사용자 가이드

AWS Security Hub

AWS Security Hub: 사용자 가이드

Table of Contents

AWS Security Hub란 무엇입니까?

AWS Security Hub에서는 AWS에서 보안 상태를 포괄적으로 파악할 수 있으며 보안 업계 표준 및 모범 사례와 비교하여 AWS 환경을 확인할 수 있습니다.

Security Hub는 AWS 계정, AWS 서비스 및 지원되는 서드 파티 제품에서 보안 데이터를 수집하여 보안 추세를 분석하고 우선순위가 가장 높은 보안 문제를 파악하는 데 도움을 줍니다.

조직의 보안 상태를 관리하는 데 도움이 되도록 Security Hub는 여러 보안 표준을 지원합니다. 여기에는 AWS에서 개발한 AWS 기본 보안 모범 사례(FSBP) 표준과 인터넷 보안 센터(CIS), 결제 카드 산업 데이터 보안 표준(PCI DSS), 미국 국립표준기술연구소(NIST) 등의 외부 규정 준수 프레임워크가 포함됩니다. 각 표준에는 몇 가지 보안 제어 기능이 포함되며, 각각의 보안 제어 기능은 보안 모범 사례를 나타냅니다. Security Hub는 보안 제어 기능에 대한 검사를 실행하고 제어 기능에 대한 조사 결과를 생성하여 보안 모범 사례에 대한 규정 준수를 평가하는 데 도움을 드립니다.

Security Hub는 제어 결과를 생성하는 것 외에도 Amazon, Amazon Inspector GuardDuty, Amazon Macie와 AWS 서비스 같은 다른 제품과 지원되는 타사 제품으로부터도 조사 결과를 수신합니다. 이를 통해 사용자는 다양한 보안 관련 문제를 한 눈에 파악할 수 있습니다. Security Hub의 조사 결과를 기타 AWS 서비스 및 지원되는 타사 제품에도 보낼 수 있습니다.

Security Hub는 보안 문제를 분류하고 해결하는 데 도움이 되는 자동화 기능을 제공합니다. 예를 들어, 보안 검사에 실패할 경우 자동화 규칙을 사용하여 중요한 조사 결과를 자동으로 업데이트할 수 있습니다. 또한 Amazon과의 통합을 활용하여 특정 결과에 대한 자동 응답을 EventBridge 트리거할 수 있습니다.

주제

Security Hub의 이점

Security Hub가 사용자의 AWS 환경 전반에서 규정 준수 및 보안 상태를 모니터링하는 데 도움을 주는 몇 가지 주요 방법은 다음과 같습니다.

결과 수집 및 우선 순위 지정에 대한 노력 감소

Security Hub는 통합 AWS 서비스 및 AWS 파트너 제품의 계정 전반에서 보안 결과를 수집하고 우선순위를 지정하려는 노력을 줄여줍니다. Security Hub는 표준 조사 결과 형식인 AWS Security Finding Format(ASFF)을 사용하여 조사 결과 데이터를 처리합니다. 이렇게 하면 무수히 많은 소스에서 나온 조사 결과를 여러 형식으로 관리할 필요가 없습니다. Security Hub는 또한 가장 중요한 결과를 우선순위로 지정할 수 있도록 공급자 간 결과를 상호 연관시킵니다.

모범 사례 및 표준에 대한 자동 보안 검사

Security Hub에서는 AWS 모범 사례 및 업계 표준을 기반으로 연속적인 계정 수준 구성 및 보안 검사를 자동으로 실행합니다. Security Hub는 이러한 검사 결과를 사용하여 보안 점수를 계산하고 주의가 필요한 특정 계정과 리소스를 파악합니다.

여러 계정 및 공급자의 결과 통합 보기

Security Hub는 계정 및 공급자 제품 전반에 걸친 보안 탐지 결과를 통합하여 Security Hub 콘솔에 결과를 표시합니다. Security Hub API, AWS CLI 또는 SDK를 통해 조사 결과를 검색할 수도 있습니다. 전반적인 현재 보안 상태를 확인하여 추세를 파악하고 잠재적인 문제를 식별하며 필요한 수정 단계를 수행할 수 있습니다.

조사 결과 업데이트 및 수정 작업을 자동화하는 기능

정의된 기준에 따라 조사 결과를 수정하거나 숨기는 자동화 규칙을 만들 수 있습니다. Security Hub는 아마존과의 통합도 지원합니다 EventBridge. 특정 결과의 수정 작업을 자동화하기 위해 결과가 생성될 때 수행할 사용자 지정 작업을 정의할 수 있습니다. 예를 들어 결과를 티켓팅 시스템 또는 자동 문제 해결 시스템으로 전송하도록 사용자 지정 작업을 구성할 수 있습니다.

Security Hub에 액세스하기

Security Hub는 대부분의 AWS 리전에서 사용할 수 있습니다. 현재 Security Hub를 사용할 수 있는 리전 목록은 AWS 일반 참조의 AWS Security Hub 엔드포인트 및 할당량을 참고하세요. AWS 계정의 AWS 리전을 관리하는 방법에 대한 자세한 내용은 AWS Account Management참조 가이드의 사용자의 계정이 사용할 수 있는 AWS 리전 지정하기를 참조하세요.

각 리전에서는 다음 방법 중 하나를 사용하여 Security Hub에 액세스하여 사용할 수 있습니다.

Security Hub 콘솔

AWS Management Console는 AWS 리소스를 생성하고 관리하는 데 사용할 수 있는 브라우저 기반 인터페이스입니다. 이 콘솔의 일부인 Security Hub 콘솔은 Security Hub 계정, 데이터 및 리소스에

대한 액세스를 제공합니다. Security Hub 콘솔을 사용하여 조사 결과 보기, 자동화 규칙 생성, 집계 영역 생성 등의 Security Hub 작업을 수행할 수 있습니다.

Security Hub API

Security Hub API를 사용하면 프로그래밍 방식으로 Security Hub 계정, 데이터 및 리소스에 액세스할 수 있습니다. API를 사용하면 HTTPS 요청을 Security Hub에 직접 보낼 수 있습니다. API에 대한 자세한 내용은 AWS Security Hub API 참조 섹션을 참조하세요.

AWS CLI

AWS CLI를 사용하여 시스템 명령줄에서 명령을 실행하여 Security Hub 작업을 수행할 수 있습니다. 경우에 따라 명령줄을 사용하는 것이 콘솔을 사용하는 것보다 더 빠르고 편리할 수 있습니다. 작업을 수행하는 스크립트를 작성할 때도 명령줄이 유용합니다. AWS CLI 설치 및 사용에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서를 참조하세요.

AWS SDK

AWS는 다양한 프로그래밍 언어 및 플랫폼(예: Java, Go, Python, C++, .NET)을 위한 라이브러리와 샘플 코드로 구성된 SDK를 제공합니다. SDK는 Security Hub 및 기타 AWS 서비스에 원하는 언어로 편리하게 프로그래밍 방식으로 액세스할 수 있는 기능을 제공합니다. 이는 또한 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. AWS SDK 설치 및 사용에 대한 자세한 내용은 AWS 기반의 도구를 참조하세요.

Important

Security Hub는 사용자가 Security Hub를 활성화한 후에 생성된 결과만 감지하고 통합합니다. Security Hub 를 활성화하기 전에 생성된 보안 결과를 소급하여 감지하고 통합하지 않습니다. Security Hub는 계정에서 Security Hub를 활성화한 리전의 결과만 수신하고 처리합니다. CIS AWS 기반 벤치마크 보안 검사를 완전히 준수하려면 모든 AWS 리전에서 Security Hub를 활성화해야 합니다.

관련 서비스

AWS 환경을 더욱 안전하게 보호하려면 Security Hub와 함께 기타 AWS 서비스를 사용하는 것을 고려해 보세요.

Security Hub 조사 결과를 보내거나 받는 기타 AWS 서비스의 목록은 AWS 서비스AWS Security Hub와의 통합를 참조하세요.

Security Hub는 AWS Config에서 서비스 연결 규칙을 사용하여 대부분의 제어 기능에 대한 보안 검사를 실행합니다. Security Hub가 대부분의 제어 기능에 대한 조사 결과를 생성하려면 AWS Config에서 AWS Config를 활성화하고 리소스를 기록해야 합니다. 자세한 설명은 구성 AWS Config 섹션을 참조하세요.

Security Hub 무료 평가판 및 요금

AWS 계정에서 Security Hub를 처음 활성화할 때 해당 계정이 30일 Security Hub 무료 평가판에 자동으로 등록됩니다.

무료 평가판 사용 중에 Security Hub를 사용하는 경우, AWS Config 항목과 같이 Security Hub가 상호 작용하는 기타 서비스의 사용에 대해 요금이 부과됩니다. Security Hub 보안 표준에 의해서만 활성화되는 AWS Config 규칙에는 요금이 부과되지 않습니다.

무료 평가판 기간이 끝날 때까지는 Security Hub 사용 요금이 청구되지 않습니다.

> **Note**
>
> Security Hub 무료 평가판은 중국(베이징) 리전에서는 지원되지 않습니다.

사용량 세부 정보 및 예상 비용 보기

Security Hub는 Security Hub 사용에 대한 예상 30일 비용을 포함한 사용 정보를 제공합니다. 사용량 세부 정보에는 무료 평가판 사용 잔여 시간이 포함됩니다. 사용량 정보는 무료 평가판 종료 후 Security Hub 비용이 어느 정도 될지 파악하는 데 도움이 될 수 있습니다. 무료 평가판 사용이 종료된 후에도 사용량 정보를 확인할 수 있습니다.

사용량 정보를 표시하려면 (콘솔)

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 사용량을 선택합니다.

추정 월별 비용은 30일 동안 예상되는 결과 및 보안 검사에 대한 사용자 계정의 Security Hub 사용량에 근거하여 계산됩니다.

사용 정보 및 예상 비용은 현재 계정 및 현재 지역에만 해당됩니다. 집계 영역에서 사용량 정보 및 예상 비용에는 연결된 리전이 포함되지 않습니다. 연결된 리전에 대한 자세한 내용은 the section called “크로스 리전 집계 활성화 작동 방법” 섹션을 참조하세요.

요금 내역

수집된 결과 및 보안 검사에 대한 Security Hub 요금의 부과 방법에 대한 자세한 내용은 Security Hub 요금을 참조하세요.

Security Hub 개념

이 항목에서는 서비스를 시작하는 데 도움이 되는 AWS Security Hub의 주요 개념과 용어에 대해 설명합니다.

계정

AWS 리소스가 포함된 표준 Amazon Web Services (AWS) 계정입니다. AWS 계정으로 로그인하고 Security Hub를 활성화할 수 있습니다.

계정은 다른 계정을 초대하여 Security Hub를 활성화하고 Security Hub의 해당 계정에 연결할 수 있습니다. 멤버십 초대 수락은 선택 사항입니다. 초대가 수락되면 계정은 관리자 계정이 되며, 추가된 계정은 멤버 계정이 됩니다. 관리자 계정은 멤버 계정에 있는 조사 결과를 볼 수 있습니다.

에 AWS Organizations등록한 경우 조직은 조직의 Security Hub 관리자 계정을 지정합니다. Security Hub 관리자 계정은 다른 조직 계정을 멤버 계정으로 활성화할 수 있습니다.

한 계정이 관리자 계정이면서 동시에 멤버 계정일 수 없습니다. 계정에는 관리자 계정이 하나만 있을 수 있습니다.

자세한 내용은 관리자 및 구성원 계정 관리 섹션을 참조하십시오.

관리자 계정

관련된 멤버 계정의 조사 결과를 볼 수 있는 액세스 권한이 부여된 Security Hub의 계정입니다.

계정은 다음 방법 중 하나로 관리자 계정이 됩니다.

- 계정이 Security Hub에서 다른 계정에 연결되도록 해당 계정을 초대합니다. 해당 계정이 초대를 수락하면 이 계정이 멤버 계정이 되고 초대한 계정은 이들의 관리자 계정이 됩니다.
- 계정은 조직 관리 계정에 의해 Security Hub 관리자 계정으로 지정됩니다. Security Hub 관리자 계정은 모든 조직 계정을 멤버 계정으로 활성화할 수 있으며 다른 계정을 멤버 계정으로 초대할 수도 있습니다.

계정에는 관리자 계정이 하나만 있을 수 있습니다. 한 계정이 관리자 계정이면서 동시에 멤버 계정일 수 없습니다.

집계 리전

집계 지역을 설정하면 단일 AWS 리전 창에서 여러 보안 결과를 볼 수 있습니다.

집계 리전은 사용자가 조사 결과를 보고 관리하는 리전입니다. 조사 결과는 연결된 리전의 집계 리전에 집계됩니다. 조사 결과 업데이트는 리전 전체에 복제됩니다.

집계 리전에서 보안 표준, 통찰력, 조사 결과 페이지에는 연결된 모든 리전의 데이터가 포함됩니다.

크로스 리전 집계 활성화 섹션을 참조하십시오.

보관된 결과

`RecordState`가 `ARCHIVED`로 설정되어 있는 결과입니다. 조사 결과를 보관하면 조사 결과 공급자가 해당 조사 결과가 더 이상 관련이 없다고 판단한다는 의미입니다. 기록 상태는 조사 결과에 대한 조사 상태를 추적하는 워크플로우 상태와는 별개입니다.

조사 결과 공급자는 Security Hub API의 `BatchImportFindings` 작업을 사용하여 자신이 생성한 조사 결과를 보관할 수 있습니다. Security Hub는 다음 기준 중 하나에 따라 제어 기능이 비활성화되거나 연결된 리소스가 삭제된 경우 제어 기능에 대한 조사 결과를 자동으로 보관합니다.

- 조사 결과는 3~5일 안에는 업데이트되지 않습니다(이는 최선을 다한 결과이며 보장되지는 않는다는 점을 유념하십시오).
- 관련 AWS Config 평가 결과가 반환됩니다`NOT_APPLICABLE`.

기본적으로 보관된 조사 결과는 Security Hub 콘솔에 있는 조사 결과 목록에서 제외됩니다. 보관된 조사 결과를 포함하도록 필터를 업데이트할 수 있습니다.

Security Hub API의 `GetFindings` 작업은 활성 조사 결과와 보관된 조사 결과를 모두 반환합니다. 레코드 상태에 대한 필터를 포함할 수 있습니다.

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS 보안 탐지 형식 (ASFF)

Security Hub에서 집계하거나 생성하는 조사 결과 콘텐츠의 표준화된 형식입니다. AWS 보안 검색 결과 형식을 사용하면 Security Hub를 사용하여 보안 서비스, 타사 솔루션 또는 AWS Security Hub 자체에서 보안 검사를 실행하여 생성된 결과를 보고 분석할 수 있습니다. 자세한 정보는 AWS 보안 검색 형식 (ASFF)을 참조하세요.

컨트롤

정보의 기밀성, 무결성 및 가용성을 보호하고 정의된 보안 요구 사항을 충족하도록 설계된 정보 시스템 또는 조직에 대해 규정된 보호 조치 또는 대책입니다. 보안 표준은 제어 기능의 모음과 연관되어 있습니다.

보안 제어 기능이라는 용어는 표준 전반에서 단일 제어 ID와 제목을 가지고 있는 제어 기능을 말합니다. 표준 제어 기능이라는 용어는 표준별 제어 ID와 제목을 가지고 있는 제어 기능을 말합니다. 현재 Security Hub는 AWS GovCloud (US) Region 및 중국 리전에서는 표준 제어 기능만 지원합니다. 보안 제어 기능은 다른 모든 리전에서 지원됩니다.

