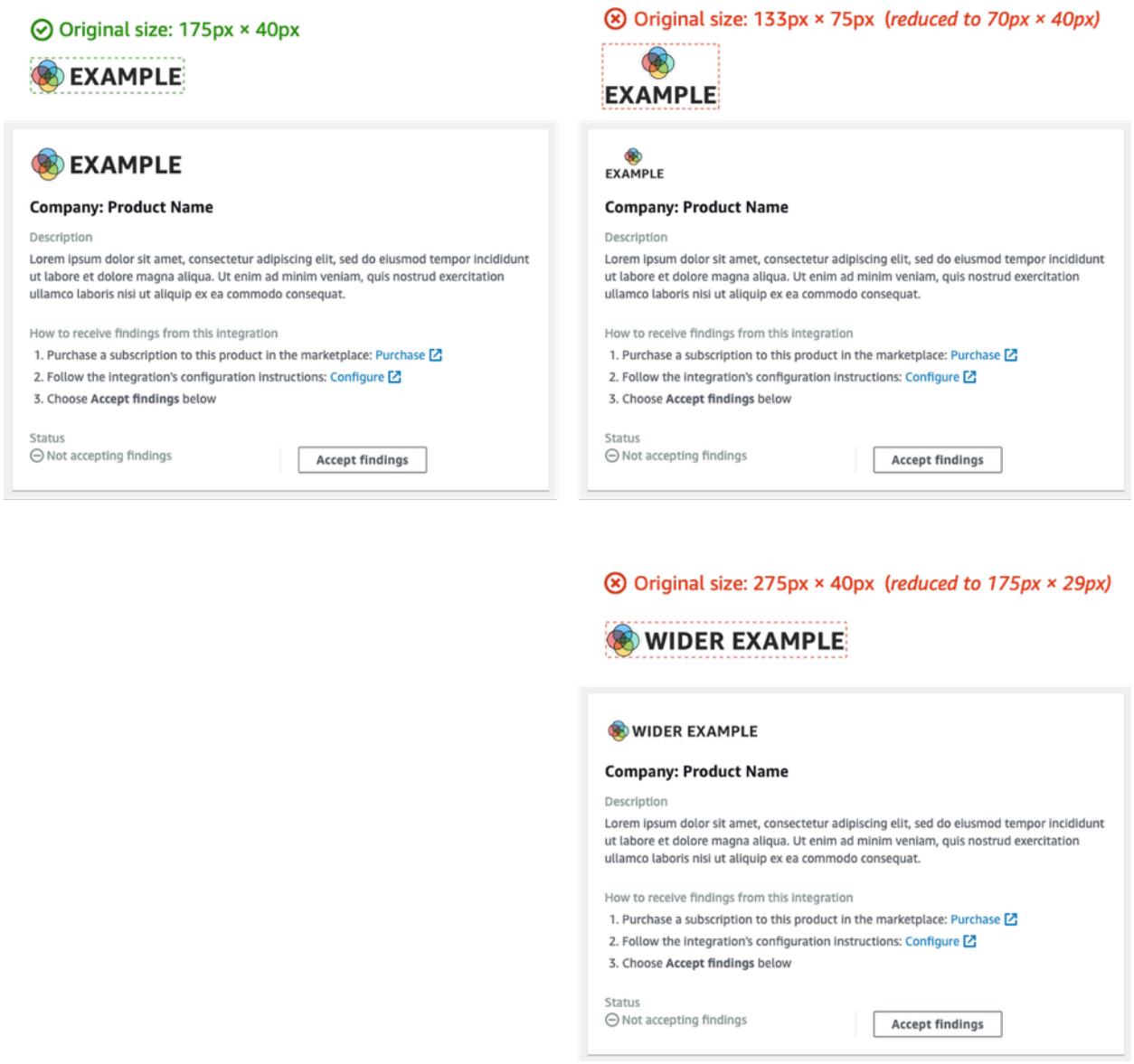
직사각형 로고가 가장 잘 작동합니다.

다음 이미지는 Security Hub 콘솔에 이상적인 로고가 표시되는 방식을 보여줍니다.



로고가 이러한 치수와 일치하지 않으면 Security Hub에서 크기를 최대 높이 40px, 최대 너비는 175px로 축소됩니다. 이는 로고가 Security Hub 콘솔에 표시되는 방식에 영향을 줍니다.

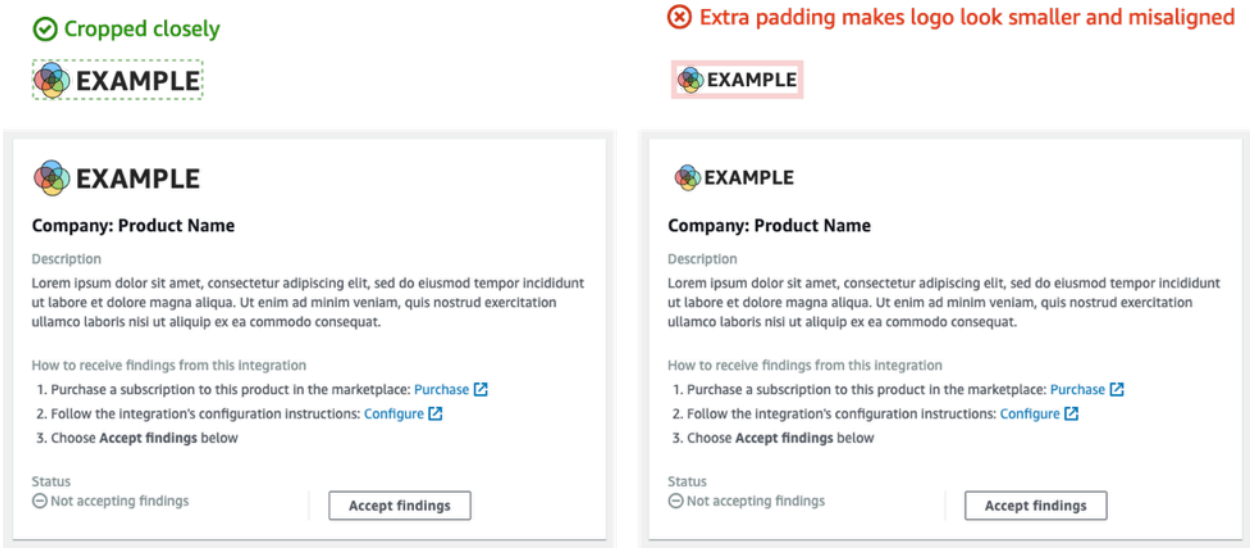
다음 이미지는 이상적인 크기를 사용한 로고의 표시를 넓거나 더 큰 로고와 비교합니다.



자르기

로고 이미지를 최대한 가깝게 자릅니다. 추가 패딩을 제공하는 것이 아닙니다.

다음 이미지는 밀접하게 잘린 로고와 추가 패딩이 있는 로고의 차이점을 보여줍니다.



결과 생성 및 업데이트에 대한 교리

검색 결과를 생성하고 업데이트하는 방법을 계획할 때AWS Security Hub다음 원칙에 유의해야 합니다.

고객이 쉽게 조치를 취할 수 있도록 결과를 구체적으로 지정합니다.

고객은 대응 및 수정 조치를 자동화하고 조사 결과를 다른 결과와 상호 연관시키고자 합니다. 이를 지원하기 위해 결과는 다음과 같은 특징이 있어야 합니다.

- 일반적으로 단일 또는 기본 리소스를 처리해야 합니다.
- 단일 검색 유형을 가져야 합니다.
- 단일 보안 이벤트를 처리해야 합니다.

검색 결과에 여러 보안 이벤트에 대한 데이터가 포함되어 있으면 고객이 검색 결과에 대한 조치를 취하기가 더 어렵습니다.

모든 검색 필드를AWSASFF의 Security Finding 형식 고객이 Security Hub를 신뢰할 수 있는 원천으로 사용할 수 있습니다.

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

고객은 검색 결과의 Security Hub 버전에 모든 데이터가 표시되기를 원합니다. 누락된 데이터는 보안 정보의 중앙 소스로서 Security Hub에 대한 신뢰를 잃게 됩니다.

결과에서 중복성을 최소화합니다. 고객이 볼륨을 찾는 것을 압도하지 마십시오.

Security Hub 일반적인 로그 관리 도구가 아닙니다. 매우 실행 가능한 검색 결과를 Security Hub에 전송해야 하며, 고객이 다른 결과에 직접 응답하거나, 수정하거나, 상호 연관시킬 수 있습니다.