사용자 지정 작업

선택한 결과를 보내기 위한 Security Hub EventBridge 메커니즘입니다. 사용자 지정 작업은 Security Hub에서 생성됩니다. 그러면 EventBridge 규칙에 연결됩니다. 이 규칙은 사용자 지정 작업 ID와 연결된 결과가 수신될 때 수행할 특정 작업을 정의합니다. 예를 들어, 사용자 지정 작업을 사용하여 특정 조사 결과 또는 작은 조사 결과 집합을 응답 또는 수정 작업 흐름에 보낼 수 있습니다. 자세한 내용은 the section called “사용자 지정 작업 생성(콘솔)” 섹션을 참조하십시오.

위임된 관리자 계정(조직)

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

Security Hub에서 Security Hub 관리자 계정은 Security Hub의 위임된 관리자 계정이기도 합니다. 조직 관리 계정이 Security Hub 관리자 계정을 처음 지정하면 Security Hub가 조직을 호출하여 해당 계정을 위임된 관리자 계정으로 설정합니다.

그런 다음에는 조직 관리 계정이 모든 리전에서 Security Hub 관리자 계정으로 위임된 관리자 계정을 선택해야 합니다.

결과

보안 점검 또는 보안 관련 감지의 관찰 가능한 기록입니다. Security Hub는 제어 기능에 대한 보안 검사를 완료한 후 조사 결과를 생성합니다. 이를 제어 기능의 조사 결과라고 합니다. 조사 결과는 타사 제품 통합에서도 나올 수 있습니다.

Security Hub의 조사 결과에 대한 자세한 내용은 조사 결과 섹션을 참조하십시오.

> **Note**
>
> 조사 결과는 가장 최근 업데이트 후 90일 또는 업데이트가 없는 경우 생성일 이후 90일에 삭제됩니다. 결과를 90일 이상 저장하려면 결과를 Amazon S3 버킷으로 EventBridge 라우팅하는 규칙을 구성할 수 있습니다.

크로스 리전 집계 활성화

연결된 리전의 조사 결과, 통찰력, 제어 기능 규정 준수 상태, 보안 점수를 집계 리전으로 집계합니다. 그런 다음에는 집계 리전에서 모든 데이터를 보고 집계 리전에서 조사 결과 및 통찰력을 업데이트할 수 있습니다.

크로스 리전 집계 활성화 섹션을 참조하십시오.

조사 결과 수집

다른 AWS 서비스 및 타사 파트너 제공업체로부터 Security Hub로 결과 가져오기

조사 결과 수집 이벤트에는 새로운 조사 결과와 기존의 조사 결과에 대한 업데이트가 모두 포함됩니다.

인사이트

집계 설명 및 선택적 필터로 정의된 관련 조사 결과의 모음입니다. 인사이트는 주의와 개입이 필요한 보안 영역을 식별합니다. Security Hub는 수정할 수 없는 관리된(기본) 몇 가지 통찰력을 제공합니다. 또한 사용자 지정 Security Hub 통찰력을 생성하여 사용자 AWS 환경 및 사용에 따른 고유한 보안 문제를 추적할 수 있습니다. 자세한 정보는 인사이트을 참조하세요.

연결된 리전

크로스 리전 집계를 활성화하면, 연결된 리전은 조사 결과, 통찰력, 제어 기능 규정 준수 상태, 보안 점수를 집계 리전으로 집계하는 리전입니다.

연결된 리전에서 조사 결과 및 통찰력 페이지에는 해당 리전의 조사 결과만 포함됩니다.

크로스 리전 집계 활성화 섹션을 참조하십시오.

멤버 계정

관리자 계정에 조사 결과를 보고 조치를 취할 수 있는 권한을 부여한 계정입니다.

계정은 다음 방법 중 하나로 멤버 계정이 됩니다.

- 이 계정은 다른 계정의 초대를 수락합니다.
- 조직 계정의 경우, Security Hub 관리자 계정이 이 계정을 멤버 계정으로 활성화합니다.

관련 요구 사항

제어에 매핑되는 일련의 업계 또는 규정 요구 사항입니다.

규칙

제어의 준수 여부를 평가하는 데 사용되는 자동화된 기준 세트입니다. 규칙이 평가되면 통과하거나 실패할 수 있습니다. 평가에서 규칙의 통과 여부를 확인할 수 없는 경우 규칙이 경고 상태에 있는 것입니다. 규칙을 평가할 수 없는 경우 사용할 수 없는 상태입니다.

보안 점검

단일 리소스를 기준으로 규칙을 구체적으로 point-in-time 평가하여`PASSED`, `FAILEDWARNING`, 또는 `NOT_AVAILABLE` 상태가 됩니다. 보안 점검을 실행하면 결과가 생성됩니다.

Security Hub 관리자 계정

조직의 Security Hub 멤버십을 관리하는 조직 계정입니다.

조직 관리 계정은 각 리전에 있는 Security Hub 관리자 계정을 지정합니다. 조직 관리 계정은 모든 리전에서 동일한 Security Hub 관리자 계정을 선택해야 합니다.

Security Hub 관리자 계정은 조직에서 Security Hub에 대해 위임된 관리자 계정이기도 합니다.

Security Hub 관리자 계정은 어떤 조직 계정이든 멤버 계정으로 활성화할 수 있습니다. Security Hub 관리자 계정은 다른 계정을 멤버 계정으로 초대할 수도 있습니다.

보안 표준

규정 준수를 위해 충족시키거나 달성해야 하는 특성(일반적으로 측정 가능하고 제어 형식을 취함)을 명시한, 주제에 대해 게시된 진술입니다. 보안 표준은 규제 프레임워크, 모범 사례 또는 사내 정책을 기반으로 할 수 있습니다. 제어 기능은 Security Hub에서 지원되는 하나 이상의 표준과 연결될 수 있습니다. Security Hub의 보안 표준에 대한 자세한 내용은 표준 및 제어 섹션을 참조하십시오.

심각도

Security Hub 제어 기능에 할당된 심각도는 해당 제어 기능의 중요성을 식별합니다. 제어 기능의 심각도는 심각, 높음, 중간, 낮음 또는 정보일 수 있습니다. 제어 기능의 조사 결과에 할당된 심각도는 해당 제어 기능 자체의 심각도와 동일합니다. Security Hub가 제어 기능에 심각도를 할당하는 방법에 대한 자세한 내용은 제어 조사 결과에 심각도 할당을 참고하십시오.

워크플로 상태

결과에 대한 조사의 상태입니다. `Workflow.Status` 속성을 사용하여 추적했습니다.

워크플로우 상태는 초기에 `NEW`입니다. 리소스 소유자에게 결과에 대한 작업을 수행하도록 통지한 경우 워크플로우 상태를 `NOTIFIED`로 설정할 수 있습니다. 결과가 문제가 아니고 작업이 필요하지 않은 경우 워크플로우 상태를 `SUPPRESSED`로 설정합니다. 결과를 검토하고 수정한 후 워크플로우 상태를 `RESOLVED`로 설정합니다.

기본적으로 대부분의 조사 결과 목록에는 워크플로우 상태가 NEW 또는 NOTIFIED인 조사 결과만 포함됩니다. 컨트롤에 대한 조사 결과 목록에는 RESOLVED 조사 결과도 포함됩니다.

GetFindings 작업의 경우 워크플로우 상태에 대한 필터를 포함할 수 있습니다.

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

Security Hub 콘솔은 조사 결과에 대한 워크플로우 상태를 설정하는 옵션을 제공합니다. 고객(또는 고객을 대신해 조사 결과 공급자의 조사 결과를 업데이트하기 위해 작업하는 SIEM, 티켓팅, 인시던트 관리 또는 SOAR 도구)도 BatchUpdateFindings를 사용하여 워크플로우 상태를 업데이트할 수 있습니다.

Security Hub를 활성화하기 전의 권장 사항

다음 권장 사항은 사용을 시작하는 데 도움이 될 수 AWS Security Hub있습니다.

과 AWS Organizations통합

AWS Organizations AWS 관리자는 여러 AWS 계정 조직 단위 (OU) 를 통합하고 중앙에서 관리할 수 있는 글로벌 계정 관리 서비스입니다. 예산, 보안 및 규정 준수 요구 사항을 지원하도록 설계된 계정 관리 및 통합 결제 기능을 제공합니다. 추가 비용 없이 제공되며 Security Hub AWS 서비스 GuardDuty, Amazon 및 Amazon Macie를 포함한 여러 제품과 통합됩니다.

계정 관리를 자동화하고 간소화하려면 Security Hub 및 AWS Organizations를 통합하는 것이 좋습니다. Security Hub를 사용하는 조직이 여러 개 AWS 계정 있는 경우 Organizations와 통합할 수 있습니다.

통합 활성화에 대한 지침은 Security Hub와 통합 AWS Organizations 섹션을 참조하세요.

중앙 구성 사용

Security Hub와 Organizations를 통합하면 중앙 구성이라는 기능을 사용하여 조직의 Security Hub를 설정하고 관리할 수 있습니다. 중앙 구성을 사용하면 관리자가 조직의 보안 적용 범위를 사용자 지정할 수 있으므로 중앙 구성 사용을 권장합니다. 적절한 경우 위임된 관리자는 구성원 계정이 자체 보안 범위 설정을 구성하도록 허용할 수 있습니다.

중앙 구성을 통해 위임된 관리자는 계정, OU 등에 AWS 리전걸쳐 Security Hub를 구성할 수 있습니다. 위임된 관리자는 구성 정책을 만들어 Security Hub를 구성합니다. 구성 정책 내에서 다음 설정을 지정할 수 있습니다.

- Security Hub의 활성화 또는 비활성화 여부
- 활성화 및 비활성화되는 보안 표준
- 활성화 및 비활성화되는 보안 제어
- 일부 제어의 파라미터를 사용자 지정할지 여부

위임된 관리자는 전체 조직에 대한 단일 구성 정책을 만들거나 다양한 계정 및 OU에 대해 서로 다른 구성 정책을 만들 수 있습니다. 예를 들어 테스트 계정과 프로덕션 계정은 서로 다른 구성 정책을 사용할 수 있습니다.

구성 정책을 사용하는 구성원 계정 및 OU는 중앙에서 관리하며 위임된 관리자만 구성할 수 있습니다. 위임된 관리자는 특정 구성원 계정과 OU를 자체 관리형으로 지정하여 구성원이 리전별로 자체 설정을 구성할 수 있도록 할 수 있습니다.

중앙 구성에 대해 자세히 알아보려면 중앙 구성 작동 방식 섹션을 참조하세요.

구성 AWS Config

AWS Security Hub 서비스 연결 AWS Config 규칙을 사용하여 대부분의 컨트롤에 대한 보안 검사를 수행합니다.

이러한 제어를 지원하려면 AWS 리전 Security Hub가 활성화된 각 계정의 모든 계정 (관리자 계정과 구성원 계정 모두) 에서 AWS Config 활성화해야 합니다. 또한 각 활성화된 표준에 대해 제어를 활성화하는 데 필요한 리소스를 기록하도록 AWS Config 구성해야 합니다.

Security Hub 표준을 AWS Config 활성화하기 전에 리소스 기록을 켜는 것이 좋습니다. 리소스 기록이 꺼져 있을 때 Security Hub에서 보안 검사를 실행하려고 하면 검사 결과 오류가 반환됩니다.

Security Hub는 AWS Config 사용자를 대신해 관리하지 않습니다. 이미 AWS Config 활성화한 경우 AWS Config 콘솔 또는 API를 통해 설정을 구성할 수 있습니다.

표준을 활성화했지만 AWS Config활성화하지 않은 경우 Security Hub는 다음 일정에 따라 AWS Config 규칙을 생성하려고 시도합니다.

- 표준을 활성화한 당일
- 표준을 활성화한 다음 날
- 표준을 활성화한 지 3일 후
- 표준을 활성화한 지 7일 후 (이후 7일마다 계속)

중앙 구성을 사용하는 경우 Security Hub는 하나 이상의 표준을 사용하도록 설정하는 구성 정책을 다시 적용할 때도 AWS Config 규칙을 만들려고 합니다.

활성화 AWS Config

AWS Config 아직 활성화하지 않았다면 다음 방법 중 하나로 활성화할 수 있습니다.

- 콘솔 또는 AWS CLI — 콘솔 또는 AWS Config AWS Config 콘솔을 사용하여 수동으로 활성화할 수 AWS CLI있습니다. AWS Config 개발자 안내서의 AWS Config시작하기 섹션을 참조하십시오.

- AWS CloudFormation 템플릿 - 많은 AWS Config 계정에서 활성화하려는 경우 CloudFormation 템플릿 활성화를 AWS Config 사용하여 활성화할 수 AWS Config있습니다. 이 템플릿에 액세스하려면 AWS CloudFormation 사용 설명서의 AWS CloudFormation StackSets 샘플 템플릿을 참조하십시오.
- Github 스크립트 — Security Hub는 여러 지역의 여러 계정에 대해 Security Hub를 활성화하는 GitHub 스크립트를 제공합니다. 이 스크립트는 Organizations와 통합하지 않았거나 조직에 속하지 않은 계정이 있는 경우에 유용합니다. 이 스크립트를 사용하여 Security Hub를 활성화하면 해당 계정에 대해서도 자동으로 AWS Config 활성화됩니다.

Security Hub 보안 검사를 실행하는 AWS Config 데 도움이 되도록 설정하는 방법에 대한 자세한 내용은 클라우드 보안 상태를 효과적으로 관리하기 AWS Config 위한 AWS Security Hub 최적화를 참조하십시오.

에서 리소스 기록 켜기 AWS Config

기본 AWS Config 설정으로 리소스 기록을 켜면 실행 중인 위치에서 AWS Config 검색된 지원되는 모든 유형의 지역 리소스가 기록됩니다. AWS 리전 지원되는 유형의 글로벌 리소스를 AWS Config 기록하도록 구성할 수도 있습니다. 글로벌 리소스는 한 리전에만 기록하면 됩니다(중앙 구성을 사용하는 경우 이 리전을 홈 리전으로 사용하는 것이 좋습니다).

를 사용하여 CloudFormation StackSets AWS Config활성화하는 경우 두 개를 다르게 실행하는 것이 좋습니다 StackSets. 하나를 StackSet 실행하여 글로벌 리소스를 포함한 모든 리소스를 단일 지역에 기록하세요. 두 번째 명령을 StackSet 실행하여 다른 지역의 글로벌 리소스를 제외한 모든 리소스를 기록하세요.

의 AWS Systems Manager기능인 빠른 설정을 사용하여 계정 및 지역 AWS Config 전체에서 리소스 기록을 신속하게 구성할 수도 있습니다. 빠른 설정 프로세스 중에 글로벌 리소스를 기록할 리전을 선택할 수 있습니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 AWS Config 구성 레코더 섹션을 참조하십시오.

보안 제어 Config.1은 해당 지역이 IAM (글로벌 리소스를 기록하지 않고 IAM) 글로벌 리소스를 기록하지 않고 IAM 글로벌 리소스를 기록해야 하는 제어를 활성화한 경우 애그리게이터에서 연결된 지역 AWS Identity and Access Management (검색 결과 수집기에 전혀 포함되지 않은 홈 지역 및 지역) 이외의 지역에 대해 실패한 검색 결과를 생성합니다. 연결된 지역에서 Config.1은 IAM 글로벌 리소스가 기록되었는지 여부를 확인하지 않습니다. 각 컨트롤에 필요한 리소스 목록은 을 참조하십시오. AWS Config 제어 결과를 생성하는 데 필요한 리소스

다중 계정 스크립트를 사용하여 Security Hub를 활성화하면 모든 리전에서 전역 리소스를 포함한 모든 리소스에 대한 리소스 기록이 자동으로 활성화됩니다. 그런 다음 단일 리전에만 전역 리소스를 기록하도록 구성을 업데이트할 수 있습니다. 자세한 내용은 AWS Config 개발자 안내서의 리소스 AWS Config 레코드 선택을 참조하십시오.