검색 결과에 사소한 변경만 있으면 새 검색 결과를 만드는 대신 검색 결과를 업데이트하십시오.

심각도 점수 또는 리소스 식별자와 같이 검색 결과가 크게 변경되면 새 검색 결과를 만듭니다.

예를 들어 개별 포트 스캔에 대한 검색 결과를 실시간으로 생성하는 것은 매우 실행 가능하지 않습니다. 포트 스캔은 지속적으로 발생할 수 있기 때문에 대량의 결과를 생성합니다. TOR 노드에서 MongoDB 포트에서 포트 스캔에 대한 단일 검색에서 마지막 스캔 시간과 스캔 횟수를 업데이트하는 것이 훨씬 더 매력적이고 정확합니다.

고객이 검색 결과를 사용자 정의하여 보다 의미 있게 만들 수 있습니다.

고객은 특정 검색 필드를 조정하여 환경 또는 요구 사항에 보다 관련성이 높아지기를 원합니다.

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

결과 매핑에 대한 지침AWSASFF(Security Finding 형식)

다음 지침을 사용하여 결과를 ASFF에 매핑합니다. 각 ASFF 필드 및 객체에 대한 자세한 설명은 단원을 참조하십시오.AWSASFF(Security Finding 형식)의AWS Security Hub사용 설명서.

식별 정보

`SchemaVersion`은(는) 항상 `2018-10-08`입니다.

`ProductArn`ARN은 다음과 같습니다.AWS Security Hub사용자에게 할당합니다.

`Id`Security Hub가 검색 결과를 인덱싱하는 데 사용하는 값입니다 다른 검색 결과를 덮어쓰지 않도록 검색 결과 식별자는 고유해야 합니다. 검색 결과를 업데이트하려면 동일한 식별자로 검색 결과를 다시 제출하십시오.

`GeneratorId`다음과 같을 수 있습니다.`Id`또는 Amazon과 같은 개별 논리 단위를 참조할 수 있습니다.GuardDuty감지기 ID,AWS Config레코더 ID 또는 IAM 액세스 분석기 ID입니다.

Title 및 Description

`Title`영향을 받는 리소스에 대한 몇 가지 정보를 포함해야 합니다.`Title`는 공백을 포함하여 256자로 제한됩니다.

더 긴 세부 정보 추가`Description`.`Description`는 공백을 포함하여 1024자로 제한됩니다. 설명에 잘림을 추가하는 것을 고려할 수 있습니다. 다음은 그 예입니다:

```
"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.",
```

찾기 유형

검색 유형 정보를 다음 위치에 제공합니다.`FindingProviderFields.Types`.

`Types`와 일치해야 합니다.ASFF에 대한 유형 분류 체계.

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

타임스탬프

ASFF 형식에는 몇 가지 다른 타임스탬프가 포함되어 있습니다.

`CreatedAt` 및 `UpdatedAt`

제출해야 합니다.`CreatedAt`과`UpdatedAt`전화를 걸 때마다`BatchImportFindings`각 검색 결과에 대해.

값은 파이썬 3.8의 ISO8601 형식과 일치해야 합니다.

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

`FirstObservedAt` 및 `LastObservedAt`

`FirstObservedAt`과`LastObservedAt`시스템에서 검색 결과를 관찰했을 때 일치해야 합니다. 이 정보를 기록하지 않으면 이러한 타임스탬프를 제출할 필요가 없습니다.

값은 파이썬 3.8의 ISO8601 형식과 일치합니다.

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

Severity

심각도 정보를 다음과 같이 제공합니다.`FindingProviderFields.Severity`object에는 다음 필드가 포함됩니다.

`Original`

시스템의 심각도 값입니다.`Original`사용하는 시스템을 수용하기 위해 임의의 문자열이 될 수 있습니다.

`Label`

검색 심각도에 대한 필수 Security Hub 표시기입니다. 허용 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 합니다.

준수를 준수하는 결과는 항상 있어야 합니다.`Label`로 설정`INFORMATIONAL`. 의 예`INFORMATIONAL`결과는 통과한 보안 검사에서 얻은 결과입니다.AWS Firewall Manager수정된 결과.

고객은 보안 운영 팀에 할 일 목록을 제공하기 위해 검색 결과를 심각도에 따라 분류하는 경우가 많습니다. 검색 심각도를 다음과 같이 설정할 때 보수적이어야 합니다.`HIGH`또는`CRITICAL`.

통합 설명서에는 매핑 근거가 포함되어야 합니다.

Remediation

`Remediation`에는 두 가지 요소가 있습니다. 이러한 요소는 Security Hub 콘솔에서 결합됩니다.

`Remediation.Recommendation.Text`의 에 이 나타납니다.문제 해결검색 결과 세부 정보 섹션을 참조하십시오. 이 값은 다음과 같이 하이퍼링크되어 있습니다.`Remediation.Recommendation.Url`.

현재 Security Hub 표준, IAM 액세스 분석기 및 Firewall Manager 검색 결과만 검색 결과를 수정하는 방법에 대한 설명서에 대한 하이퍼링크를 표시합니다.

SourceUrl

사용 전용`SourceUrl`특정 검색 결과를 위해 본체에 딥 링크 URL을 제공할 수 있는 경우 그렇지 않으면 매핑에서 생략합니다.

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

Malware, Network, Process, ThreatIntelIndicators

해당되는 경우 사용`Malware`,`Network`,`Process`또는`ThreatIntelIndicators`. 이러한 각 개체는 Security Hub 콘솔에 노출됩니다. 보내는 검색 결과의 컨텍스트에서 이러한 객체를 사용합니다.

예를 들어 알려진 명령 및 제어 노드에 아웃바운드 연결을 만드는 맬웨어를 탐지하는 경우 EC2 인스턴스에 대한 세부 정보를 다음 위치에 제공합니다.`Resource.Details.AwsEc2Instance`. 관련 항목 제공`Malware`,`Network`, 및`ThreatIntelIndicator`EC2 인스턴스의 객체입니다.

Malware

`Malware`은 최대 5개의 맬웨어 정보 배열을 수용하는 목록입니다. 리소스 및 검색 결과와 관련된 맬웨어 항목을 만듭니다.

각 항목에는 다음 필드가 포함됩니다.

`Name`

맬웨어의 이름입니다. 값은 최대 64자의 문자열입니다.

`Name`심사된 위협 인텔리전스 또는 연구원 출처에서 온 것이어야 합니다.

`Path`

맬웨어에 대한 경로입니다. 값은 최대 512자의 문자열입니다.`Path`다음과 같은 경우를 제외하고 Linux 또는 Windows 시스템 파일 경로여야 합니다.

- S3 버킷 또는 EFS 공유의 객체를 YARA 규칙과 비교하여 스캔하는 경우`Path`는 S3://또는 HTTPS 객체 경로입니다.
- Git 저장소에서 파일을 스캔하는 경우`Path`는 Git URL 또는 복제 경로입니다.

`State`

맬웨어의 상태입니다. 허용 값은 다음과 같습니다.`OBSERVED`| `REMOVAL_FAILED`|`REMOVED`.

검색 제목과 설명에서 맬웨어에 발생한 상황에 대한 컨텍스트를 제공해야 합니다.

예::Malware.State입니다REMOVED그러면 검색 제목 및 설명에 상품이 경로에 있는 맬웨어를 제거했음을 반영해야 합니다.

다음의 경우,Malware.State입니다OBSERVED그러면 검색 제목 및 설명에 제품에 경로에 있는 이 맬웨어가 발견되었음을 반영해야 합니다.

Type

맬웨어의 유형을 나타냅니다. 허용 값은 다음과 같습니다.ADWARE|BLENDED_THREAT|BOTNET_AGENT|COIN_MINER|EXPLOIT_KIT|KEYLOGGER|MACRO|POTENT

다음에 대한 추가 가치가 필요한 경우TypeSecurity Hub 팀에 문의하십시오.

Network

Network단일 객체입니다. 네트워크 관련 세부 정보를 여러 개 추가할 수 없습니다. 필드를 매핑할 때 다음 지침을 따릅니다.

대상 및 소스 정보

대상 및 소스는 TCP 또는 VPC 흐름 로그 또는 WAF 로그를 쉽게 매핑할 수 있습니다. 그들은 당신이 공격에 대한 발견에 대한 네트워크 정보를 설명 할 때 사용하기가 더 어렵습니다.

일반적으로 소스는 공격이 시작된 곳이지만 아래에 나열된 다른 출처가 있을 수 있습니다. 문서의 출처를 설명하고 검색 제목 및 설명에도 설명해야 합니다.