Security Hub가 AWS Config 규칙을 기반으로 하는 제어 결과를 정확하게 보고하려면 관련 리소스에 대한 기록을 활성화해야 합니다. 컨트롤 및 관련 AWS Config 리소스 목록은 을 참조하십시오AWS Config 제어 결과를 생성하는 데 필요한 리소스.AWS Config 리소스 상태 변경에 대한 연속 기록과 일일 기록 중에서 선택할 수 있습니다. 일별 기록을 선택하면 리소스 상태가 변경될 경우 AWS Config 는 24시간이 끝날 때마다 리소스 구성 데이터를 제공합니다. 변경 사항이 없는 경우에는 데이터가 제공되지 않습니다. 이로 인해 24시간이 완료될 때까지 변경 트리거 제어에 대한 Security Hub 결과 생성이 지연될 수 있습니다.

> **Note**
>
> 보안 검사 후 새로운 조사 결과를 생성하고 잘못된 조사 결과를 방지하려면 기본 리소스를 평가하기 위해 구성 레코더에 연결된 IAM 역할에 대한 충분한 권한이 있어야 합니다.

비용 고려 사항

리소스 기록과 관련된 비용에 대한 자세한 내용은 AWS Security Hub 가격 및 AWS Config 가격을 참조하십시오.

Security Hub는 AWS Config 구성 항목을 업데이트하여 구성 레코더 비용에 `AWS::Config::ResourceCompliance` 영향을 줄 수 있습니다. AWS Config 규칙과 연결된 Security Hub 컨트롤이 규정 준수 상태를 변경하거나, 활성화 또는 비활성화되거나, 매개 변수가 업데이트될 때마다 업데이트가 발생할 수 있습니다. AWS Config 구성 레코더를 Security Hub에만 사용하고 이 구성 항목을 다른 용도로는 사용하지 않는 경우 AWS Config 콘솔이나 콘솔에서 해당 레코더에 대한 녹화를 끄는 것이 좋습니다 AWS CLI. 이렇게 하면 AWS Config 비용을 줄일 수 있습니다. Security Hub에서 보안 검사를 하기 위해 `AWS::Config::ResourceCompliance`을 기록할 필요는 없습니다.

Security Hub 활성화

AWS Security Hub를 활성화하는 방법은 AWS Organizations와 통합하거나 수동으로 활성화하는 두 가지 방법이 있습니다.

다중 계정 및 다중 리전 환경을 위해 Organizations과의 통합을 권장합니다. 독립형 계정이 있는 경우 Security Hub를 수동으로 설정해야 합니다.

필요한 권한 확인

Amazon Web Services(AWS)에 가입한 후 해당 기능을 사용하려면 Security Hub를 활성화해야 합니다. Security Hub를 활성화하려면 먼저 Security Hub 콘솔 및 API 작업에 액세스할 수 있는 권한을 설정해야 합니다. 사용자 또는 AWS 관리자는 AWS Identity and Access Management(IAM)를 사용하여 `AWSSecurityHubFullAccess`라는 AWS 관리형 정책을 IAM ID에 연결함으로써 이를 수행할 수 있습니다.

Organizations 통합을 통해 Security Hub를 활성화하고 관리하려면 `AWSSecurityHubOrganizationsAccess`라는 AWS 관리형 정책도 연결해야 합니다.

자세한 내용은 AWSAWS Security Hub의 관리형 정책 섹션을 참조하세요.

Organizations 통합을 통해 Security Hub 활성화

AWS Organizations를 통해 Security Hub 사용을 시작하려면 조직의 AWS Organizations 관리 계정은 계정을 조직의 Security Hub 위임된 관리자 계정으로 지정합니다. Security Hub는 현재 리전의 위임된 관리자 계정에서 자동으로 활성화됩니다.

원하는 방법을 선택하고 단계에 따라 위임된 관리자를 지정합니다.

Security Hub console

온보딩 시 Security Hub 위임된 관리자를 지정하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. Security Hub로 이동하기를 선택합니다. Organizations 관리 계정에 로그인하라는 메시지가 표시됩니다.
3. 위임된 관리자 지정 페이지의 위임된 관리자 계정 섹션에서 위임된 관리자 계정을 지정합니다. 다른 AWS 보안 및 규정 준수 서비스에 설정한 것과 동일한 위임된 관리자를 선택하는 것이 좋습니다.

4. 위임된 관리자 설정을 선택합니다.

Security Hub API

Organizations 관리 계정에서 `EnableOrganizationAdminAccount` API를 호출합니다. Security Hub 위임된 관리자 계정의 AWS 계정 ID를 입력합니다.

AWS CLI

조직 관리 계정에서 `enable-organization-admin-account` 명령을 실행합니다. Security Hub 위임된 관리자 계정의 AWS 계정 ID를 입력합니다.

명령 예시:

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

Organizations와의 통합에 대한 자세한 내용은 Security Hub와 통합 AWS Organizations 섹션을 참조하세요.

위임된 관리자를 지정한 후에는 중앙 구성을 사용하여 Security Hub를 계속 설정하는 것이 좋습니다. 콘솔에 그렇게 하라는 메시지가 표시됩니다. 중앙 구성을 사용하면 조직의 Security Hub를 활성화하고 구성하는 프로세스를 간소화하고 조직에 적절한 보안 범위를 확보할 수 있습니다.

중앙 구성을 사용하면 위임된 관리자가 리전별로 구성하는 대신 여러 조직 계정 및 리전에서 Security Hub를 사용자 지정할 수 있습니다. 전체 조직에 대한 구성 정책을 만들거나 계정 및 OU별로 다른 구성 정책을 만들 수 있습니다. 정책은 관련 계정에서 Security Hub를 활성화 또는 비활성화할지 여부와 활성화되는 보안 표준 및 제어를 지정합니다.

위임된 관리자는 계정을 중앙 관리형 계정 또는 자체 관리형 계정으로 지정할 수 있습니다. 중앙 관리형 계정은 위임된 관리자만 구성할 수 있습니다. 자체 관리형 계정은 자체 설정을 지정할 수 있습니다.

중앙 구성을 사용하지 않는 경우 위임된 관리자가 Security Hub를 구성할 수 있는 권한이 더 제한됩니다. 자세한 내용은 를 통한 계정 관리 AWS Organizations 섹션을 참조하세요.

수동으로 Security Hub 활성화

독립형 계정이 있는 경우 또는 AWS Organizations와 통합하지 않는 경우 Security Hub를 수동으로 활성화해야 합니다. 독립형 계정은 AWS Organizations와 통합할 수 없으며 수동 활성화를 사용해야 합니다.

Security Hub를 수동으로 활성화하는 경우 Security Hub 관리자 계정을 지정하고 다른 계정을 구성원 계정으로 초대합니다. 예비 구성원 계정이 관리자 계정의 초대를 수락하면 Security Hub 관리자-구성원 관계가 성립됩니다.

원하는 방법을 선택하고 단계에 따라 Security Hub를 활성화하세요. 콘솔에서 Security Hub를 활성화하면 지원되는 보안 표준을 활성화하는 옵션도 제공됩니다.

Security Hub console

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 처음에 Security Hub 콘솔을 열면 Security Hub로 이동을 선택합니다.
3. 시작 페이지의 보안 표준 섹션에는 Security Hub에서 지원하는 보안 표준이 나열됩니다.

   표준을 활성화하려면 확인란을 선택하고, 비활성화하려면 확인란의 선택을 취소합니다.

   언제든지 표준 또는 해당 개별 제어를 활성화하거나 비활성화할 수 있습니다. 보안 표준 및 제어 관리에 대한 자세한 내용은 AWS Security Hub의 보안 제어 및 표준을 참조하세요.
4. Security Hub 활성화를 선택합니다.

Security Hub API

`EnableSecurityHub` API를 호출합니다. API에서 Security Hub를 활성화하면 다음의 기본 보안 표준이 자동으로 활성화됩니다.

- AWS 기본 보안 모범 사례
- 인터넷 보안 센터(CIS) AWS 파운데이션 벤치마크 v1.2.0

이러한 표준을 사용하지 않으려면 `EnableDefaultStandards`를 `false`로 설정합니다.

`Tags` 파라미터를 사용하여 허브 리소스에 태그 값을 할당할 수도 있습니다.

AWS CLI

`enable-security-hub` 명령을 실행합니다. 기본 표준을 활성화하려면 `--enable-default-standards`을 포함하세요. 기본 표준을 활성화하지 않으려면 `--no-enable-default-standards`을 포함하세요. 기본 보안 표준은 다음과 같습니다.

- AWS 기본 보안 모범 사례
- 인터넷 보안 센터(CIS) AWS 파운데이션 벤치마크 v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

예

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

다중 계정 활성화 스크립트

> **Note**
>
> 이 스크립트 대신 중앙 구성을 사용하여 다중 계정 및 리전에서 Security Hub를 활성화하고 구성하는 것이 좋습니다.

GitHub의 Security Hub 다중 계정 활성화 스크립트를 사용하면 계정 및 리전 전체에서 Security Hub를 활성화할 수 있습니다. 또한 이 스크립트는 구성원 계정에 초대를 보내고 AWS Config을 활성화하는 프로세스를 자동화합니다.

스크립트는 글로벌 리소스를 포함한 모든 리전의 모든 리소스에 대한 리소스 기록을 자동으로 활성화합니다. 글로벌 리소스 기록을 단일 리전으로 제한하지 않습니다.

여러 계정과 리전에서 Security Hub를 비활성화하는 해당 스크립트가 있습니다.

Security Hub 활성화 후의 다음 단계

Security Hub를 활성화한 후에는 보안 요구 사항에 중요한 보안 표준 및 보안 제어를 활성화하는 것이 좋습니다. 제어를 활성화하면 Security Hub가 보안 검사를 실행하고 제어 결과를 생성하기 시작합니다. 또한 Security Hub와 다른 AWS 서비스 및 타사 솔루션 간의 통합을 활용하여 Security Hub에서 결과를 확인할 수도 있습니다.

중앙 구성 작동 방식

중앙 구성은 여러 AWS 계정 및 AWS 리전에서 Security Hub를 설정하고 관리하는 데 도움이 되는 Security Hub 기능입니다. 중앙 구성을 사용하려면 먼저 Security Hub 및 를 통합해야 AWS Organizations합니다. 조직을 만들고 조직에 위임된 Security Hub 관리자 계정을 지정하여 서비스를 통합할 수 있습니다.

위임된 Security Hub 관리자 계정에서 Security Hub 서비스, 보안 표준 및 보안 제어를 여러 리전의 조직 계정 및 OU(조직 단위)에 구성하는 방법을 지정할 수 있습니다. 홈 리전이라고 하는 하나의 기본 리전에서 몇 단계만 거치면 이러한 설정을 구성할 수 있습니다. 중앙 구성을 사용하지 않는 경우 각 계정 및 리전에서 개별적으로 Security Hub를 구성해야 합니다.

중앙 구성을 사용하는 경우 위임된 관리자는 구성할 계정과 OU를 선택할 수 있습니다. 위임된 관리자가 구성원 계정 또는 OU를 자체 관리형으로 지정하는 경우 구성원은 각 리전에서 개별적으로 자체 설정을 구성할 수 있습니다. 위임된 관리자가 구성원 계정 또는 OU를 중앙 관리형형으로 지정하는 경우 위임된 관리자만 여러 리전에 걸쳐 구성원 계정 또는 OU를 구성할 수 있습니다. 조직의 모든 계정과 OU를 중앙 관리형, 자체 관리형 또는 이 둘의 조합으로 지정할 수 있습니다.

중앙 관리형 계정을 구성하기 위해 위임된 관리자는 Security Hub 구성 정책을 사용합니다. 구성 정책을 통해 위임된 관리자는 Security Hub의 활성화 또는 비활성화 여부와 활성화 및 비활성화되는 표준 및 제어를 지정할 수 있습니다. 구성 정책은 특정 제어의 파라미터를 사용자 지정하는 데에도 사용할 수 있습니다.

구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다. 위임된 관리자는 중앙 구성을 사용하기 전에 조직의 홈 리전과 연결된 리전을 지정합니다. 위임된 관리자는 전체 조직을 위한 단일 구성 정책을 만들거나 여러 구성 정책을 만들어 여러 계정 및 OU에 대한 변수 설정을 구성할 수 있습니다.

이 섹션에서는 중앙 구성의 개요를 다룹니다.

중앙 구성의 이점

중앙 구성의 이점은 다음과 같습니다.

Security Hub 서비스 및 기능의 구성 간소화

중앙 구성을 사용하는 경우 Security Hub는 조직의 보안 모범 사례를 구성하는 프로세스를 안내합니다. 또한 결과 구성 정책을 지정된 계정 및 OU에 자동으로 배포합니다. 새 보안 제어 자동 활성화

와 같은 기존 Security Hub 설정이 있는 경우 해당 설정을 구성 정책의 시작점으로 사용할 수 있습니다. 또한 Security Hub 콘솔의 구성 페이지에는 구성 정책, 각 정책을 사용하는 계정 및 OU에 대한 실시간 요약이 표시됩니다.

계정 및 리전 전반에 걸쳐 구성

중앙 구성을 사용하여 여러 계정 및 리전에 걸쳐 Security Hub를 구성할 수 있습니다. 이렇게 하면 조직의 각 부분이 일관된 구성과 적절한 보안 범위를 유지할 수 있습니다.

계정과 OU마다 서로 다른 구성 수용

중앙 구성을 사용하면 조직의 계정과 OU를 다양한 방식으로 구성하도록 선택할 수 있습니다. 예를 들어 테스트 계정과 프로덕션 계정에는 서로 다른 구성이 필요할 수 있습니다. 새 계정이 조직에 가입할 때 적용되는 구성 정책을 만들 수도 있습니다.

구성 드리프트 방지

구성 드리프트는 사용자가 위임된 관리자의 선택 사항과 충돌하는 서비스나 기능을 변경할 때마다 발생합니다. 중앙 구성은 이러한 드리프트를 방지합니다. 계정이나 OU를 중앙 관리형으로 지정하면 조직의 위임된 관리자만 해당 계정이나 OU를 구성할 수 있습니다. 특정 계정이나 OU에서 자체 설정을 구성하도록 하려면 해당 계정이나 OU를 자체 관리형으로 지정할 수 있습니다.

중앙 구성을 사용해야 하는 사람

중앙 구성은 여러 Security Hub 계정을 포함하는 AWS 환경에 가장 유용합니다. 여러 계정의 Security Hub를 중앙에서 관리할 수 있도록 설계되었습니다.

중앙 구성을 사용하여 Security Hub 서비스, 보안 표준 및 보안 제어를 구성할 수 있습니다. 또한 이를 사용하여 특정 제어의 파라미터를 사용자 지정할 수 있습니다. 표준과 제어에 대한 자세한 내용은 Security Hub의 AWS 보안 제어 및 표준 섹션을 참조하세요.

중앙 구성 용어 및 개념

다음 주요 용어 및 개념을 이해하면 Security Hub 중앙 구성을 사용하는 데 도움이 될 수 있습니다.