- EC2 인스턴스에 대한 DDoS 공격의 경우 소스가 공격자이지만 실제 DDoS 공격은 수백만 개의 호스트를 사용할 수 있습니다. 대상은 EC2 인스턴스의 퍼블릭 IPv4 주소입니다.DirectionIN입니다.
- EC2 인스턴스에서 알려진 명령 및 제어 노드로 통신하는 것으로 관찰되는 맬웨어의 경우 소스는 EC2 인스턴스의 IPV4 주소입니다. 대상은 명령 및 제어 노드입니다.Direction입니다OUT. 또한 제공 할 것입니다.Malware과ThreatIntelIndicators.

Protocol

Protocol특정 프로토콜을 제공할 수 없는 한 항상 인터넷 할당 번호 기관 (IANA) 등록 이름에 매핑됩니다. 항상 이 옵션을 사용하고 포트 정보를 제공해야 합니다.

Protocol소스 및 대상 정보와는 독립적입니다. 그렇게 하는 것이 합리적일 때만 제공하십시오.

Direction

Direction항상 상대적입니다.AWS네트워크 경계.

- IN입력 중임을 의미합니다.AWS(VPC, 서비스).
- OUT종료 중임을 의미합니다.AWS네트워크 경계.

Process

Process단일 객체입니다. 프로세스 관련 세부 정보는 여러 개 추가할 수 없습니다. 필드를 매핑할 때 다음 지침을 따릅니다.

Name

Name는 실행 파일의 이름과 일치해야 합니다. 최대 64자까지 가능합니다.

Path

Path는 프로세스 실행 파일의 파일 시스템 경로입니다. 최대 512자까지 사용할 수 있습니다.

Pid, **ParentPid**

Pid과ParentPid는 Linux 프로세스 식별자 (PID) 또는 Windows 이벤트 ID와 일치해야 합니다. 차별화하려면 EC2 Amazon 머신 이미지 (AMI) 를 사용하여 정보를 제공합니다. 고객은 아마도 Windows와 Linux를 차별화할 수 있습니다.

타임스탬프 (**LaunchedAt**과**TerminatedAt**)

이 정보를 확실하게 검색할 수 없고 밀리초까지 정확하지 않은 경우 제공하지 마십시오.

고객이 포렌식 조사를 위해 타임스탬프를 사용하는 경우 타임스탬프가 없는 것이 잘못된 타임스탬프를 갖는 것보다 낫습니다.

ThreatIntelIndicators

ThreatIntelIndicators는 최대 5개의 위협 인텔리전스 객체 배열을 허용합니다.

각 항목에 대해Type특정 위협의 맥락에 있습니다. 허용 값은 다음과 같습니다.DOMAIN|EMAIL_ADDRESS|HASH_MD5|HASH_SHA1|HASH_SHA256|HASH_SHA512|IPV4_ADDRESS|IPV6_

다음은 위협 인텔리전스 지표를 매핑하는 방법의 예입니다.

- 코발트 스트라이크와 연관되어 있다는 것을 알고 있는 프로세스를 발견했습니다. 당신은 이것을 다음에서 배웠습니다FireEye의 블로그.

  Type를 PROCESS로 설정합니다. 또한Process프로세스에 대한 객체입니다.
- 메일 필터가 알려진 악성 도메인에서 잘 알려진 해시된 패키지를 보내는 사람을 발견했습니다.

  생성 2개ThreatIntelIndicator객체입니다. 하나의 객체는DOMAIN. 다른 하나는HASH_SHA1.
- 야라 규칙 (로키, 펜리르, Awss3) 으로 멀웨어를 발견했습니다.VirusScan,BinaryAlert).

  생성 2개ThreatIntelIndicator객체입니다. 하나는 맬웨어를 위한 것입니다. 다른 하나는HASH_SHA1.

Resources

용Resources제공된 리소스 유형 및 세부 필드를 사용할 수 있습니다. Security Hub ASFF에 새로운 리소스를 지속적으로 추가하고 있습니다. ASFF 변경 사항에 대한 월별 로그를 받으려면 문의하십시오.<securityhub-partners@amazon.com>.

모델링된 리소스 유형에 대한 세부 정보 필드에 정보를 맞출 수 없는 경우 나머지 세부 정보를Details.Other.

ASFF에서 모델링되지 않은 리소스의 경우Type에Other. 자세한 내용은 단원을 참조하십시오.Details.Other.

다음을 사용할 수도 있습니다.Other비-에 대한 리소스 유형AWS결과.

ProductFields

사용 전용ProductFields다른 큐레이션된 필드를 사용할 수 없는 경우Resources또는 다음과 같은 설명 객체ThreatIntelIndicators,Network또는Malware.

사용하는 경우ProductFields이 결정에 대한 엄격한 근거를 제시해야 합니다.

Compliance

사용 전용Compliance조사 결과가 규정 준수와 관련이 있는 경우

Security Hub 사용Compliance컨트롤에 따라 생성 된 결과에 대해 설명합니다.

Firewall Manager 사용Compliance규정 준수와 관련되어 있기 때문에 연구 결과에 대해 설명합니다.

제한된 필드

이러한 필드는 고객이 검색 결과에 대한 조사를 추적하기 위한 것입니다.

이러한 필드 또는 개체에 매핑하지 마십시오.

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

이러한 필드의 경우 에 있는 필드에 매핑합니다.`FindingProviderFields`객체입니다. 최상위 필드에 매핑하지 마십시오.

- `Confidence`— 서비스의 기능이 비슷하거나 검색 결과에 따라 100% 인 경우에만 신뢰도 점수 (0-99) 를 포함하십시오.
- `Criticality`— 중요도 점수 (0-99) 는 검색 결과와 관련된 리소스의 중요성을 표현하기 위한 것입니다.
- `RelatedFindings`— 동일한 리소스 또는 검색 유형 관련 검색 결과를 추적할 수 있는 경우에만 관련 검색 결과를 제공합니다. 관련 검색 결과를 식별하려면 이미 Security Hub에 있는 검색 결과의 검색 결과 식별자를 참조해야 합니다.

사용 지침**`BatchImportFindings`**API

를 사용하는 경우`BatchImportFindings`에 결과를 전송하는 API 연산AWS Security Hub에서 다음 지침을 사용합니다.

- 반드시 전화해야 합니다.`BatchImportFindings`검색 결과와 연결된 계정을 사용합니다. 연결된 계정의 식별자는`AwsAccountId`검색 결과에 대한 속성입니다.
- 가능한 가장 큰 배치를 보냅니다. Security Hub는 배치당 최대 100개의 검색 결과, 검색 결과당 최대 240KB, 배치당 최대 6MB까지 수용할 수 있습니다.
- 스로틀 속도 제한은 리전당 계정당 10 TPS이며, 버스트는 30 TPS입니다.
- 제한 또는 네트워크 문제가 있는 경우 검색 결과 상태를 유지하는 메커니즘을 구현해야 합니다. 또한 검색 결과가 규정 준수 안팎으로 이동함에 따라 검색 결과 업데이트를 제출할 수 있도록 찾기 상태가 필요합니다.

- 문자열의 최대 길이 및 기타 제한 사항에 대한 자세한 내용은 단원을 참조하십시오.AWSASFF(Security Finding 형식)의AWS Security Hub사용 설명서.

제품 준비 체크리스트

이AWS Security HubAPN 파트너 팀은 이 체크리스트를 사용하여 통합을 시작할 준비가 되었는지 확인합니다.

ASFF 매핑

이러한 질문은 검색 결과에 대한 매핑과 관련이 있습니다.AWSASFF의 Security Finding 형식

파트너의 모든 검색 데이터가 ASFF에 매핑되어 있습니까?

모든 연구 결과를 ASFF에 어떤 식으로든 매핑하십시오.

모델링된 리소스 유형과 같은 선별된 필드 사용`Network`,`Malware`또는`ThreatIntelIndicators`.

다른 모든 것을 매핑합니다.`Resource.Details.Other`또는`ProductFields`적절히 말입니다.

파트너가 사용합니까?**`Resource.Details`**필드 (예:**`AwsEc2instance`**,**`AwsS3Bucket`**, 및**`Container`**? 파트너가 사용합니까?**`Resource.Details.Other`**ASFF에서 모델링되지 않은 리소스 세부 정보를 정의하려면?

가능한 경우 EC2 인스턴스, S3 버킷 및 Security Group과 같은 선별된 리소스에 대해 제공된 필드를 검색 결과에 사용합니다.

리소스와 관련된 기타 정보 매핑`Resource.Details.Other`직접 일치가 없는 경우에만

파트너가 값을 다음으로 매핑합니까?**`UserDefinedFields`**?

`UserDefinedFields`는 사용하지 마십시오.

다음과 같이 선별된 다른 필드를 사용하는 것이 좋습니다.`Resource.Details.Other`또는`ProductFields`.

파트너가 정보를 다음과 같이 매핑합니까?**`ProductFields`**다른 ASFF 필드에 매핑 될 수 있습니까?

사용 전용`ProductFields`버전 관리 정보, 제품별 심각도 검색 결과 또는 선별된 필드에 매핑할 수 없는 기타 정보와 같은 제품별 정보`Resources.Details.Other`.

파트너가 자신의 타임스탬프를 가져오나요?**FirstObservedAt**?

이FirstObservedAt타임스탬프는 제품에서 발견 결과가 관찰된 시간을 기록하기 위한 것입니다. 가능한 경우 이 필드를 매핑합니다.

파트너가 업데이트하려는 검색 결과를 제외하고 각 검색 결과 식별자에 대해 생성된 고유 값을 제공합니까?

Security Hub의 모든 검색 결과는 검색 결과 식별자에 색인화됩니다 (Id속성). 이 값은 검색 결과가 실수로 업데이트되지 않도록 항상 고유해야 합니다.

또한 검색 결과를 업데이트하기 위해 찾기 식별자 상태를 유지해야 합니다.

파트너가 결과를 생성기 ID에 매핑하는 값을 제공합니까?

GeneratorID검색 ID와 동일한 값을 가져서는 안 됩니다.

GeneratorID결과를 생성한 항목에 따라 논리적으로 연결할 수 있어야 합니다.

이는 제품 내의 하위 구성 요소 (제품 A - 취약점 대 제품 A - EDR) 이거나 이와 유사한 구성 요소일 수 있습니다.

파트너가 제품과 관련된 방식으로 필요한 검색 유형 네임스페이스를 사용합니까? 파트너가 검색 유형에 권장되는 검색 유형 범주 또는 분류기를 사용합니까?

검색 유형 분류는 제품이 생성하는 검색 결과와 밀접하게 매핑되어야 합니다.

에 설명된 첫 번째 수준 네임스페이스AWS보안 검색 형식이 필요합니다.

두 번째 및 세 번째 수준의 네임스페이스 (범주 또는 분류자) 에 사용자 정의 값을 사용할 수 있습니다.

파트너가 네트워크 흐름 정보를 캡처합니까?**Network**필드 (네트워크 데이터가 있는 경우)

제품이 캡처되는 경우NetFlow정보, 에 매핑Network필드.

파트너 캡처 프로세스 (PID) 정보가**Process**필드 (프로세스 데이터가 있는 경우)

제품이 프로세스 정보를 캡처하는 경우Process필드.

파트너가 맬웨어 정보를 캡처합니까?**Malware**필드 (맬웨어 데이터가 있는 경우)

제품이 맬웨어 정보를 캡처하는 경우Malware필드.

파트너가 위협 인텔리전스 정보를 캡처합니까?**ThreatIntelIndicators**필드 (위협 인텔리전스 데이터가 있는 경우)

제품이 위협 인텔리전스 정보를 캡처하는 경우ThreatIntelIndicators필드.

파트너가 연구 결과에 대한 신뢰 등급을 제공합니까? 그렇다면 이론적 근거가 제공됩니까?

이 필드를 사용할 때마다 설명서와 매니페스트에 이론적 근거를 제공하십시오.

파트너가 검색 결과에서 리소스 ID에 정식 ID 또는 ARN을 사용합니까?

식별 시AWS리소스를 사용하는 것이 가장 좋은 방법은 ARN을 사용하는 것입니다. ARN을 사용할 수 없는 경우 표준 리소스 ID를 사용합니다.

통합 설정 및 기능

이러한 질문은 설정과 관련이 있습니다.day-to-day통합의 기능입니다.

파트너가 다음을 제공합니까?infrastructure-as-codeIAC (Terraform) 와 같은 Security Hub와의 통합을 배포하는 템플릿AWS CloudFormation또는AWS Cloud Development Kit (AWS CDK)?

고객 계정에서 검색 결과를 보내거나 사용할 통합의 경우CloudWatch결과를 소비하는 이벤트, 일부 형태의 IAC 템플릿이 필요합니다.

AWS CloudFormation선호하지만AWS CDK또는 테라폼을 사용할 수도 있습니다.

파트너 제품이 Security Hub와의 통합을 위해 콘솔에 원클릭 설정이 있습니까?

일부 파트너 제품은 제품에 토글 또는 유사한 메커니즘을 사용하여 통합을 활성화합니다. 이렇게 하면 자동으로 리소스와 권한을 프로비저닝할 수 있습니다. 제품 계정에서 검색 결과를 보내는 경우 원클릭 설정이 선호되는 방법입니다.

파트너는 가치에 대한 결과만 보내나요?

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

Security Hub 일반적인 로그 관리 도구가 아닙니다. 가능한 모든 로그를 Security Hub에 보내면 안 됩니다.

파트너가 고객당 하루에 보낼 결과 수와 평균 및 버스트 빈도 (평균 및 버스트) 에 대한 견적을 제공했습니까?

고유한 검색 결과 수는 Security Hub의 부하를 계산하는 데 사용됩니다. 고유 검색 결과는 다른 검색 결과와는 다른 ASFF 매핑이 있는 검색 결과로 정의됩니다.

예를 들어, 하나의 검색 결과만 채워진 경우`ThreatIntelIndicators`다른 하나는 채워져 있습니다.`Resources.Details.AWSEc2Instance`이 두 가지 독특한 발견입니다.

파트너가 4xx 및 5xx 오류를 효과적으로 처리하여 조절되지 않고 모든 결과를 나중에 보낼 수 있습니까?

현재 30—50 TPS 버스트율이 있습니다.BatchImportFindingsAPI 연산. 4xx 또는 5xx 오류가 반환되는 경우 나중에 전체적으로 다시 시도할 수 있도록 실패한 검색 결과의 상태를 유지해야 합니다. 죽은 편지 대기열 또는 다른 대기열을 통해 이 작업을 수행할 수 있습니다.AWSAmazon SNS 또는 Amazon SQS SQS와 같은 메시징 서비스입니다.

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

원래 검색 결과 ID를 덮어써서 검색 결과를 업데이트할 계획이라면 올바른 검색 결과를 위해 올바른 정보가 업데이트되도록 상태를 유지하는 메커니즘이 있어야 합니다.

검색 결과를 제공하는 경우BatchUpdateFindings결과를 업데이트하는 작업. 이 작업은 고객만 사용해야 합니다. 사용자만 사용합니다.BatchUpdateFindings조사 결과를 조사하고 조치를 취할 때.

파트너가 이전에 전송된 성공 결과를 손상시키지 않는 방식으로 재시도를 처리합니까?

오류가 발생한 경우 원래 찾기 ID를 유지하는 메커니즘이 있어야 오류 발생 시 성공적인 검색 결과를 복제하거나 덮어쓰지 않습니다.

파트너가 다음을 호출하여 검색 결과를 업데이트합니까?**BatchImportFindings**기존 검색 결과의 찾기 ID로 작업 하시겠습니까?

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

이BatchUpdateFindings작업은 고객만 사용해야 합니다.

파트너가 다음을 사용하여 검색 결과를 업데이트합니까?**BatchUpdateFindings**API?

조사 결과에 대한 조치를 취하는 경우BatchUpdateFindings특정 필드를 업데이트하는 작업입니다.

파트너가 검색 결과가 생성되는 시점과 제품에서 Security Hub로 전송되는 시간 사이의 지연 시간에 대한 정보를 제공합니까?

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

이 정보는 매니페스트에 필요합니다.

파트너의 아키텍처가 고객 계정에서 검색 결과를 Security Hub로 전송하려는 경우 이를 성공적으로 입증했습니까? 파트너의 아키텍처가 자체 계정에서 검색 결과를 Security Hub로 전송하려는 경우 이를 성공적으로 입증했습니까?

테스트 중에는 제품 ARN에 제공된 계정과 다른 사용자가 소유한 계정에서 검색 결과를 성공적으로 보내야 합니다.

제품 ARN 소유자의 계정에서 검색 결과를 보내면 API 작업의 특정 오류 예외를 우회할 수 있습니다.