중앙 구성

조직의 위임된 Security Hub 관리자 계정이 여러 계정 및 리전에 걸쳐 Security Hub 서비스, 보안 표준 및 보안 제어를 구성하는 데 도움이 되는 Security Hub 기능입니다. 이러한 설정을 구성하기 위

해 위임된 관리자는 조직의 중앙 관리형 계정에 대한 Security Hub 구성 정책을 만들고 관리합니다. 자체 관리형 계정은 각 리전에서 개별적으로 자체 설정을 구성할 수 있습니다. 중앙 구성을 사용하려면 Security Hub 및 를 통합해야 AWS Organizations합니다.

홈 리전

위임된 관리자가 구성 정책을 만들고 관리하여 Security Hub를 AWS 리전 중앙에서 구성하는 방법입니다. 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다.

홈 리전은 Security Hub 집계 영역 역할도 하며 연결된 리전으로부터 조사 결과, 인사이트 및 기타 데이터를 수신합니다.

2019년 3월 20일 또는 그 이후에 AWS 도입된 지역을 옵트인 지역이라고 합니다. 옵트인 리전은 홈 리전이 될 수 없고 연결된 리전일 수 있습니다. 옵트인 리전 목록은 AWS 계정 관리 참조 안내서의 리전 활성화 및 비활성화 전 고려 사항을 참조하세요.

연결된 리전

홈 지역에서 구성할 수 있습니다. AWS 리전 구성 정책은 홈 리전의 위임된 관리자가 생성합니다. 이 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다. 중앙 구성을 사용하려면 연결된 리전을 최소한 하나 이상 지정해야 합니다.

또한 연결된 리전은 결과, 인사이트 및 기타 데이터를 홈 리전으로 보냅니다.

2019년 3월 20일 또는 그 이후에 AWS 도입된 지역을 옵트인 지역이라고 합니다. 구성 정책을 적용하려면 먼저 계정에 대해 해당 리전을 활성화해야 합니다. Organizations 관리 계정은 구성원 계정의 옵트인 리전을 활성화할 수 있습니다. 자세한 내용은 계정 관리 참조 가이드의 AWS 리전 계정에서 사용할 수 있는AWS 계정 지정을 참조하십시오.

Security Hub 구성 정책

위임된 관리자가 중앙 관리형 계정에 대해 구성할 수 있는 Security Hub 설정 모음입니다. 여기에는 다음이 포함됩니다.

- Security Hub를 활성화 또는 비활성화할지 여부.
- 하나 이상의 보안 표준을 사용할지 여부.
- 활성화된 표준 전반에서 활성화할 보안 제어. 위임된 관리자가 활성화해야 하는 특정 제어 목록을 제공하여 이 작업을 수행할 수 있으며, Security Hub에서는 다른 모든 제어(새 제어가 릴리스된 경우 포함)을 비활성화합니다. 또는 위임된 관리자가 비활성화해야 하는 특정 제어 목록을 제공할 수 있으며, Security Hub에서는 다른 모든 제어(새 제어가 릴리스된 경우 포함)를 활성화합니다.

- 사용 가능한 표준에서 사용할 수 있는 제어를 선택할 수 있도록 파라미터를 사용자 지정할 수도 있습니다.

구성 정책은 하나 이상의 계정, OU(조직 단위) 또는 루트와 연결된 후 홈 리전 및 연결된 모든 리전에 적용됩니다.

Security Hub 콘솔에서 위임된 관리자는 Security Hub 권장 구성 정책을 선택하거나 사용자 지정 구성 정책을 만들 수 있습니다. Security Hub API 및 를 사용하는 AWS CLI경우 위임된 관리자는 사용자 지정 구성 정책만 생성할 수 있습니다. 위임된 관리자는 최대 20개의 사용자 지정 구성 정책을 만들 수 있습니다.

권장 구성 정책에서는 Security Hub, AWS 기본 보안 모범 사례(FSBP) 표준, 모든 기존 및 신규 FSBP 제어가 활성화됩니다. 파라미터를 허용하는 제어는 기본값을 사용합니다. 권장 구성 정책은 전체 조직에 적용됩니다.

조직에 다른 설정을 적용하거나 다른 계정 및 OU에 다른 구성 정책을 적용하려면 사용자 지정 구성 정책을 만드세요.

로컬 구성

Security Hub를 통합한 후의 조직 기본 구성 유형 및 AWS Organizations. 로컬 구성을 사용하면 위임된 관리자가 현재 리전의 새 조직 계정에서 Security Hub 및 기본 보안 표준을 자동으로 활성화하도록 선택할 수 있습니다. 위임된 관리자가 자동으로 기본 표준을 활성화하면 이러한 표준의 일부인 모든 제어도 새 조직 계정의 기본 파라미터와 함께 자동으로 활성화됩니다. 이러한 설정은 기존 계정에는 적용되지 않으므로 계정이 조직에 가입한 후에 구성 드리프트가 발생할 수 있습니다. 기본 표준의 일부인 특정 제어를 비활성화하고 추가 표준 및 제어를 구성하는 작업은 각 계정 및 리전에서 개별적으로 수행해야 합니다.

로컬 구성에서는 구성 정책 사용을 지원하지 않습니다. 구성 정책을 사용하려면 중앙 구성으로 전환해야 합니다.

수동 계정 관리

Security Hub를 통합하지 AWS Organizations 않거나 독립 실행형 계정이 있는 경우 각 지역의 각 계정에 대한 설정을 개별적으로 지정해야 합니다. 수동 계정 관리는 구성 정책 사용을 지원하지 않습니다.

중앙 구성 API

Security Hub 위임된 관리자만 홈 리전에서 중앙 관리형 계정의 구성 정책을 관리하는 데 사용할 수 있는 Security Hub 작업입니다. 작업에는 다음이 포함됩니다.

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

계정별 API

Security Hub 작업: Security Hub, 표준 및 제어를 account-by-account 기반으로 활성화하거나 비활성화하는 데 사용할 수 있습니다. 이러한 작업은 각 개별 리전에서 사용됩니다.

자체 관리형 계정은 계정별 작업을 사용하여 자체 설정을 구성할 수 있습니다. 중앙 관리형 계정은 홈 리전 및 연결된 리전에서 다음과 같은 계정별 작업을 사용할 수 없습니다. 해당 리전에서는 위임된 관리자만 중앙 구성 작업과 구성 정책을 통해 중앙 관리형 계정을 구성할 수 있습니다.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

중앙 관리 계정의 소유자는 Security Hub API의 일부 `Get` 또는 `Describe` 작업을 사용하여 계정 상태를 확인할 수 있습니다.

중앙 구성 대신 로컬 구성 또는 수동 계정 관리를 사용하는 경우 이러한 계정별 작업을 사용할 수 있습니다.

자체 관리 계정도 사용 `*Invitations` 및 `*Members` 운영할 수 있습니다. 하지만 자체 관리 계정에서는 이러한 작업을 사용하지 않는 것이 좋습니다. 위임된 관리자와 다른 조직에 속한 자체 구성원이 구성원 계정에 있는 경우 정책 연결이 실패할 수 있습니다.

조직 단위(OU)

AWS Organizations In 및 Security Hub는 그룹을 위한 AWS 계정컨테이너입니다. 또한 조직 단위(OU)는 다른 OU를 포함할 수 있기 때문에 사용자는 위쪽에는 상위 OU가, 아래쪽에는 OU 가지가, 맨 끝에는 나뭇잎에 해당하는 계정이 있는 거꾸로 된 나무 형태의 계층 구조를 만들 수 있습니다. 각 OU는 정확히 하나의 상위 항목을 가질 수 있으며, 각 계정은 한 OU의 구성원만 될 수 있습니다.

AWS Organizations 또는 에서 OU를 관리할 수 AWS Control Tower있습니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 단위 관리 또는 AWS Control Tower 사용 설명서의 AWS Control Tower로 조직 및 계정 관리를 참조하세요.

위임된 관리자는 구성 정책을 특정 계정 또는 OU에 연결하거나 조직의 모든 계정 및 OU를 포괄하는 루트와 연결할 수 있습니다.

중앙 관리형

위임된 관리자만 구성 정책을 사용하여 여러 리전에 걸쳐 구성할 수 있는 계정, OU 또는 루트입니다.

위임된 관리자 계정은 계정을 중앙에서 관리할지 여부를 지정합니다. 위임된 관리자는 계정 상태를 중앙 관리형에서 자체 관리형으로 또는 그 반대로 변경할 수도 있습니다.

자체 관리형

자체 Security Hub 설정을 관리하는 계정, OU 또는 루트입니다. 자체 관리형 계정은 계정별 작업을 사용하여 각 리전에서 개별적으로 Security Hub를 구성합니다. 이는 중앙 관리형 계정과 대조가 됩니다. 중앙 관리형 계정은 구성 정책을 통해 여러 리전의 위임된 관리자만 구성할 수 있습니다.

위임된 관리자 계정은 계정을 자체 관리할지 여부를 지정합니다. 위임된 관리자 계정은 계정의 상태를 자체 관리형에서 중앙 관리형로 또는 그 반대로 변경할 수도 있습니다.

위임된 관리자는 계정이나 OU에 자체 관리형 동작을 적용할 수 있습니다. 또는 계정 또는 OU가 상위 항목으로부터 자체 관리형 동작을 상속받을 수도 있습니다. 위임된 관리자 계정 자체가 자체 관리형 계정일 수 있습니다.

구성 정책 연결

구성 정책과 계정, 조직 단위(OU) 또는 루트 간의 링크입니다. 정책 연결이 존재하는 경우 계정, OU 또는 루트는 구성 정책에 정의된 설정을 사용합니다. 연결은 다음 두 경우 중 하나에 존재합니다.

- 위임된 관리자가 계정, OU 또는 루트에 구성 정책을 직접 적용하는 경우
- 계정 또는 OU가 상위 OU 또는 루트로부터 구성 정책을 상속하는 경우

연결은 다른 구성이 적용되거나 상속될 때까지 존재합니다.

적용된 구성 정책

위임된 관리자가 대상 계정, OU 또는 루트에 구성 정책을 직접 적용하는 구성 정책 연결의 한 유형입니다. 대상은 구성 정책에서 정의하는 방식으로 구성되며 위임된 관리자만 구성을 변경할 수 있습니다. 루트에 적용할 경우 구성 정책은 적용 또는 가장 가까운 상위 항목으로부터의 상속을 통해 다른 구성을 사용하지 않는 조직 내 모든 계정과 OU에 영향을 미칩니다.

위임된 관리자는 자체 관리형 구성을 특정 계정, OU 또는 루트에 적용할 수도 있습니다.

상속된 구성 정책

계정이나 OU가 가장 가까운 상위 OU 또는 루트의 구성을 채택하는 구성 정책 연결의 한 유형입니다. 구성 정책은 계정이나 OU에 직접 적용되지 않는 경우 가장 가까운 상위 항목의 구성을 상속합니다. 정책의 모든 요소가 상속됩니다. 즉, 계정이나 OU는 정책의 일부만 선택적으로 상속하도록 선택할 수 없습니다. 가장 가까운 상위 항목이 자체 관리형인 경우 하위 계정 또는 OU는 상위 항목의 자체 관리형 동작을 상속합니다.

상속은 적용된 구성을 무시할 수 없습니다. 즉, 구성 정책 또는 자체 관리형 구성이 계정이나 OU에 직접 적용되는 경우 해당 구성을 사용하며 상위 항목의 구성을 상속하지 않습니다.

루트

내부 AWS Organizations 및 Security Hub는 조직의 최상위 상위 노드입니다. 위임된 관리자가 루트에 구성 정책을 적용하면 해당 정책이 적용 또는 상속을 통해 다른 정책을 사용하거나 자체 관리형로 지정되지 않는 한 조직의 모든 계정 및 OU와 정책이 연결됩니다. 관리자가 루트를 자체 관리형으로 지정하면 적용 또는 상속을 통한 구성 정책을 사용하지 않는 한 조직의 모든 계정과 OU가 자체 관리형입니다. 루트가 자체 관리형이고 현재 구성 정책이 없는 경우 조직의 모든 새 계정은 현재 설정을 유지합니다.

조직에 가입하는 새 계정은 특정 OU에 할당되기 전까지는 루트에 속합니다. 새 계정이 OU에 할당되지 않은 경우 위임된 관리자가 해당 계정을 자체 관리형 계정으로 지정하지 않는 한 루트 구성을 상속합니다.

중앙 구성 사용 시작

AWS Security Hub 위임된 관리자 계정은 중앙 구성을 사용하여 AWS 리전 전반에 걸친 다중 계정 및 OU(조직 단위)에 대한 Security Hub, 표준 및 제어를 구성할 수 있습니다.

이 섹션에서는 중앙 구성을 위한 사전 조건과 중앙 구성 사용을 시작하는 방법에 대해 설명합니다.

중앙 구성을 위한 사전 조건

중앙 구성 사용을 시작하기 전에 Security Hub를 AWS Organizations와 통합하고 홈 리전을 지정해야 합니다. Security Hub 콘솔을 사용하는 경우 이러한 사전 조건은 중앙 구성의 옵트인 워크플로에 포함됩니다.

Organizations과 통합

중앙 구성을 사용하려면 Security Hub 및 Organizations를 통합해야 합니다.

이러한 서비스를 통합하려면 먼저 Organizations에서 조직을 만들어야 합니다. 그런 다음 Organizations 관리 계정에서 Security Hub 위임된 관리자 계정을 지정합니다. 지침은 Security Hub와 통합 AWS Organizations 섹션을 참조하세요.

원하는 홈 리전에 위임된 관리자를 지정해야 합니다. 중앙 구성 사용을 시작하면 연결된 모든 리전에도 동일한 위임된 관리자가 자동으로 설정됩니다. Organizations 관리 계정은 위임된 관리자 계정으로 설정할 수 없습니다.

> **Important**
>
> 중앙 구성을 사용하는 경우 Security Hub 콘솔 또는 Security Hub API를 사용하여 위임된 관리자 계정을 변경하거나 제거할 수 없습니다. Organizations 관리 계정이 AWS Organizations API를 사용하여 Security Hub 위임된 관리자를 변경하거나 제거하는 경우 Security Hub는 자동으로 중앙 구성을 중지합니다. 구성 정책도 연결 해제되고 삭제됩니다. 구성원 계정은 위임된 관리자가 변경되거나 제거되기 전의 구성을 유지합니다.

홈 리전 지정

중앙 구성을 사용하려면 홈 리전을 지정해야 합니다. 홈 리전은 위임된 관리자가 조직을 구성하는 리전입니다.

중앙 구성을 사용하려면 홈 리전에서 구성할 수 있는 연결된 리전을 하나 이상 지정해야 합니다.

> **Note**
>
> 홈 리전은 AWS가 옵트인 리전으로 지정한 리전일 수 없습니다. 옵트인 리전은 기본적으로 비활성화되어 있습니다. 옵트인 리전 목록은 AWS 계정 관리 참조 안내서의 리전 활성화 및 비활성화 전 고려 사항을 참조하세요.

위임된 관리자는 홈 리전에서만 구성 정책을 만들고 관리할 수 있습니다. 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다. 이러한 리전 중 일부에만 적용되고 다른 리전에는 적용되지 않는 구성 정책을 만들 수 없습니다.

홈 리전은 연결된 리전으로부터 조사 결과, 인사이트 및 기타 데이터를 수신하는 Security Hub 집계 영역이기도 합니다.