파트너가 Security Hub 하트비트 검색 결과를 제공합니까?

통합이 올바르게 작동하고 있음을 표시하려면 하트비트 검색 결과를 보내야 합니다. 하트비트 검색 결과는 5분마다 전송되며 검색 유형 사용`Heartbeat`.

이는 제품 계정에서 검색 결과를 보내는 경우 중요합니다.

테스트 중에 파트너가 Security Hub 제품 팀의 계정과 통합되었습니까?

사전 프로덕션 검증 중에 검색 예제를 Security Hub 제품 팀에 보내야 합니다.AWS계정. 이 예제에서는 검색 결과가 올바르게 전송 및 매핑되었음을 보여 줍니다.

설명서

이러한 질문은 사용자가 제공하는 통합 문서와 관련이 있습니다.

파트너가 전용 웹 사이트에서 문서를 호스팅합니까?

문서는 웹 사이트에서 정적 웹 페이지, 위키, 문서 읽기 또는 기타 전용 형식으로 호스팅되어야 합니다.

호스팅 설명서GitHub전용 웹 사이트 요구 사항을 충족하지 않습니다.

파트너 설명서에서 Security Hub 통합을 설정하는 방법에 대한 지침을 제공합니까?

iAC 템플릿 또는 콘솔 기반 “원클릭” 통합을 사용하여 통합을 설정할 수 있습니다.

파트너 설명서에 사용 사례에 대한 설명이 제공됩니까?

매니페스트에서 제공하는 사용 사례는 설명서에 설명되어 있어야 합니다.

파트너 설명서에서 전송한 결과에 대한 근거를 제공합니까?

보내는 검색 결과 유형에 대한 근거를 제공해야 합니다.

예를 들어 제품에서 취약점, 맬웨어 및 바이러스 백신에 대한 검색 결과를 생성할 수 있지만 취약성 및 맬웨어 검색 결과는 Security Hub에만 보냅니다. 이 경우 바이러스 백신 검색 결과를 보내지 않는 이유에 대한 근거를 제공해야 합니다.

파트너 문서는 파트너가 연구 결과를 ASFF에 매핑하는 방법에 대한 근거를 제공합니까?

ASFF에 대한 제품의 기본 검색 결과를 매핑하는 데 대한 근거를 제공해야 합니다. 고객은 특정 제품 정보를 찾을 위치를 알고 싶어합니다.

파트너 설명서는 파트너가 검색 결과를 업데이트하는 경우 결과를 업데이트하는 방법에 대한 지침을 제공합니까?

상태를 유지하고, 멱등성을 보장하며, 결과를 덮어쓰는 방법에 대한 정보를 고객에게 제공합니다.up-to-date정보.

파트너 설명서에서 지연 시간 찾기에 대해 설명합니까?

지연 시간을 최소화하여 고객이 Security Hub에서 가능한 한 빨리 결과를 확인할 수 있습니다.

이 정보는 매니페스트에 필요합니다.

파트너 설명서에서 심각도 점수가 ASFF 심각도 점수에 어떻게 매핑되는지 설명합니까?

지도 방법에 대한 정보 제공`Severity.Original`에`Severity.Label`.

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

파트너 문서가 신뢰 등급에 대한 근거를 제공합니까?

신뢰 점수를 제공하는 경우 이 점수는 순위가 매겨져야 합니다.

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

파트너 설명서에 파트너가 지원하는 지역과 지원하지 않는 지역에 기록되어 있습니까?

참고 고객이 통합을 시도하지 않을 리전을 알 수 있도록 지원되거나 지원되지 않는 리전입니다.

제품 카드 정보

이러한 질문은 다음에 표시된 제품의 카드와 관련이 있습니다.통합Security Hub 콘솔의 페이지입니다.

가 제공됩니까?AWS계정 ID가 유효하며 12자리 숫자를 포함합니까?

계정 식별자는 12자리 숫자입니다. 계정 ID에 12자리 미만이 포함된 경우 제품 ARN은 유효하지 않습니다.

상품 설명에 200자 이하의 문자가 포함되어 있습니까?

매니페스트 내의 JSON에 제공된 제품 설명은 공백을 포함하여 200자 이하여야 합니다.

구성 링크가 통합에 대한 설명서로 연결됩니까?

구성 링크는 온라인 설명서로 연결되어야 합니다. 기본 웹 사이트 또는 마케팅 페이지로 연결되어서는 안됩니다.

구매 링크 (제공된 경우) 가AWS Marketplace상품 리스팅이 있습니까?

구매 링크를 제공하는 경우AWS Marketplace입력. Security Hub에서 호스팅하지 않는 구매 링크를 허용하지 않습니다.AWS.

상품 카테고리에 상품이 올바르게 설명되어 있습니까?

매니페스트에서 최대 3개의 제품 범주를 제공할 수 있습니다. JSON과 일치해야 하며 사용자 정의가 될 수 없습니다. 세 개 이상의 상품 카테고리를 제공할 수 없습니다.

회사 및 제품 이름이 유효하고 정확합니까?

회사 이름은 16자 이하여야 합니다.

상품 이름은 24자 이하여야 합니다.

제품 카드 JSON의 제품 이름은 매니페스트의 이름과 일치해야 합니다.

마케팅 정보

이러한 질문은 통합을 위한 마케팅과 관련이 있습니다.

Security Hub 파트너 페이지에 대한 제품 설명이 공백을 포함하여 700자 이내입니까?

Security Hub 파트너 페이지에는 공백을 포함하여 최대 700자만 허용됩니다.

팀에서 더 긴 설명을 편집합니다.

Security Hub 파트너 페이지 로고가 600 x 300px 이하입니까?

회사 로고가 600 x 300픽셀 이하인 PNG 또는 JPG로 공개적으로 액세스할 수 있는 URL을 제공합니다.

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

이자세히 알아보기링크는 파트너의 기본 웹 사이트 또는 문서 정보로 연결되어서는 안 됩니다.

이 링크는 항상 통합에 대한 마케팅 정보가 포함된 전용 웹 페이지로 이동해야 합니다.

파트너가 통합 사용 방법에 대한 데모 또는 교육 비디오를 제공합니까?

데모 또는 통합 연습 비디오 는 선택 사항이지만 권장됩니다.

아님AWS파트너 네트워크 블로그 게시물은 파트너 및 파트너 개발 관리자 또는 파트너 개발 담당자와 함께 공개됩니까?

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

이 게시물은 직접 만든 블로그 게시물과 별개입니다.

4-6 주 리드 타임을 허용합니다. 이러한 노력은 개인 제품 ARN을 사용한 테스트가 완료된 후 시작해야 합니다.

파트너 주도의 보도 자료가 출시되고 있습니까?

파트너 개발 관리자 또는 파트너 개발 담당자와 협력하여 외부 보안 서비스 부사장으로부터 견적을 받을 수 있습니다. 이 견적은 보도 자료에서 사용할 수 있습니다.

파트너 주도의 블로그 게시물이 공개되고 있습니까?

블로그 게시물을 작성하여 외부 통합을 선보일 수 있습니다.AWS파트너 네트워크 블로그.

파트너 주도의 웨비나를 출시하고 있습니까?

자체 웹 세미나를 생성하여 통합을 보여줄 수 있습니다.

Security Hub 팀의 지원이 필요한 경우 개인 제품 ARN을 사용하여 테스트를 완료한 후 제품 팀과 협력하십시오.

파트너가 소셜 미디어 지원을 요청했습니까?AWS?

릴리스 후 다음 작업을 수행할 수 있습니다.AWS보안 마케팅 리드 사용AWS웹 세미나에 대한 세부 정보를 공유하는 공식 소셜 미디어 채널.

AWS Security Hub파트너 FAQ

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

1. Security Hub 통합의 이점은 무엇인가요?
   - 고객 만족도— Security Hub와 통합해야 하는 가장 큰 이유는 고객이 요청하기 때문입니다.

     Security Hub 다음과 같은 보안 및 규정 준수 센터입니다.AWS고객. 첫 번째 정류장으로 설계되었습니다.AWS보안 및 규정 준수 전문가는 매일 보안 및 규정 준수 상태를 파악합니다.

     고객의 말에 귀를 기울입니다. Security Hub에서 검색 결과를 보고 싶은지 여부를 알려줍니다.
   - 검색 기회— Security Hub 콘솔 내에서 인증된 통합을 통해 파트너의 링크를 포함하여 파트너를 홍보합니다.AWS Marketplace리스팅. 이는 고객이 새로운 보안 제품을 발견할 수 있는 좋은 방법입니다.
   - 마케팅 기회— 승인된 통합이 있는 공급업체는 웹 세미나에 참여하고, 보도 자료를 발행하고, 매끄러운 시트를 만들고, 통합 시연을 수행할 수 있습니다.AWS고객.
2. 어떤 유형의 파트너가 있습니까?
   - 결과를 Security Hub로 보내는 파트너
   - Security Hub에서 결과를 받는 파트너
   - 조사 결과를 주고받는 파트너
   - 고객이 자신의 환경에서 Security Hub를 설정, 사용자 지정 및 사용할 수 있도록 지원하는 컨설팅 파트너
3. Security Hub와의 파트너 통합은 어떻게 높은 수준에서 작동합니까?

   고객 계정 내에서 또는 본인의 고객 계정에서 결과를 수집합니다.AWS검색 결과의 형식을 계산하고 변환하십시오.AWSASFF (Security Finding 형식 그런 다음 해당 결과를 적절한 Security Hub 리전 엔드포인트로 푸시합니다

   다음을 사용할 수도 있습니다.CloudWatchSecurity Hub에서 결과를 받는 이벤트.
4. Security Hub와의 통합을 완료하기 위한 기본 단계는 무엇입니까?
   a. 파트너 매니페스트 정보를 제출합니다.
   b. 검색 결과를 보안 허브로 보낼 경우 Security Hub 함께 사용할 제품 ARN을 수신합니다.
   c. 검색 결과를 ASFF에 매핑합니다. the section called “ASFF 매핑 지침” 섹션을 참조하세요.
   d. 검색 결과를 Security Hub에서 수신하고 검색 결과를 수신하기 위한 아키텍처를 정의합니다. 에 설명된 교리를 따르십시오.the section called “결과 생성 및 업데이트에 대한 교리”.

e. 고객을 위한 배포 프레임워크를 만듭니다. 예,AWS CloudFormation스크립트는 이러한 목적을 달성할 수 있습니다.

f. 설정을 문서화하고 고객을 위한 구성 지침을 제공합니다.

g. 고객이 제품과 함께 사용할 수 있는 사용자 지정 인사이트 (상관 관계 규칙) 를 정의합니다.

h. Security Hub 팀과의 통합을 시연합니다.

i. 승인을 위한 마케팅 정보 (웹 사이트 언어, 보도 자료, 아키텍처 슬라이드, 비디오, 매끄러운 시트) 를 제출합니다.

5. 파트너 매니페스트를 제출하는 프로세스는 무엇입니까? 그리고AWS결과를 Security Hub로 보내는 서비스?

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

   7일 이내에 제품 ARN이 발급됩니다.

6. Security Hub에 어떤 유형의 결과를 보내야 합니까?

   Security Hub 요금은 수집된 결과 수를 기준으로 합니다. 따라서 고객에게 가치를 제공하지 않는 검색 결과를 보내지 않아야 합니다.

   예를 들어 일부 취약점 관리 공급업체는 CVSS (공통 취약점 점수 시스템) 점수가 3 이상인 검색 결과만 가능한 10점 중 하나만 보냅니다.

7. Security Hub로 결과를 보낼 수 있는 다른 방법은 무엇입니까?

   주요 접근 방식은 다음과 같습니다.

   - 자신이 지정한 검색 결과에서 결과를 보냅니다.AWS다음을 사용하는 계정BatchImportFindings작업.
   - 고객 계정 내에서 다음을 사용하여 검색 결과를 보냅니다.BatchImportFindings작업. ASSUME 역할 접근법을 사용할 수 있지만 이러한 접근법은 필요하지 않습니다.

   사용에 대한 전반적인 가이드라인BatchImportFindings참조the section called “사용 지침BatchImportFindingsAPI”.

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

   파트너는 솔루션 아키텍처에 크게 의존하기 때문에 이를 위해 다양한 접근 방식을 사용했습니다.

   예를 들어 일부 파트너는 다음과 같이 배포할 수 있는 Python 앱을 빌드합니다.AWS CloudFormation스크립트. 이 스크립트는 고객 환경에서 파트너의 결과를 수집하여 ASFF로 변환한 다음 Security Hub 지역 엔드포인트로 보냅니다.

다른 파트너는 고객에게 클릭 한 번으로 결과를 Security Hub로 푸시할 수 있는 전체 마법사를 구축합니다.

9. Security Hub로 결과를 전송해야 할 시점을 어떻게 알 수 있습니까?

   Security Hub는BatchImportFindingsAPI 작업을 통해 모든 검색 결과를 모든 고객을 위해 Security Hub에 보낼 수 있습니다.

   일부 고객이 아직 Security Hub에 가입하지 않은 경우 Security Hub에서는 이러한 검색 결과를 수집하지 않습니다. 배치에 있는 승인된 결과만 수집합니다.

10. 결과를 고객의 Security Hub 인스턴스에 전송하려면 어떤 단계를 완료해야 합니까?

    a. 올바른 IAM 정책이 적용되었는지 확인합니다.

    b. 계정에 대한 제품 구독 (리소스 정책) 을 활성화합니다. 다음 중 하나를 사용하십시오.EnableImportFindingsForProductAPI 작업 또는통합페이지. 고객이 이 작업을 수행하거나 교차 계정 역할을 사용하여 고객을 대신할 수 있습니다.

    c. 다음을 확인하십시오.`ProductArn`제품 공개 ARN은 발견 중 하나입니다.

    d. 다음을 확인하십시오.`AwsAccountId`검색 결과 중 고객의 계정 ID입니다.

    e. 결과에 따라 잘못된 형식의 데이터가 없는지 확인하십시오.AWSASFF (Security Finding 형식 예를 들어 필수 필드가 채워지고 잘못된 값이 없습니다.

    f. 검색 결과를 올바른 Regional 엔드포인트로 일괄 전송합니다.

11. 검색 결과를 보내려면 어떤 IAM 권한이 있어야 합니까?

    호출하는 IAM 사용자 또는 역할에 대해 IAM 정책을 구성해야 합니다.BatchImportFindings또는 다른 API 호출.

    가장 쉬운 테스트는 관리자 계정에서 수행하는 것입니다. 이를 다음과 같이 제한할 수 있습니다.`action: 'securityhub:BatchImportFindings'`과`resource: <productArn and/or productSubscriptionArn>`.

    리소스 정책을 요구하지 않고 동일한 계정의 리소스를 IAM 정책으로 구성할 수 있습니다.

    호출자의 IAM 정책 문제를 배제하려면BatchImportFindings에서 호출자에 대한 IAM 정책을 다음과 같이 설정합니다.

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

```
}
```

없는지 확인하십시오.Deny호출자에 대한 정책. 이 작업을 수행한 후 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 제품에서 결과를 받으려면 고객 (또는 고객을 대신하여 작동하는 교차 계정 역할이 있는 파트너) 이 제품 구독을 설정해야 합니다. 콘솔에서 이 작업을 수행하려면통합페이지. API에서 이 작업을 수행하려면EnableImportFindingsForProductAPI 연산.

제품 구독은 파트너의 결과를 고객이 수신하거나 보낼 수 있도록 권한을 부여하는 리소스 정책을 생성합니다. 자세한 내용은 사용 사례 및 권한 섹션을 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 요청할 수 있습니다.

다음으로 바꿉니다.BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT를 선택하면 제품 ARN에 나열된 계정에서만 검색 결과를 Security Hub로 보낼 수 있습니다.

다음으로 바꿉니다.BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT을 (를) 구독한 고객 계정에서만 검색 결과를 보낼 수 있습니다.

13고객이 관리자 계정을 만들고 몇 개의 구성원 계정을 추가했다고 가정합니다. 고객이 각 회원 계정을 구독해야 합니까? 또는 고객이 관리자 계정에서만 구독하고 모든 구성원 계정의 리소스에 대해 검색 결과를 보낼 수 있습니까?

이 질문은 관리자 계정 등록을 기반으로 모든 구성원 계정에 대한 권한이 생성되는지 여부를 묻습니다.

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

14. 내 제품 ARN이란 무엇입니까?

제품 ARN은 Security Hub가 사용자를 위해 생성하고 검색 결과를 제출하는 데 사용하는 고유 식별자입니다. Security Hub 허브와 통합하는 각 제품에 대한 제품 ARN을 받게 됩니다. 올바른 제품 ARN은 Security Hub로 보내는 모든 검색 결과의 일부여야 합니다. 제품 ARN이 없는 결과는 삭제됩니다. 제품 ARN은 다음 형식을 사용합니다.