크로스 리전 집계를 위한 집계 영역을 이미 설정했다면 이 리전이 중앙 구성의 기본 홈 리전입니다. 중앙 구성을 사용하기 전에 현재 조사 결과 집계자를 삭제하고 원하는 홈 리전에 새 조사 결과 집계자를 생성하여 홈 리전을 변경할 수 있습니다. 조사 결과 집계자는 홈 리전 및 연결된 리전을 지정하는 Security Hub 리소스입니다.

홈 리전을 지정하려면 집계 영역 설정 단계를 따르세요. 이미 홈 리전이 있는 경우 GetFindingAggregator API를 호출하여 현재 연결된 리전을 포함하여 해당 리전에 대한 세부 정보를 확인할 수 있습니다.

중앙 구성 시작

원하는 방법을 선택하고 단계에 따라 조직의 중앙 구성 사용을 시작하세요.

Security Hub console

조직을 중앙에서 구성하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정 및 구성을 선택합니다. 그런 다음 중앙 구성 시작을 선택합니다.

   Security Hub에 온보딩하는 경우 Security Hub로 이동을 선택합니다.
3. 위임된 관리자 지정 페이지에서 위임된 관리자 계정을 선택하거나 계정 ID를 입력합니다. 해당하는 경우 다른 AWS 보안 및 규정 준수 서비스에 설정한 것과 동일한 위임된 관리자를 선택하는 것이 좋습니다. 위임된 관리자 설정을 선택합니다.
4. 조직 중앙 집중화 페이지의 리전 섹션에서 홈 리전을 선택합니다. 계속하려면 홈 리전에 로그인해야 합니다. 크로스 리전 집계를 위한 집계 영역을 이미 설정한 경우 해당 리전이 홈 리전으로 표시됩니다. 홈 리전을 변경하려면 리전 설정 편집을 선택합니다. 그런 다음 원하는 홈 리전을 선택하고 이 워크플로로 돌아갈 수 있습니다.
5. 홈 리전에 연결할 리전을 하나 이상 선택합니다. 필요에 따라 나중에 지원되는 리전을 홈 리전에 자동으로 연결할지 여부를 선택합니다. 여기서 선택한 리전은 위임된 관리자가 홈 리전에서 구성할 수 있습니다. 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다.

6. 확인 및 계속을 선택합니다.
7. 이제 중앙 구성을 사용할 수 있습니다. 계속해서 콘솔 프롬프트에 따라 첫 번째 구성 정책을 생성합니다. 구성 정책을 아직 만들 준비가 되지 않았다면 아직 구성할 준비가 되지 않았음을 선택합니다. 나중에 탐색 창에서 설정 및 구성을 선택하여 정책을 만들 수 있습니다. 구성 정책 생성에 대한 지침은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요.

Security Hub API

Security Hub를 중앙에서 구성하려면

1. 위임된 관리자 계정의 보안 인증 정보를 사용하여 홈 리전에서 UpdateOrganizationConfiguration API를 호출합니다.
2. `AutoEnable` 필드를 `false`로 설정합니다.
3. `OrganizationConfiguration` 객체의 `ConfigurationType` 필드를 `CENTRAL`로 설정합니다. 이 작업은 다음과 같은 영향을 미칩니다.
   - 통화 계정을 연결된 모든 리전의 Security Hub 위임된 관리자로 지정합니다.
   - 연결된 모든 리전의 위임된 관리자 계정에서 Security Hub를 활성화합니다.
   - 통화 계정을 Security Hub를 사용하고 조직에 속하는 신규 및 기존 계정의 Security Hub 위임된 관리자로 지정합니다. 이는 홈 리전 및 연결된 모든 리전에서 발생합니다. 통화 계정은 Security Hub가 활성화된 구성 정책에 연결된 경우에만 새 조직 계정의 위임된 관리자로 설정됩니다. 통화 계정은 Security Hub가 이미 활성화된 경우에만 기존 조직 계정의 위임된 관리자로 설정됩니다.
   - 연결된 모든 리전에서 AutoEnable을 `false`로 설정하고 홈 리전 및 연결된 모든 리전에서 AutoEnableStandards를 `NONE`으로 설정합니다. 이러한 파라미터는 중앙 구성을 사용할 때 홈 리전 및 연결된 리전과 관련이 없지만 구성 정책을 사용하여 조직 계정에서 Security Hub 및 기본 보안 표준을 자동으로 활성화할 수 있습니다.
4. 이제 중앙 구성을 사용할 수 있습니다. 위임된 관리자는 조직의 Security Hub를 구성하는 구성 정책을 만들 수 있습니다. 구성 정책 생성에 대한 지침은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요.

API 요청 예시:

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
```

```
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Security Hub를 중앙에서 구성하려면

1. 위임된 관리자 계정의 보안 인증 정보를 사용하여 홈 리전에서 update-organization-configuration 명령을 실행합니다.
2. `no-auto-enable` 파라미터를 포함합니다.
3. `organization-configuration` 객체의 `ConfigurationType` 필드를 `CENTRAL`로 설정합니다. 이 작업은 다음과 같은 영향을 미칩니다.
   - 통화 계정을 연결된 모든 리전의 Security Hub 위임된 관리자로 지정합니다.
   - 연결된 모든 리전의 위임된 관리자 계정에서 Security Hub를 활성화합니다.
   - 통화 계정을 Security Hub를 사용하고 조직에 속하는 신규 및 기존 계정의 Security Hub 위임된 관리자로 지정합니다. 이는 홈 리전 및 연결된 모든 리전에서 발생합니다. 통화 계정은 Security Hub가 활성화된 구성 정책에 연결된 경우에만 새 조직 계정의 위임된 관리자로 설정됩니다. 통화 계정은 Security Hub가 이미 활성화된 경우에만 기존 조직 계정의 위임된 관리자로 설정됩니다.
   - 연결된 모든 리전에서 자동 활성화 옵션을 no-auto-enable로 설정하고 홈 리전 및 연결된 모든 리전에서 auto-enable-standards를 `NONE`으로 설정합니다. 이러한 파라미터는 중앙 구성을 사용할 때 홈 리전 및 연결된 리전과 관련이 없지만 구성 정책을 사용하여 조직 계정에서 Security Hub 및 기본 보안 표준을 자동으로 활성화할 수 있습니다.
4. 이제 중앙 구성을 사용할 수 있습니다. 위임된 관리자는 조직의 Security Hub를 구성하는 구성 정책을 만들 수 있습니다. 구성 정책 생성에 대한 지침은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요.

명령 예시:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

계정 및 OU 관리 유형 선택

중앙 구성을 사용하는 경우 AWS Security Hub 위임된 관리자는 각 조직 계정 및 OU (조직 구성 단위)를 중앙 관리 또는 자체 관리로 지정할 수 있습니다. 계정 또는 OU의 관리 유형에 따라 Security Hub 설정을 지정하고 변경하는 방법이 결정됩니다.

자체 관리 계정 또는 OU는 각 AWS 리전계정에서 고유한 Security Hub 설정을 개별적으로 구성할 수 있습니다. 위임된 관리자는 자체 관리형 계정 또는 OU에 대한 Security Hub 설정을 구성할 수 없으며 구성 정책을 해당 계정과 연결할 수 없습니다. 반면, 위임된 관리자만이 홈 리전 및 연결된 리전 전체에서 중앙 관리형 계정 및 OU에 대한 Security Hub 설정을 구성할 수 있습니다. 구성 정책을 중앙 관리형 계정 및 OU에 연결할 수 있습니다.

위임된 관리자는 계정이나 OU의 상태를 자체 관리형과 중앙 관리형 간에 전환할 수 있습니다. 기본적으로 Security Hub API를 통해 중앙 구성을 시작하면 모든 계정과 OU는 자체 관리합니다. 콘솔에서 관리 유형은 첫 번째 구성 정책에 따라 달라집니다. 첫 번째 정책에 연결하는 계정과 OU는 중앙에서 관리합니다. 다른 계정과 OU는 기본적으로 자체에서 관리합니다.

구성 정책을 자체 관리 계정과 연결하면 해당 정책이 자체 관리형 지정보다 우선 적용됩니다. 계정은 중앙에서 관리되며 구성 정책에 반영된 설정을 채택합니다.

하위 계정과 OU는 자체 관리형 상위 계정의 자체 관리형 동작을 상속할 수 있습니다. 이는 하위 계정과 OU가 중앙 관리형 상위 계정으로부터 구성 정책을 상속받는 것과 마찬가지입니다. 자세한 정보는 적용 및 상속을 통한 정책 연결을 참조하세요.

자체 관리 계정 또는 OU는 상위 노드나 루트에서 구성 정책을 상속할 수 없습니다. 예를 들어 조직의 모든 계정과 OU가 루트의 구성 정책을 상속받도록 하려면 자체 관리형 노드의 관리 유형을 중앙 관리로 변경해야 합니다.

자체 관리 계정의 설정 지정

자체 관리형 계정은 각 리전에서 개별적으로 자체 설정을 구성해야 합니다.

자체 관리 계정의 소유자는 각 지역에서 Security Hub API의 다음 작업을 호출하여 설정을 구성할 수 있습니다.

- Security Hub 서비스를 활성화 또는 비활성화하는 `EnableSecurityHub` 및 `DisableSecurityHub`
- 표준을 활성화 또는 비활성화하는 `BatchEnableStandards` 및 `BatchDisableStandards`
- 제어를 활성화 또는 비활성화하는 `BatchUpdateStandardsControlAssociations` 또는 `UpdateStandardsControl`

자체 관리 계정도 사용 `*Invitations` 및 운영할 수 있습니다. `*Members` 하지만 자체 관리 계정에서는 이러한 작업을 사용하지 않는 것이 좋습니다. 위임된 관리자와 다른 조직에 속한 자체 구성원이 구성원 계정에 있는 경우 정책 연결이 실패할 수 있습니다.

Security Hub API 작업에 대한 설명은 AWS Security Hub API 참조를 참조하세요.

자체 관리 계정은 Security Hub AWS CLI 콘솔을 사용하거나 각 지역에서 설정을 구성할 수도 있습니다.

자체 관리형 계정은 Security Hub 구성 정책 및 정책 연결과 관련된 API를 호출할 수 없습니다. 위임된 관리자만 중앙 구성 API를 호출하고 구성 정책을 사용하여 중앙 관리형 계정을 구성할 수 있습니다.

관리 유형의 계정 및 OU 선택

원하는 방법을 선택하고 단계에 따라 계정 또는 OU를 중앙 관리형 또는 자체 관리형으로 지정합니다.

Security Hub console

계정 또는 OU의 관리 유형을 선택하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. Configuration(구성)을 선택합니다.
3. 조직 탭에서 대상 계정 또는 OU를 선택합니다. 편집을 선택합니다.
4. 위임된 관리자가 대상 계정 또는 OU를 구성하도록 하려면 구성 정의 페이지의 관리 유형에서 중앙 관리형을 선택합니다. 그런 다음 기존 구성 정책을 대상과 연결하려면 특정 정책 적용을 선택합니다. 대상이 가장 가까운 상위 항목의 구성을 상속하도록 하려면 내 조직에서 상속을 선택합니다. 계정이나 OU에서 자체 설정을 구성하도록 하려면 자체 관리형을 선택합니다.
5. 다음을 선택합니다. 변경 사항을 검토하고 저장을 선택합니다.

Security Hub API

계정 또는 OU의 관리 유형을 선택하려면

1. 홈 리전의 Security Hub 위임된 관리자 계정에서 StartConfigurationPolicyAssociation API를 호출합니다.
2. `ConfigurationPolicyIdentifier` 필드에서 계정이나 OU가 자체 설정을 제어하도록 하려면 `SELF_MANAGED_SECURITY_HUB`를 입력합니다. 위임된 관리자가 계정 또는 OU에 대한

설정을 제어하도록 하려면 관련 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 제공합니다.

3. `Target`필드에 관리 유형을 변경하려는 대상의 AWS 계정 ID, OU ID 또는 루트 ID를 입력합니다. 그러면 자체 관리형 동작 또는 지정된 구성 정책이 대상과 연결됩니다. 대상의 하위 계정은 자체 관리형 동작 또는 구성 정책을 상속할 수 있습니다.

자체 관리형 계정을 지정하기 위한 API 요청 예시:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

계정 또는 OU의 관리 유형을 선택하려면

1. 홈 리전의 Security Hub 위임된 관리자 계정에서 start-configuration-policy-association 명령을 실행합니다.
2. `configuration-policy-identifier` 필드에서 계정이나 OU가 자체 설정을 제어하도록 하려면 `SELF_MANAGED_SECURITY_HUB`를 입력합니다. 위임된 관리자가 계정 또는 OU에 대한 설정을 제어하도록 하려면 관련 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 제공합니다.
3. `target`필드에 관리 유형을 변경하려는 대상의 AWS 계정 ID, OU ID 또는 루트 ID를 제공하십시오. 그러면 자체 관리형 동작 또는 지정된 구성 정책이 대상과 연결됩니다. 대상의 하위 계정은 자체 관리형 동작 또는 구성 정책을 상속할 수 있습니다.

자체 관리형 계정을 지정하기 위한 명령 예시:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Security Hub 구성 정책의 작동 방식

위임된 관리자 계정은 조직의 Security Hub, 보안 표준 및 보안 제어를 구성하는 AWS Security Hub 구성 정책을 만들 수 있습니다. 구성 정책을 생성한 후 위임된 관리자는 이를 계정, 조직 단위(OU) 또는 루트에 연결할 수 있습니다. 위임된 관리자는 구성 정책을 보거나 편집하거나 삭제할 수도 있습니다.

정책 고려 사항

Security Hub에서 구성 정책을 만들 전에 다음 사항을 고려하세요.

- 구성 정책을 적용하려면 연결해야 합니다 – 구성 정책을 만든 후 하나 이상의 계정, OU(조직 단위) 또는 루트와 연결할 수 있습니다. 구성 정책은 직접 적용을 통해 또는 상위 OU로부터의 상속을 통해 계정 또는 OU와 연결할 수 있습니다.
- 계정 또는 OU는 하나의 구성 정책에만 연결할 수 있습니다. — 설정 충돌을 방지하기 위해 계정 또는 OU는 한 번에 하나의 구성 정책에만 연결할 수 있습니다. 또는 계정이나 OU를 자체 관리할 수도 있습니다.
- 구성 정책은 완전합니다 - 구성 정책은 완전한 설정 사양을 제공합니다. 예를 들어 하위 계정은 한 정책의 일부 제어에 대한 설정과 다른 정책의 다른 제어에 대한 설정을 수락할 수 없습니다. 정책을 하위 계정에 연결할 때는 하위 계정에서 사용할 모든 설정이 정책에 지정되어 있는지 확인하세요.
- 구성 정책은 되돌릴 수 없습니다. 구성 정책을 계정이나 OU에 연결한 후에는 되돌릴 수 있는 옵션이 없습니다. 예를 들어 CloudWatch 컨트롤을 사용하지 않도록 설정하는 구성 정책을 특정 계정에 연결한 다음 해당 정책을 분리하면 해당 계정에서 CloudWatch 컨트롤이 계속 사용 중지됩니다. CloudWatch 컨트롤을 다시 활성화하려면 컨트롤을 사용하도록 설정하는 새 정책에 계정을 연결할 수 있습니다. 또는 계정을 자체 관리형으로 변경하고 계정에서 각 CloudWatch 컨트롤을 활성화할 수 있습니다.
- 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다 – 구성 정책은 홈 리전 및 연결된 모든 리전의 모든 관련 계정에 영향을 미칩니다. 이러한 리전 중 일부에만 적용되고 다른 리전에는 적용되지 않는 구성 정책을 만들 수 없습니다. 단, 전역 리소스와 관련된 제어는 예외입니다.