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

예를 들면, 다음과 같이 지정합니다.

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

Security Hub 배포된 각 리전에 대해 제품 ARN이 제공됩니다. 계정 ID, 회사 및 제품 이름은 파트너 매니페스트 제출물에 의해 결정됩니다. 지역 코드를 제외하고 제품 ARN과 연결된 정보는 절대 변경하지 않습니다. 지역 코드는 검색 결과를 제출하는 지역과 일치해야 합니다.

일반적인 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 잠겨 있습니다.

Security Hub가 새 리전에서 시작되면 표준 리전 코드를 사용하여 해당 리전에 대한 제품 ARN을 생성합니다.

또한 모든 계정에는 비공개 제품 ARN이 자동으로 프로비저닝됩니다. 공식 공개 제품 ARN을 받기 전에 이 ARN을 사용하여 자체 개발 계정 내에서 검색 결과 가져오기를 테스트할 수 있습니다.

15. Security Hub로 결과를 전송하려면 어떤 형식을 사용해야 합니까?

결과는 다음 위치에 제공되어야 합니다.AWSASFF (Security Finding 형식 자세한 내용은 단원을 참조하십시오.AWSASFF(Security Finding 형식)의AWS Security Hub사용 설명서.

기본 발견의 모든 정보가 ASFF에 완전히 반영된다는 기대가 있습니다. 사용자 정의 필드`ProductFields`과`Resource.Details.Other`미리 정의된 필드에 깔끔하게 맞지 않는 데이터를 매핑할 수 있습니다.

16.사용할 올바른 리전 엔드포인트는 무엇입니까?

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

17.리전별 엔드포인트 목록은 어디에서 찾을 수 있습니까?

단원을 참조하십시오.Security Hub 엔드.

18.리전 간 결과를 제출할 수 있습니까?

Security Hub는 아직 네이티브 결과에 대한 리전 간 제출을 지원하지 않습니다.AWSAmazon과 같은 서비스GuardDuty, Amazon Macie, Amazon Inspector. 고객이 허용하는 경우 Security Hub에서는 다른 리전에서 검색 결과를 제출하지 못하도록 차단하지 않습니다.

이러한 의미에서 어디서나 Regional 엔드포인트를 호출할 수 있으며 ASFF의 리소스 정보가 엔드포인트의 리전과 일치하지 않아도 됩니다. 하지만`ProductArn`엔드포인트의 리전과 일치해야 합니다.

19.결과 일괄 발송을 위한 규칙과 지침은 무엇입니까?

한 번의 호출로 최대 100개의 검색 결과 또는 240KB까지 일괄 처리할 수 있습니다.`BatchImportFindings`. 이 한도까지 가능한 한 많은 결과를 대기열에 올리고 일괄 처리하십시오.

여러 계정의 검색 결과 집합을 일괄 처리할 수 있습니다. 그러나 배치의 계정이 Security Hub에 가입되지 않은 경우 전체 일괄 처리가 실패합니다. 이는 API Gateway 기준 권한 부여 모델의 한계입니다.

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

20.내가 만든 검색 결과에 대한 업데이트를 보낼 수 있습니까?

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

고객은 새로운 결과 및 검색 결과 업데이트에 대해 측정되고 요금이 청구됩니다.

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

예. 고객이 액세스 권한을 부여한 경우BatchUpdateFindingsAPI 작업을 사용하면 해당 작업을 사용하여 특정 필드를 업데이트할 수 있습니다. 이 작업은 고객, SIEM, 티켓 시스템 및 보안 오케스트레이션, 자동화 및 응답 (SOAR) 플랫폼에서 사용할 수 있도록 설계되었습니다.

22.연구 결과는 어떻게 노화됩니까?

Security Hub는 마지막 업데이트 날짜로부터 90일 후에 결과를 만료합니다. 이 시간이 지나면 오래된 결과가 Security Hub 허브에서 제거됩니다.OpenSearch클러스터.

동일한 검색 결과 ID로 검색 결과를 업데이트하고 노화된 경우 Security Hub에 새 검색 결과가 생성됩니다.

고객이 사용할 수 있음CloudWatch검색 결과를 Security Hub에서 이동하는 이벤트입니다. 이렇게 하면 모든 결과를 고객이 선택한 대상에게 보낼 수 있습니다.

일반적으로 Security Hub에서는 90일마다 새 검색 결과를 생성하고 검색 결과를 영원히 업데이트하지 않는 것이 좋습니다.

23.Security Hub 어떤 스로틀을 적용합니까?

Security Hub 스위치GetFindingsAPI 호출 (액세스 결과에 대한 권장 접근 방식이 사용됨)CloudWatch이벤트.

Security Hub는 API Gateway 및 Lambda 호출에 의해 시행되는 것 이상으로 내부 서비스, 파트너 또는 고객에 대해 다른 제한을 구현하지 않습니다.

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

목표는 초기 발견과 연구 결과에 대한 업데이트 모두에 대해 가능한 한 거의 실시간으로 이루어지는 것입니다. 검색 결과를 생성한 후 5분 이내에 Security Hub로 보내야 합니다.

25.Security Hub에서 결과를 받으려면 어떻게 해야 합니까?

결과를 수신하려면 다음 방법 중 하나를 사용합니다.

- 모든 검색 결과가 자동으로CloudWatch이벤트. 고객이 특정 항목을 만들 수 있습니다.CloudWatchSIEM 또는 S3 버킷과 같은 특정 대상에 검색 결과를 전송하는 이벤트 규칙입니다. 이 기능은 기존 기능을 대체했습니다.GetFindingsAPI 연산.
- 사용CloudWatch사용자 지정 작업에 대한 이벤트. Security Hub를 통해 고객은 콘솔 내에서 특정 검색 결과 또는 검색 결과 그룹을 선택하고 이에 대한 조치를 취할 수 있습니다. 예를 들어 검색 결과를 SIEM, 티켓팅 시스템, 채팅 플랫폼 또는 교정 워크플로우로 보낼 수 있습니다. 이는 고객이

Security Hub 내에서 수행하는 경고 분류 워크플로의 일부입니다. 이러한 작업을 사용자 지정 작업이라고 합니다.

사용자가 사용자 지정 작업을 선택하면CloudWatch이벤트는 이러한 특정 결과에 대해 생성됩니다. 이 기능을 활용하고 구축할 수 있습니다.CloudWatch고객이 사용자 지정 작업의 일부로 사용할 이벤트 규칙 및 대상입니다. 이 기능은 특정 유형이나 클래스의 모든 검색 결과를CloudWatch이벤트. 사용자가 특정 결과에 대한 조치를 취하는 것입니다.

다음과 같은 사용자 지정 작업 API 작업을 사용할 수 있습니다.`CreateActionTarget`를 사용하여 상품에 사용 가능한 작업을 자동으로 생성합니다 (예:AWS CloudFormation템플릿). 또한 사용할 수 있습니다.CloudWatch이벤트 규칙 API 연산을 생성하여 대응하는CloudWatch사용자 지정 작업과 연결된 이벤트 규칙입니다. 사용AWS CloudFormation템플릿을 만들 수도 있습니다.CloudWatch모든 검색 결과 또는 특정 특성을 가진 모든 검색 결과를 Security Hub에서 자동으로 수집하기 위한 이벤트 규칙

26.MSSP (관리형 보안 서비스 공급자) 가 Security Hub 파트너가 되기 위한 요구 사항은 무엇입니까?

고객에게 서비스 제공의 일부로 Security Hub가 어떻게 사용되는지 보여 주어야 합니다.

Security Hub 사용에 대해 설명하는 사용자 설명서가 있어야 합니다.

MSSP가 검색 결과 제공자인 경우 검색 결과를 Security Hub에 보내는 방법을 보여 주어야 합니다.

MSSP가 Security Hub 허브에서 검색 결과만 수신하는 경우 최소한AWS CloudFormation템플릿을 적절히 설정합니다.CloudWatch이벤트 규칙.

27.비 MSSP APN 컨설팅 파트너가 Security Hub 파트너가 되기 위한 요구 사항은 무엇입니까?

APN 컨설팅 파트너인 경우 Security Hub 파트너가 될 수 있습니다. 특정 고객이 다음 작업을 수행하는 데 어떻게 도움을 주었는지에 대한 두 가지 비공개 사례 연구를 제출해야 합니다.

- 고객에게 필요한 IAM 권한으로 Security Hub 설정합니다.
- 콘솔의 파트너 페이지에 있는 구성 지침을 사용하여 이미 통합된 ISV (독립 소프트웨어 공급업체) 솔루션을 Security Hub에 연결하는 데 도움이 됩니다.
- 맞춤형 제품 통합을 통해 고객을 지원합니다.
- 고객 요구 사항 및 데이터 세트와 관련된 맞춤형 인사이트를 구축합니다.
- 사용자 지정 작업을 빌드합니다.
- 문제 해결 플레이북을 빌드합니다.
- Security Hub 규정 준수 표준에 부합하는 빠른 시작을 구축하십시오. Security Hub 팀에서 이를 검증해야 합니다.

사례 연구는 공개적으로 공유할 필요가 없습니다.

28.고객과 Security Hub와의 통합을 배포하는 방법에 대한 요구 사항은 무엇입니까?

Security Hub와 파트너 제품 간의 통합 아키텍처는 파트너의 솔루션 운영 방식에 따라 파트너마다 다릅니다. 통합에 대한 설정 프로세스가 15분 이상 걸리지 않도록 해야 합니다.

통합 소프트웨어를 고객에게 배포하는 경우AWS환경, 활용해야 합니다AWS CloudFormation통합을 단순화하기 위한 템플릿 일부 파트너는 원클릭 통합을 만들었으며, 이는 매우 권장됩니다.

29.내 문서 요구 사항은 무엇입니까?

제품 및 Security Hub 간의 통합 및 설정 프로세스를 설명하는 설명서에 대한 링크를 제공해야 합니다.AWS CloudFormation템플릿.

이 설명서에는 ASFF 사용에 대한 정보도 포함되어야 합니다. 특히, 다른 검색 결과에 사용 중인 ASFF 검색 결과 유형을 나열해야 합니다. 기본 인사이트 정의가 있는 경우 여기에 포함시키는 것이 좋습니다.

다른 잠재적 정보를 포함시키는 것이 좋습니다.

- Security Hub 허브와의 통합을 위한 사용 사례
- 전송된 검색 결과의 평균 양
- 통합 아키텍처
- 현재 사용하고 지원하지 않는 리전
- 검색 결과가 생성되는 시점과 Security Hub로 전송되는 시점 사이의 지연 시간
- 검색 결과 업데이트 여부

30.사용자 지정 인사이트란 무엇입니까?

검색 결과에 대한 사용자 지정 인사이트를 정의하는 것이 좋습니다. Insights는 고객이 주의와 조치가 가장 필요한 조사 결과 및 리소스의 우선 순위를 지정하는 데 도움이 되는 경량의 상관 관계 규칙입니다.

Security Hub`CreateInsight`API 연산. 고객 계정의 일부로 고객 계정 내에서 사용자 지정 인사이트를 만들 수 있습니다.AWS CloudFormation템플릿. 이러한 통찰력은 고객의 콘솔에 나타납니다.

31.대시보드 위젯을 제출할 수 있나요?

아니요, 현재는 지원되지 않습니다. 관리된 통찰력만 생성할 수 있습니다.

32.가격 책정 모델은 무엇입니까?

단원을 참조하십시오.Security Hub.

33.통합 최종 승인 프로세스의 일부로 검색 결과를 Security Hub 데모 계정에 제출하려면 어떻게 해야 합니까?

제공된 제품 ARN을 사용하여 검색 결과를 Security Hub 데모 계정으로 전송합니다.us-west-2지역으로. 조사 결과에 데모 계좌 번호가 포함되어야 합니다.AwsAccountIdASFF의 필드입니다. 데모 계좌 번호를 받으려면 Security Hub 팀에 문의하십시오.

민감한 데이터 또는 개인 식별 정보를 보내지 마십시오. 이 데이터는 공개 데모에 사용됩니다. 이 데이터를 보내면 데모에서 데이터를 사용할 수 있는 권한을 부여합니다.

34.오류 또는 성공 메시지는 무엇입니까?**BatchImportFindings**?

Security Hub는 인증에 대한 응답 및 응답을 제공합니다.BatchImportFindings. 더욱 뚜렷한 성공, 실패 및 오류 메시지가 개발 중입니다.

35.소스 서비스가 담당하는 오류 처리는 무엇입니까?

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

36.일반적인 문제에 대한 몇 가지 해결 방법은 무엇입니까?

원래 요청 ping에 대한AuthorizerConfigurationException이 중 하나가 잘못된 형태로 인해 발생합니다.AwsAccountId또는ProductArn.

문제 해결 시 다음 사항에 유의하십시오.

- AwsAccountId정확히 12자리 숫자여야 합니다.
- ProductArn다음 형식이어야 합니다. arn:aw:보안 허브:*<us-west-2 or us-east-1>*:*<accountId>*:제품/*<company-id>*/*<product-id>*

  계정 ID는 Security Hub 팀에서 제공한 제품 ARN에 포함된 ID와 변경되지 않습니다.

AccessDeniedException잘못된 계정으로 또는 잘못된 계정으로 검색 결과가 전송되거나 계정에ProductSubscription. 오류 메시지에는 리소스 유형이 다음과 같은 ARN이 포함됩니다.product또는product-subscription. 이 오류는 교차 계정 호출 중에만 발생합니다. 전화를 걸면BatchImportFindings동일한 계정에 대한 자체 계정AwsAccountId과ProductArn작업은 IAM 정책을 사용하며 와는 관계가 없습니다.ProductSubscriptions.

사용하는 고객 계정과 제품 계정이 실제 등록 계정인지 확인하십시오. 일부 파트너는 제품 ARN의 제품 계정 번호를 사용했지만 완전히 다른 계정을 사용하여 전화를 시도합니다.`BatchImportFindings`. 다른 경우에는`ProductSubscriptions`다른 고객 계정 또는 자체 제품 계정용 그들은 창조하지 않았습니다.`ProductSubscriptions`결과를 가져오려고 시도한 고객 계정에 대한 것입니다.

37. 질문, 의견 및 버그는 어디에서 보내나요?

    `<securityhub-partners@amazon.com>`

38. 글로벌과 관련된 아이템에 대해 검색 결과를 보낼 대상 지역AWS서비스? 예를 들어 IAM 관련 검색 결과는 어디에서 보내야 합니까?

    검색 결과가 검색된 동일한 리전으로 검색 결과를 보냅니다. IAM과 같은 서비스의 경우 솔루션이 여러 리전에서 동일한 IAM 문제를 발견할 수 있습니다. 이 경우 검색 결과는 문제가 감지된 모든 리전으로 전송됩니다.

    고객이 세 리전에서 Security Hub를 실행하고 세 리전 모두에서 동일한 IAM 문제가 감지되면 검색 결과를 세 리전 모두에 보냅니다.

    문제가 해결되면 원래 검색 결과를 보낸 모든 리전으로 검색 결과에 업데이트를 보냅니다.

파트너 통합 가이드 문서 기록

다음 표에서는 이 안내서의 문서 업데이트를 설명합니다.

변경 사항	설명	날짜
콘솔 로고에 대한 요구 사항 업데이트	파트너가 Security Hub 콘솔에 표시할 로고의 라이트 모드 버전과 다크 모드 버전을 모두 제공해야 함을 나타내도록 파트너 매니페스트 및 로고 가이드라인을 업데이트했습니다. 로고는 SVG 형식이어야 합니다.	2021년 5월 10일
새 통합 파트너의 사전 요구 사항을 업데이트했습니다.	이제 Security Hub에 가입한 파트너도 이용할 수 있습니다 AWSISV 파트너 경로 및 다음을 완료한 통합 제품을 사용하는 사용자AWS기초 기술 검토(FTR). 이전에는 모든 통합 파트너가 다음과 같은 조건을 갖추어야 했습니다.AWS티어 파트너를 선택하세요.	2021년 4월 29일
신규FindingProviderFields ASFF의 객체	결과 매핑에 대한 정보를 ASFF로 업데이트했습니다. 에 대한Confidence ,Criticality ,RelatedFindings ,Severity, 및Types, 파트너는 자신의 가치를 다음 필드에 매핑합니다.FindingProviderFields .	2021년 3월 18일
결과 생성 및 업데이트에 대한 새로운 원칙	Security Hub에서 새로운 결과를 생성하고 기존 결과를 업데	2020년 12월 4일

	이트하기 위한 새로운 지침을 추가했습니다.	
이 가이드의 최초 릴리스	이것은파트너 통합 가이드에서 제공합니다AWS통합 구축 방법에 대한 정보를 제공하는 파트너AWS Security Hub.	2020년 6월 23일

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