  2019년 3월 20일 또는 그 이후에 AWS 도입된 지역을 옵트인 지역이라고 합니다. 구성 정책이 계정에 적용되기 전에 해당 계정의 리전을 활성화해야 합니다. Organizations 관리 계정은 구성원 계정의 옵트인 리전을 활성화할 수 있습니다. 옵트인 지역을 활성화하는 방법에 대한 지침은 계정 관리 참조 가이드에서 AWS 리전 계정에서 사용할 수 있는 영역AWS 지정을 참조하십시오.

  정책이 홈 리전 또는 하나 이상의 연결된 리전에서 사용할 수 없는 제어를 구성하는 경우 Security Hub는 사용할 수 없는 리전의 제어 구성을 건너뛰고 제어를 사용할 수 있는 리전에 구성을 적용합니다.

- 구성 정책은 리소스입니다 - 구정 정책은 리소스로서 Amazon 리소스 이름(ARN) 및 범용 고유 식별자(UUID)를 포함합니다. 제품 ARN은 `arn:partition:securityhub:region:delegated administrator account ID:configuration-policy/configuration policy UUID` 형식을 사용합니다. 자체 관리형 구성에는 ARN 또는 UUID가 없습니다. 자체 관리형 구성의 식별자는 입니다. `SELF_MANAGED_SECURITY_HUB`

구성 정책 유형

각 구성 정책은 다음 설정을 지정합니다.

- Security Hub를 활성화하거나 비활성화합니다.
- 하나 이상의 보안 표준을 활성화합니다.
- 활성화된 표준 전반에서 어떤 보안 제어를 사용할 수 있는지 표시합니다. 이를 위해 활성화해야 하는 특정 제어 목록을 제공할 수 있습니다. 그러면 Security Hub에서 새 제어가 릴리스될 때 새 제어를 포함한 다른 모든 제어를 비활성화합니다. 또는 비활성화해야 하는 특정 제어의 목록을 제공할 수 있습니다. 그러면 Security Hub에서 새 제어가 릴리스될 때 이를 포함하여 다른 모든 제어를 활성화합니다.
- 사용 가능한 표준에서 사용할 수 있는 제어를 선택할 수 있도록 파라미터를 사용자 지정할 수도 있습니다.

중앙 구성 정책에는 AWS Config 레코더 설정이 포함되지 않습니다. Security Hub에서 제어 결과를 생성하려면 필요한 리소스에 대한 기록을 별도로 AWS Config 활성화하고 설정해야 합니다. 자세한 정보는 구성 AWS Config을 참조하세요.

중앙 구성을 사용하는 경우 Security Hub는 홈 지역을 제외한 모든 지역의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다. 구성 정책을 통해 사용하도록 선택한 기타 제어 기능은 사용 가능한 모든 지역에서 사용할 수 있습니다. 이러한 컨트롤에 대한 검색 결과를 한 지역으로만 제한하려면 AWS Config 레코더 설정을 업데이트하고 홈 지역을 제외한 모든 지역에서 글로벌 리소스 기록을 끄면 됩니다. 중앙 구성을 사용하면 홈 지역 및 연결된 지역에서 사용할 수 없는 컨트롤에 대한 적용 범위가 부족해집니다. 글로벌 리소스와 관련된 컨트롤 목록은 을 참조하십시오글로벌 리소스를 처리하는 제어.

권장 구성 정책

Security Hub 콘솔에서 처음으로 구성 정책을 생성할 때는 Security Hub 권장 정책을 선택할 수 있습니다.

권장 정책은 Security Hub, AWS 기본 보안 모범 사례 (FSBP) 표준, 모든 기존 및 새로운 FSBP 제어를 지원합니다. 파라미터를 허용하는 제어는 기본값을 사용합니다. 권장 정책은 루트(신규 및 기존 모든 계정 및 OU)에 적용됩니다. 조직을 위한 권장 정책을 만든 후 위임된 관리자 계정에서 수정할 수 있습니다. 예를 들어 추가 표준 또는 제어를 활성화하거나 특정 FSBP 제어를 비활성화할 수 있습니다. 구성 정책 수정에 대한 지침은 Security Hub 구성 정책 업데이트 섹션을 참조하세요.

사용자 지정 구성 정책

위임된 관리자는 권장 정책 대신 최대 20개의 사용자 지정 구성 정책을 만들 수 있습니다. 단일 사용자 지정 정책을 전체 조직에 연결하거나 계정 및 OU가 서로 다른 사용자 지정 정책을 연결할 수 있습니다. 사용자 지정 구성 정책에서 원하는 설정을 지정합니다. 예를 들어 FSBP, CIS(인터넷 보안 센터) AWS 파운데이션 벤치마크 v1.4.0 및 Amazon Redshift 제어를 제외한 해당 표준의 모든 제어를 활성화하는 사용자 지정 정책을 생성할 수 있습니다. 사용자 지정 구성 정책에 사용하는 세분화 수준은 조직 전체의 의도한 보안 적용 범위에 따라 달라집니다.

> **Note**
>
> Security Hub를 비활성화하는 구성 정책을 위임된 관리자 계정과 연결할 수 없습니다. 이러한 정책을 다른 계정과 연결할 수는 있지만 위임된 관리자와의 연결은 건너뜁니다. 위임된 관리자 계정은 현재의 구성을 유지합니다.

사용자 지정 구성 정책을 만든 후 권장 구성을 반영하도록 구성 정책을 업데이트하여 권장 구성 정책으로 전환할 수 있습니다. 하지만 첫 번째 정책을 만든 후에는 Security Hub 콘솔에 권장 구성 정책을 생성할 수 있는 옵션이 표시되지 않습니다.

적용 및 상속을 통한 정책 연결

처음에 중앙 구성을 선택하면 조직은 연결되지 않으면 옵트인 전과 동일한 방식으로 동작합니다. 그러면 위임된 관리자가 구성 정책 또는 자체 관리 동작과 계정, OU 또는 루트 간에 연결을 설정할 수 있습니다. 적용 또는 상속을 통해 연결을 설정할 수 있습니다.

위임된 관리자 계정에서 구성 정책을 계정, OU 또는 루트에 직접 적용할 수 있습니다. 또는 위임된 관리자가 계정, OU 또는 루트에 자체 관리형 지정을 직접 적용할 수도 있습니다.

직접 적용하지 않는 경우 계정 또는 OU는 구성 정책 또는 자체 관리 동작이 있는 가장 가까운 상위 계정의 설정을 상속합니다. 가장 가까운 상위 항목이 구성 정책에 연결되어 있는 경우 해당 정책은 해당 하위 항목에 상속되며 홈 리전의 위임된 관리자만 구성할 수 있습니다. 가장 가까운 부모가 스스로 관

리하는 경우, 자녀는 스스로 관리하는 행동을 물려받으며 각 동작에 자체 설정을 지정할 수 있습니다. AWS 리전

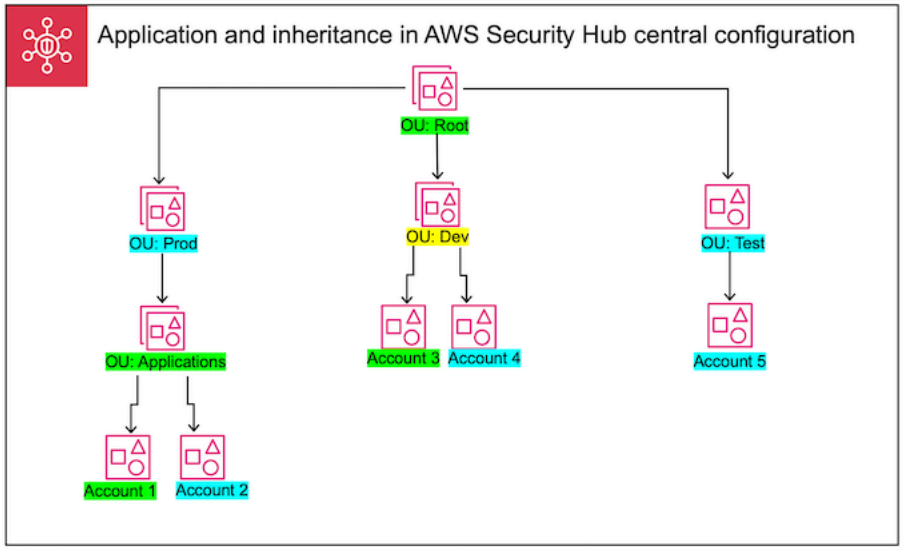
애플리케이션은 상속보다 우선합니다. 즉, 위임된 관리자가 계정이나 OU에 직접 적용한 구성 정책이나 자체 관리형 지정은 상속이 무시되지 않습니다.

구성 정책을 자체 관리 계정에 직접 적용하는 경우 정책이 자체 관리형 지정보다 우선 적용됩니다. 계정은 중앙에서 관리되며 구성 정책에 반영된 설정을 채택합니다.

구성 정책을 루트에 직접 적용하는 것이 좋습니다. 정책을 루트에 적용하면 조직에 가입한 새 계정을 다른 정책에 연결하거나 자체 관리형으로 지정하지 않는 한 루트 정책을 자동으로 상속합니다.

적용이나 상속을 통해 한 번에 하나의 구성 정책만 계정이나 OU에 연결할 수 있습니다. 이는 설정 충돌을 방지하기 위한 것입니다.

다음 다이어그램은 중앙 구성에서 정책 적용 및 상속이 작동하는 방식을 보여줍니다.



이 예제에서 녹색으로 강조 표시된 노드에는 구성 정책이 적용되어 있습니다. 파란색으로 강조 표시된 노드에는 해당 노드에 적용된 구성 정책이 없습니다. 노란색으로 강조 표시된 노드는 자체 관리형 노드로 지정되었습니다. 각 계정 및 OU는 다음 구성을 사용합니다.

- OU:Root(녹색) - 이 OU는 해당 OU에 적용된 구성 정책을 사용합니다.
- OU:Prod(파란색) - 이 OU는 OU:Root의 구성 정책을 상속합니다.
- OU:Applications(녹색) – 이 OU는 해당 OU에 적용된 구성 정책을 사용합니다.
- Account 1(녹색) - 이 계정은 해당 계정에 적용된 구성 정책을 사용합니다.
- Account 2(파란색) - 이 계정은 OU:Applications의 구성 정책을 상속합니다.
- OU:Dev(노란색) – 이 OU는 자체 관리형입니다.

- Account 3(녹색) - 이 계정은 해당 계정에 적용된 구성 정책을 사용합니다.
- Account 4(파란색) - 이 계정은 OU:Dev의 자체 관리형 동작을 상속합니다.
- OU:Test(파란색) - 이 계정은 OU:Root의 구성 정책을 상속합니다.
- Account 5(파란색) - 이 계정은 OU:Root의 구성 정책을 상속합니다. 직계 상위 항목인 OU:Test가 구성 정책과 연결되어 있지 않기 때문입니다.

구성 정책 테스트

구성 정책의 효과를 테스트하려면 조직 전체에 더 광범위하게 연결하기 전에 단일 계정이나 OU에 연결하면 됩니다.

구성 정책을 테스트하려면

1. 사용자 지정 구성 정책을 만들되, 어떤 계정에도 적용하지 않습니다. Security Hub 활성화, 표준 및 제어에 대해 지정된 설정이 올바른지 확인합니다.
2. 하위 계정이나 OU가 없는 테스트 계정 또는 OU에 구성 정책을 적용합니다.
3. 테스트 계정 또는 OU가 홈 리전 및 연결된 모든 리전에서 예상대로 구성 정책을 사용하는지 확인합니다. 또한 조직의 다른 모든 계정과 OU가 자체 관리 상태를 유지하고 각 리전에서 자체 설정을 변경할 수 있는지 확인할 수 있습니다.

단일 계정 또는 OU에서 구성 정책을 테스트한 후 다른 계정 및 OU와 연결할 수 있습니다. 정책 생성 및 연결에 대한 지침은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요. 적용된 계정의 하위 항목은 자체 관리되거나 다른 구성 정책이 적용되지 않는 한 정책을 상속합니다. 필요에 따라 구성 정책을 편집하고 추가 구성 정책을 만들 수도 있습니다.

Security Hub 구성 정책 생성 및 연결

위임된 관리자 계정은 AWS Security Hub 구성 정책을 만들고 이를 조직 계정, OU (조직 구성 단위) 또는 루트와 연결할 수 있습니다. 자체 관리형 구성을 계정, OU 또는 루트와 연결할 수도 있습니다.

구성 정책을 처음 생성하는 경우 먼저 Security Hub 구성 정책의 작동 방식 섹션을 검토하는 것이 좋습니다.

원하는 액세스 방법을 선택하고 단계에 따라 구성 정책 또는 자체 관리 구성을 만들고 연결합니다. Security Hub 콘솔을 사용하는 경우 구성을 여러 계정 또는 OU와 동시에 연결할 수 있습니다. Security Hub API 또는 AWS CLI를 사용하는 경우 각 요청에서 하나의 계정 또는 OU에만 구성을 연결할 수 있습니다.

> **Note**
>
> 중앙 구성을 사용하는 경우 Security Hub는 홈 지역을 제외한 모든 지역의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다. 구성 정책을 통해 사용하도록 선택한 기타 제어 기능은 사용 가능한 모든 지역에서 사용할 수 있습니다. 이러한 컨트롤에 대한 검색 결과를 한 지역으로만 제한하려면 AWS Config 레코더 설정을 업데이트하고 홈 지역을 제외한 모든 지역에서 글로벌 리소스 기록을 끄면 됩니다. 중앙 구성을 사용하면 홈 지역 및 연결된 지역에서 사용할 수 없는 컨트롤에 대한 적용 범위가 부족해집니다. 글로벌 리소스와 관련된 컨트롤 목록은 을 참조하십시오글로벌 리소스를 처리하는 제어.

Security Hub console

구성 정책을 만들고 연결하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 구성 및 정책 탭을 선택합니다. 그런 다음 정책 생성을 선택합니다.
3. 구성 정책을 처음 만들면 조직 구성 페이지의 구성 유형 아래에 세 가지 옵션이 표시됩니다. 구성 정책을 하나 이상 이미 만든 경우 사용자 지정 정책 옵션만 표시됩니다.

   - 권장 정책을 사용하려면 전체 조직에 AWS 권장되는 Security Hub 구성 사용을 선택합니다. 권장 정책은 모든 조직 계정에서 Security Hub를 사용하도록 설정하고, AWS 기본 보안 모범 사례 (FSBP) 표준을 사용하도록 설정하고, 모든 신규 및 기존 FSBP 제어를 활성화합니다. 제어는 기본 파라미터 값을 사용합니다.
   - 나중에 구성 정책을 만들려면 아직 구성할 준비가 되지 않았음을 선택합니다.
   - 사용자 지정 정책을 선택하여 사용자 지정 구성 정책을 생성합니다. Security Hub를 활성화 또는 비활성화할지 여부, 활성화할 표준, 해당 표준에서 활성화할 제어를 지정합니다. 필요에 따라 사용자 지정 파라미터를 지원하는 하나 이상의 활성화된 제어에 대해 사용자 지정 파라미터 값을 지정합니다.
4. 계정 섹션에서 구성 정책을 적용할 대상 계정, OU 또는 루트를 선택합니다.

   - 구성 정책을 루트에 적용하려면 모든 계정을 선택합니다. 여기에는 다른 정책이 적용되거나 상속되지 않은 조직 내 모든 계정과 OU가 포함됩니다.
   - 구성 정책을 특정 계정 또는 OU에 적용하려면 특정 계정을 선택합니다. 계정 ID를 입력하거나 조직 구조에서 계정 및 OU를 선택합니다. 정책을 생성할 때 최대 15개의 대상 (계정, OU

또는 루트) 에 정책을 적용할 수 있습니다. 더 큰 수를 지정하려면 생성 후 정책을 편집하여 추가 대상에 적용하십시오.

- 구성 정책을 현재 위임된 관리자 계정에 적용하려면 위임된 관리자만을 선택합니다.

5. 다음을 선택합니다.
6. 검토 및 배포 페이지에서 구성 정책 세부 정보를 검토합니다. 그런 다음 정책 생성 및 연결을 선택합니다. 홈 리전 및 연결된 리전에서 이 작업은 이 구성 정책과 연결된 계정의 기존 구성 설정보다 우선 적용됩니다. 계정은 적용 또는 상위 노드로부터의 상속을 통해 구성 정책에 연결될 수 있습니다. 적용된 대상의 하위 계정 및 OU는 특별히 제외되거나, 자체 관리되거나, 다른 구성 정책을 사용하지 않는 한 이 구성 정책을 자동으로 상속합니다.

Security Hub API

구성 정책을 만들고 연결하려면

1. 홈 리전의 Security Hub 위임된 관리자 계정에서 CreateConfigurationPolicy API를 호출합니다.
2. `Name`에서 구성 정책의 고유한 이름을 입력합니다. 필요에 따라 `Description`에서 구성 정책에 대한 설명을 제공할 수 있습니다.
3. `ServiceEnabled` 필드에서는 이 구성 정책에서 Security Hub를 활성화 또는 비활성화할지 여부를 지정합니다.
4. `EnabledStandardIdentifiers` 필드에서는 이 구성 정책에서 활성화할 Security Hub 표준을 지정합니다.
5. `SecurityControlsConfiguration` 개체에서는 이 구성 정책에서 활성화 또는 비활성화하려는 제어를 지정합니다. `EnabledSecurityControlIdentifiers`를 선택하면 지정된 제어가 활성화됩니다. 활성화된 표준에 속하는 다른 제어(새로 릴리스된 제어 포함)는 비활성화됩니다. `DisabledSecurityControlIdentifiers`를 선택하면 지정된 제어가 비활성화됩니다. 활성화된 표준에 속하는 다른 제어(새로 릴리스된 제어 포함)는 활성화됩니다.
6. 필요에 따라 파라미터를 사용자 지정하려는 활성화된 제어를 `SecurityControlCustomParameters` 필드에 지정할 수 있습니다. `ValueType` 필드에 `CUSTOM`을 입력하고 `Value` 필드에 사용자 지정 파라미터 값을 입력합니다. 값은 올바른 데이터 유형이어야 하며 Security Hub에서 지정한 유효한 범위 내에 있어야 합니다. 일부 제어만 사용자 지정 파라미터 값을 지원합니다. 자세한 정보는 사용자 지정 제어 파라미터을 참조하세요.
7. 구성 정책을 계정 또는 OU에 적용하려면 홈 리전의 Security Hub 위임된 관리자 계정에서 StartConfigurationPolicyAssociation API를 호출합니다.

8. ConfigurationPolicyIdentifier필드에 정책의 Amazon 리소스 이름 (ARN) 또는 범용 고유 식별자 (UUID) 를 제공하십시오. ARN과 UUID는 API에 의해 반환됩니다. CreateConfigurationPolicy 자체 관리형 구성의 경우 ConfigurationPolicyIdentifier 필드는 다음과 같습니다. SELF_MANAGED_SECURITY_HUB
9. Target 필드에는 이 구성 정책을 적용할 OU, 계정 또는 루트 ID를 입력합니다. API 요청별로 하나의 대상만 입력할 수 있습니다. 선택한 대상의 하위 계정 및 OU는 자체 관리형이거나 다른 구성 정책을 사용하지 않는 한 이 구성 정책을 자동으로 상속합니다.

구성 정책을 생성하기 위한 API 요청 예시:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
```

```
        }
    }
}
```

구성 정책을 연결하기 위한 API 요청 예시:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

구성 정책을 만들고 연결하려면

1. 홈 리전의 Security Hub 위임된 관리자 계정에서 create-configuration-policy 명령을 실행합니다.
2. name에서 구성 정책의 고유한 이름을 입력합니다. 필요에 따라 description에서 구성 정책에 대한 설명을 제공할 수 있습니다.
3. ServiceEnabled 필드에서는 이 구성 정책에서 Security Hub를 활성화 또는 비활성화할지 여부를 지정합니다.
4. EnabledStandardIdentifiers 필드에서는 이 구성 정책에서 활성화할 Security Hub 표준을 지정합니다.
5. SecurityControlsConfiguration 필드에서는 이 구성 정책에서 활성화 또는 비활성화하려는 제어를 지정합니다. EnabledSecurityControlIdentifiers를 선택하면 지정된 제어가 활성화됩니다. 활성화된 표준에 속하는 다른 제어(새로 릴리스된 제어 포함)는 비활성화됩니다. DisabledSecurityControlIdentifiers를 선택하면 지정된 제어가 비활성화됩니다. 활성화된 표준에 적용되는 다른 제어(새로 릴리스된 제어 포함)는 활성화됩니다.
6. 필요에 따라 파라미터를 사용자 지정하려는 활성화된 제어를 SecurityControlCustomParameters 필드에 지정할 수 있습니다. ValueType 필드에 CUSTOM을 입력하고 Value 필드에 사용자 지정 파라미터 값을 입력합니다. 값은 올바른 데이터 유형이어야 하며 Security Hub에서 지정한 유효한 범위 내에 있어야 합니다. 일부 제어만 사용자 지정 파라미터 값을 지원합니다. 자세한 정보는 사용자 지정 제어 파라미터을 참조하세요.

7. 구성 정책을 계정 또는 OU에 적용하려면 홈 리전의 Security Hub 위임된 관리자 계정에서 start-configuration-policy-association 명령을 실행합니다.
8. `configuration-policy-identifier` 필드에는 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. 이 ARN과 ID는 `create-configuration-policy` 명령에 의해 반환됩니다.
9. `target` 필드에는 이 구성 정책을 적용할 OU, 계정 또는 루트 ID를 입력합니다. 명령을 실행할 때마다 하나의 대상만 입력할 수 있습니다. 선택한 대상의 하위 항목은 자체 관리형이거나 다른 구성 정책을 사용하지 않는 한 이 구성 정책을 자동으로 상속합니다.

구성 정책을 만들기 위한 명령 예시:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

구성 정책을 연결하기 위한 명령 예시:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

`StartConfigurationPolicyAssociation` API는 `AssociationStatus`라는 필드를 반환합니다. 이 필드는 정책 연결이 보류 중인지 또는 성공 또는 실패 상태인지를 알려줍니다. `PENDING`에서 `SUCCESS` 또는 `FAILURE`로 상태가 변경되려면 최대 24시간이 걸릴 수 있습니다. 연결 상태에 대한 자세한 내용은 구성의 연결 상태 섹션을 참조하세요.

Security Hub 구성 정책 보기

위임된 관리자 계정은 조직의 AWS Security Hub 구성 정책 및 세부 정보를 볼 수 있습니다.

원하는 방법을 선택하고 다음 단계에 따라 정책 구성을 확인하세요.

Console

구성 정책을 보려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책책 탭을 선택하여 구성 정책의 개요를 확인합니다.
4. 구성 정책과 세부 정보 보기를 차례로 선택하여 해당 정책에 대한 추가 세부 정보를 확인합니다.

API

구성 정책을 보려면

모든 구성 정책의 요약 목록을 보려면 홈 리전의 Security Hub 위임된 관리자 계정에서 `ListConfigurationPolicies` API를 호출합니다. 필요에 따라 페이지 매김 파라미터를 제공할 수도 있습니다.

API 요청 예시:

```
{
    "MaxResults": 5,
    "NextToken": "U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf"
}
```

특정 구성 정책에 대한 세부 정보를 보려면 홈 리전의 Security Hub 위임된 관리자 계정에서 `GetConfigurationPolicy` API를 호출합니다. 세부 정보를 확인할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.

API 요청 예시:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

모든 구성 정책 및 연결의 요약 목록을 보려면 홈 리전의 Security Hub 위임된 관리자 계정에서 ListConfigurationPolicyAssociations API를 호출합니다. 필요에 따라 페이지 매김 파라미터를 제공하거나 특정 정책 ID, 연결 유형 또는 연결 상태를 기준으로 결과를 필터링할 수 있습니다.

API 요청 예시:

```
{
    "AssociationType": "APPLIED"
}
```

특정 계정, OU 또는 루트에 대한 연결을 보려면 홈 리전의 Security Hub 위임된 관리자 계정에서 GetConfigurationPolicyAssociation 또는 BatchGetConfigurationPolicyAssociations API를 호출합니다. Target에서 계정 번호, OU ID 또는 루트 ID를 입력합니다.

```
{
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

구성 정책을 보려면

모든 구성 정책의 요약 목록을 보려면 홈 리전의 Security Hub 위임된 관리자 계정에서 list-configuration-policies 명령을 실행합니다.

명령 예시:

```
aws securityhub --region us-east-1 list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

특정 구성 정책에 대한 세부 정보를 보려면 홈 리전의 Security Hub 위임된 관리자 계정에서 get-configuration-policy 명령을 실행합니다. 세부 정보를 확인할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.

```
aws securityhub --region us-east-1 get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

모든 구성 정책 및 해당 계정 연결의 요약 목록을 보려면 홈 리전의 Security Hub 위임된 관리자 계정에서 list-configuration-policy-associations 명령을 실행합니다. 필요에 따라 페이지 매김 파라미터를 제공하거나 특정 정책 ID, 연결 유형 또는 연결 상태를 기준으로 결과를 필터링할 수 있습니다.

```
aws securityhub --region us-east-1 list-configuration-policy-associations \
--association-type "APPLIED"
```

특정 계정의 연결을 보려면 홈 리전의 Security Hub 위임된 관리자 계정에서 get-configuration-policy-association 또는 batch-get-configuration-policy-associations 명령을 실행합니다. target에서 계정 번호, OU ID 또는 루트 ID를 입력합니다.

```
aws securityhub --region us-east-1 get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

구성의 연결 상태

다음 중앙 구성 API 작업은 AssociationStatus 필드를 반환합니다.

- BatchGetConfigurationPolicyAssociations
- GetConfigurationPolicyAssociation
- ListConfigurationPolicyAssociations
- StartConfigurationPolicyAssociation

이 필드는 기본 구성이 구성 정책인 경우와 자체 관리형 동작인 경우 모두 반환됩니다.

AssociationStatus의 값은 정책 연결이 보류 중인지 또는 성공 또는 실패 상태인지를 알려줍니다. PENDING에서 SUCCESS 또는 FAILURE로 상태가 변경되려면 최대 24시간이 걸릴 수 있습니다. 상위 OU 또는 루트의 연결 상태는 해당 하위 항목의 상태에 따라 달라집니다. 모든 하위 항목의 연결 상태가 SUCCESS인 경우 상위 항목의 연결 상태는 SUCCESS입니다. 하위 항목 하나 이상의 연결 상태가 FAILED인 경우 상위 항목의 연결 상태는 FAILED입니다.

AssociationStatus의 값 또한 모든 리전에 따라 다릅니다. 홈 리전 및 연결된 모든 리전에서 연결이 성공하면 AssociationStatus의 값은 SUCCESS입니다. 이러한 리전 중 하나 이상에서 연결이 실패할 경우 AssociationStatus의 값은 FAILED입니다.

다음과 같은 동작은 AssociationStatus의 값에도 영향을 미칩니다.

- 대상이 상위 OU이거나 루트인 경우 모든 하위 항목이 SUCCESS 또는 FAILED 상태일 때만 AssociationStatus가 SUCCESS 또는 FAILED입니다. 상위 항목을 구성에 처음 연결한 후 하위 계정 또는 OU의 연결 상태가 변경되는 경우(예: 연결된 리전이 추가 또는 제거되는 경우), StartConfigurationPolicyAssociation API를 다시 호출하지 않는 한 상위 항목의 연결 상태가 업데이트되지 않습니다.
- 대상이 계정이면, 홈 리전 및 연결된 모든 리전에서 연결 결과가 SUCCESS 또는 FAILED인 경우에만 AssociationStatus가 SUCCESS 또는 FAILED입니다. 대상 계정을 구성과 처음 연결한 후 대상 계정의 연결 상태가 변경되면(예: 연결된 리전이 추가 또는 제거되는 경우), 해당 연결 상태가 업데이트됩니다. 하지만 StartConfigurationPolicyAssociation API를 다시 호출하지 않는 한 변경으로 인해 상위 항목의 연결 상태가 업데이트되지 않습니다.

새 연결된 리전을 추가하는 경우 Security Hub는 새 리전의 PENDING, SUCCESS 또는 FAILED 상태에 있는 기존 연결을 복제합니다.

일반적인 연결 실패 이유

다음과 같은 일반적인 이유로 구성 정책 연결이 실패할 수 있습니다.

- Organizations 관리 계정이 구성원이 아님 – 구성 정책을 Organizations 관리 계정과 연결하려면 해당 계정에 Security Hub가 이미 활성화되어 있어야 합니다. 여기에는 관리 계정과 조직의 모든 구성원 계정이 포함됩니다.
- AWS Config가 활성화되지 않았거나 제대로 구성되어 있지 않음 - 구성 정책에서 표준을 활성화하려면 관련 리소스를 기록하도록 AWS Config를 활성화하고 구성해야 합니다.
- 위임된 관리자 계정에서 연결해야 함 - 위임된 관리자 계정에 로그인한 경우에만 대상 계정 및 OU에 정책을 연결할 수 있습니다.

- 홈 리전에서 연결해야 함 - 홈 리전에 로그인한 경우에만 대상 계정 및 OU에 정책을 연결할 수 있습니다.
- 옵트인 영역이 활성화되지 않음 – 위임된 관리자가 활성화하지 않은 옵트인 리전인 경우 연결된 리전의 구성원 계정 또는 OU에 대한 정책 연결이 실패합니다. 위임된 관리자 계정에서 리전을 활성화한 후 다시 시도할 수 있습니다.
- 구성원 계정 일시 중단됨 – 정책을 일시 중지된 구성원 계정과 연결하려고 하면 정책 연결이 실패합니다.

Security Hub 구성 정책 업데이트

위임된 관리자 계정은 필요에 따라 AWS Security Hub 구성 정책을 업데이트할 수 있습니다. 위임된 관리자는 정책 설정, 정책이 연결된 계정이나 OU 또는 둘 다를 업데이트할 수 있습니다. 정책 설정이 업데이트되면 구성 정책에 연결된 계정이 업데이트된 정책을 자동으로 사용하기 시작합니다.

구성 정책을 만들 때와 마찬가지로 다음 정책 설정을 업데이트할 수 있습니다.

- Security Hub를 활성화하거나 비활성화합니다.
- 하나 이상의 보안 표준을 활성화합니다.
- 활성화된 표준 전반에서 어떤 보안 제어를 사용할 수 있는지 표시합니다. 이를 위해 활성화해야 하는 특정 제어 목록을 제공할 수 있습니다. 그러면 Security Hub에서 새 제어가 릴리스될 때 새 제어를 포함한 다른 모든 제어를 비활성화합니다. 또는 비활성화해야 하는 특정 제어의 목록을 제공할 수 있습니다. 그러면 Security Hub에서 새 제어가 릴리스될 때 이를 포함하여 다른 모든 제어를 활성화합니다.
- 사용 가능한 표준에서 사용할 수 있는 제어를 선택할 수 있도록 파라미터를 사용자 지정할 수도 있습니다.

원하는 방법을 선택하고 다음 단계에 따라 구성 정책을 업데이트하세요.

중앙 구성을 사용하는 경우 Security Hub는 홈 지역을 제외한 모든 지역의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다. 구성 정책을 통해 사용하도록 선택한 기타 제어 기능은 사용 가능한 모든 지역에서 사용할 수 있습니다. 이러한 컨트롤에 대한 검색 결과를 한 지역으로만 제한하려면 AWS Config 레코더 설정을 업데이트하고 홈 지역을 제외한 모든 지역에서 글로벌 리소스 기록을 끄면 됩니다. 중앙 구성을 사용하면 홈 지역 및 연결된 지역에서 사용할 수 없는 컨트롤에 대한 적용 범위가 부족해집니다. 글로벌 리소스와 관련된 컨트롤 목록은 을 참조하십시오글로벌 리소스를 처리하는 제어.

Console

구성 정책을 업데이트하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭을 선택합니다.
4. 편집할 구성 정책을 선택하고 편집을 선택합니다. 원하는 경우 정책 설정을 편집합니다. 정책 설정을 변경하지 않으려면 이 섹션을 그대로 둡니다.
5. 다음을 선택합니다. 원하는 경우 정책 연결을 편집합니다. 정책 연결을 변경하지 않으려면 이 섹션을 그대로 둡니다. 정책을 업데이트할 때 최대 15개의 대상 (계정, OU 또는 루트) 에 정책을 연결하거나 연결을 끊을 수 있습니다.
6. 다음을 선택합니다.
7. 변경 사항을 검토하고 저장 및 적용을 선택합니다. 홈 리전 및 연결된 리전에서 이 작업은 이 구성 정책과 연결된 계정의 기존 구성 설정보다 우선 적용됩니다. 계정은 적용 또는 상위 노드로부터의 상속을 통해 구성 정책에 연결될 수 있습니다.

API

구성 정책을 업데이트하려면

1. 구성 정책의 설정을 업데이트하려면 홈 리전의 Security Hub 위임된 관리자 계정에서 UpdateConfigurationPolicy API를 호출합니다.
2. 업데이트할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. `ConfigurationPolicy` 아래 필드에 업데이트된 값을 입력합니다. 필요에 따라 업데이트 이유를 입력할 수도 있습니다.
4. 이 구성 정책에 새 연결을 추가하려면 홈 리전의 Security Hub 위임된 관리자 계정에서 StartConfigurationPolicyAssociation API를 호출합니다. 현재 연결을 하나 이상 제거하려면 홈 리전의 Security Hub 위임된 관리자 계정에서 StartConfigurationPolicyDisassociation API를 호출합니다.
5. `ConfigurationPolicyIdentifier` 필드에는 연결을 업데이트하려는 구성 정책의 ARN 또는 ID를 입력합니다.
6. `Target` 필드에 연결하거나 연결 해제하려는 계정, OU 또는 루트 ID를 입력합니다. 이 작업은 지정된 OU 또는 계정에 대한 이전 정책 연결을 무시합니다.

> **Note**
>
> `UpdateConfigurationPolicy` API를 호출하면 Security Hub는 `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` 및 `SecurityControlCustomParameters` 필드의 전체 목록 대체를 수행합니다. 이 API를 호출할 때마다 활성화하려는 표준의 전체 목록과 활성화 또는 비활성화하고 파라미터를 사용자 지정하려는 제어의 전체 목록을 제공하세요.

구성 정책을 업데이트하기 위한 API 요청 예시:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
```

```
                    }
                ]
            }
        }
    }
}
```

AWS CLI

구성 정책을 업데이트하려면

1. 구성 정책의 설정을 업데이트하려면 홈 리전의 Security Hub 위임된 관리자 계정에서 update-configuration-policy 명령을 실행합니다.
2. 업데이트할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. `configuration-policy` 아래 필드에 업데이트된 값을 입력합니다. 필요에 따라 업데이트 이유를 입력할 수도 있습니다.
4. 이 구성 정책에 새 연결을 추가하려면 홈 리전의 Security Hub 위임된 관리자 계정에서 start-configuration-policy-association 명령을 실행합니다. 현재 연결을 하나 이상 제거하려면 홈 리전의 Security Hub 위임된 관리자 계정에서 start-configuration-policy-disassociation 명령을 실행합니다.
5. `configuration-policy-identifier` 필드에는 연결을 업데이트하려는 구성 정책의 ARN 또는 ID를 입력합니다.
6. `target` 필드에 연결하거나 연결 해제하려는 계정, OU 또는 루트 ID를 입력합니다. 이 작업은 지정된 OU 또는 계정에 대한 이전 정책 연결을 무시합니다.

> **Note**
>
> `update-configuration-policy` 명령을 실행하면 Security Hub에서 `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` 및 `SecurityControlCustomParameters` 필드의 전체 목록 대체를 수행합니다. 이 명령을 실행할 때마다 활성화하려는 표준의 전체 목록과 활성화 또는 비활성화하고 파라미터를 사용자 지정하려는 제어의 전체 목록을 제공하세요.

구성 정책을 업데이트하기 위한 명령 예시:

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

StartConfigurationPolicyAssociation API는 AssociationStatus라는 필드를 반환합니다. 이 필드는 정책 연결이 보류 중인지 또는 성공 또는 실패 상태인지를 알려줍니다. PENDING에서 SUCCESS 또는 FAILURE로 상태가 변경되려면 최대 24시간이 걸릴 수 있습니다. 연결 상태에 대한 자세한 내용은 구성의 연결 상태 섹션을 참조하세요.

Security Hub 구성 정책 삭제 및 연결 해제

위임된 관리자 계정은 AWS Security Hub 구성 정책을 삭제할 수 있습니다. 또는 위임된 관리자 계정이 구성 정책을 유지하되 특정 계정이나 OU(조직 단위)와의 연결을 해제할 수도 있습니다.

다음 섹션에서는 두 가지 옵션에 대해 설명합니다.

구성 정책 삭제

구성 정책을 삭제하면 해당 구성 정책은 조직에 더 이상 존재하지 않습니다. 대상 계정, OU 및 조직 루트는 더 이상 구성 정책을 사용할 수 없습니다. 삭제된 구성 정책과 연결된 대상은 가장 가까운 상위 항목의 구성 정책을 상속하거나 가장 가까운 상위 그룹이 자체 관리형인 경우 자체 관리형이 됩니다. 대상이 다른 구성을 사용하도록 하려면 대상을 새 구성 정책에 연결하세요. 자세한 내용은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요.

적절한 보안 범위를 제공하려면 구성 정책을 하나 이상 만들어 조직에 연결하는 것이 좋습니다.

구성 정책을 삭제하려면 먼저 해당 정책이 현재 적용되는 계정, OU 또는 루트에서 정책을 연결 해제해야 합니다.

원하는 방법을 선택하고 다음 단계에 따라 구성 정책을 삭제하세요.

Console

구성 정책을 삭제하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭을 선택합니다. 삭제하려는 구성 정책을 선택한 다음, 삭제를 선택합니다. 구성 정책이 여전히 계정이나 OU와 연결되어 있는 경우 정책을 삭제하기 전에 먼저 해당 대상에서 정책을 연결 해제하라는 메시지가 표시됩니다.
4. 확인 메시지를 검토합니다. **`confirm`**를 입력한 다음 삭제를 선택합니다.

API

구성 정책을 삭제하려면

홈 리전의 Security Hub 위임된 관리자 계정에서 DeleteConfigurationPolicy API를 호출합니다.

삭제할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. `ConflictException` 오류가 발생하더라도 구성 정책은 조직의 계정 또는 OU에 계속 적용됩니다. 오류를 해결하려면 구성 정책을 삭제하기 전에 이러한 계정이나 OU에서 구성 정책을 연결 해제하세요.

구성 정책을 삭제하기 위한 API 요청 예시:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

구성 정책을 삭제하려면

홈 리전의 Security Hub 위임된 관리자 계정에서 delete-configuration-policy 명령을 실행합니다.

삭제할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. `ConflictException` 오류가 발생하더라도 구성 정책은 조직의 계정 또는 OU에 계속 적용됩니다. 오류를 해결하려면 구성 정책을 삭제하기 전에 이러한 계정이나 OU에서 구성 정책을 연결 해제하세요.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

계정 및 OU에서 구성 연결 해제

위임된 관리자 계정에서 현재 적용되는 구성 정책이나 자체 관리형 구성에서 대상 계정, OU 또는 루트를 연결 해제할 수 있습니다. 적용된 구성에서만 대상을 연결 해제할 수 있으며 상속된 구성에서는 연결을 해제할 수 없습니다. 상속된 구성을 변경하려면 영향을 받는 계정 또는 OU에 구성 정책 또는 자체 관리형 동작을 적용할 수 있습니다. 원하는 수정 사항이 포함된 새 구성 정책을 가장 가까운 상위 항목에 적용할 수도 있습니다.

연결을 해제해도 구성 정책은 삭제되지 않습니다. 정책은 계정에 유지되므로 조직의 다른 대상과 연결할 수 있습니다. 연결 해제가 완료되면 영향을 받는 대상은 가장 가까운 상위 항목의 구성 정책 또는 자체 관리형 동작을 상속합니다. 상속 가능한 구성이 없는 경우 대상은 연결 해제 이전의 설정을 유지하지만 자체 관리형이 됩니다.

원하는 방법을 선택하고 단계에 따라 계정, OU 또는 루트를 현재 구성에서 연결 해제하세요.

Console

현재 구성에서 계정 또는 OU의 연결을 해제하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. Organizations 탭에서 현재 구성과 연결 해제하려는 계정, OU 또는 루트를 선택합니다. 편집을 선택합니다.
4. 위임된 관리자가 대상에 직접 정책을 적용할 수 있도록 하려면 구성 정의 페이지의 관리에서 정책 적용을 선택합니다. 대상이 가장 가까운 상위 항목의 구성을 상속하도록 하려면 상속을 선택합니다. 두 경우 모두 위임된 관리자가 대상의 설정을 제어합니다. 계정이나 OU에서 자체 설정을 제어하도록 하려면 자체 관리형을 선택합니다.

5. 변경 사항을 검토한 후 다음을 선택하고 적용을 선택합니다. 이 작업은 범위 내에 있는 계정 또는 OU의 기존 구성이 현재 선택 항목과 충돌하는 경우 해당 구성을 무시합니다.

API

현재 구성에서 계정 또는 OU의 연결을 해제하려면

1. 홈 리전의 Security Hub 위임된 관리자 계정에서 StartConfigurationPolicyDisassociation API를 호출합니다.
2. `ConfigurationPolicyIdentifier`에는 연결을 해제하려는 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. 자체 관리형 동작을 분리하려면 이 필드에 `SELF_MANAGED_SECURITY_HUB`를 입력합니다.
3. `Target`에서는 이 구성 정책에서 연결 해제하려는 계정, OU 또는 루트를 입력합니다.

구성 정책의 연결을 해제하기 위한 API 요청 예시:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

현재 구성에서 계정 또는 OU의 연결을 해제하려면

1. 홈 리전의 Security Hub 위임된 관리자 계정에서 start-configuration-policy-disassociation 명령을 실행합니다.
2. `configuration-policy-identifier`에는 연결을 해제하려는 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. 자체 관리형 동작을 분리하려면 이 필드에 `SELF_MANAGED_SECURITY_HUB`를 입력합니다.
3. `target`에서는 이 구성 정책에서 연결 해제하려는 계정, OU 또는 루트를 입력합니다.

구성 정책의 연결을 해제하기 위한 명령 예시:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
```

```
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

표준 또는 제어 컨텍스트에서의 중앙 구성

AWS Security Hub 콘솔의 구성 페이지에서 또는 특정 보안 표준 또는 보안 제어의 컨텍스트에서 중앙 구성을 사용할 수 있습니다. 컨텍스트별로 이 기능을 사용하면 기존 워크플로와 통합된 방식으로 조직 전체에 표준 및 제어를 구성할 수 있습니다. 또한 결과를 검토하면서 환경에 가장 적합한 표준 및 제어를 발견하고 동시에 구성할 수 있습니다.

컨텍스트별 구성은 Security Hub 콘솔에서만 사용할 수 있습니다. 프로그래밍 방식으로 UpdateConfigurationPolicy API를 호출하여 조직의 특정 표준 또는 제어 구성 방식을 변경해야 합니다.

컨텍스트별 보안 표준 구성

단계에 따라 중앙 구성을 통해 컨텍스트별로 보안 표준을 구성하세요.

컨텍스트별로 보안 표준을 구성하려면(콘솔만 해당)

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 보안 표준을 선택합니다.
3. 구성하려는 표준에 대해 구성을 선택합니다. 특정 표준을 선택한 다음 표준 세부 정보 페이지에서 구성을 선택할 수도 있습니다. 콘솔에는 기존 Security Hub 구성 정책(구성 정책)과 각 정책의 이 표준 상태가 나열됩니다.
4. 각 구성 정책에서 옵션을 선택하여 표준을 활성화하거나 비활성합니다.
5. 변경한 후 다음을 선택합니다.
6. 변경 사항을 검토하고 적용을 선택합니다. 이 작업은 구성 정책과 연결된 모든 계정 및 OU에 영향을 줍니다. 구성은 홈 리전 및 연결된 모든 리전에 적용됩니다.

컨텍스트별 보안 제어 구성

단계에 따라 중앙 구성을 통해 컨텍스트별로 보안 제어를 구성하세요.

컨텍스트별로 보안 제어를 구성하려면(콘솔만 해당)

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 제어를 선택합니다.
3. 특정 컨트롤을 선택한 다음 구성을 선택합니다. 콘솔에는 현재 구성 정책과 각 정책의 이 제어 상태가 나열됩니다.
4. 각 구성 정책에서 옵션을 선택하여 제어를 활성화하거나 비활성합니다. 제어 파라미터를 사용자 지정하도록 선택할 수도 있습니다.
5. 변경한 후 다음을 선택합니다.
6. 변경 사항을 검토하고 적용을 선택합니다. 이 작업은 구성 정책과 연결된 모든 계정 및 OU에 영향을 줍니다. 구성은 홈 리전 및 연결된 모든 리전에 적용됩니다.

중앙 구성 사용 중지

AWS Security Hub에서 중앙 구성 사용을 중지하면 위임된 관리자는 여러 AWS 계정, OU(조직 단위) 및 AWS 리전에서 Security Hub, 보안 표준 및 보안 제어를 구성할 수 없게 됩니다. 대신 조직 계정은 대부분의 자체 설정을 각 리전에서 개별적으로 구성해야 합니다.

> **Important**
>
> 중앙 구성 사용을 중단하려면 먼저 구성 정책이든 자체 관리형 동작이든 관계없이 현재 구성에서 계정과 OU의 연결을 해제해야 합니다.
> 중앙 구성 사용을 중지하려면 먼저 구성 정책도 삭제해야 합니다.

중앙 구성을 중지하면 다음과 같은 변경 사항이 발생합니다.

- 위임된 관리자는 더 이상 조직에 대한 구성 정책을 만들 수 없습니다.
- 구성 정책이 적용되거나 상속된 계정은 현재 설정이 유지되지만 자체 관리형이 됩니다.
- 조직이 로컬 구성으로 전환합니다. 로컬 구성에서는 대부분의 Security Hub 설정을 각 조직 계정 및 리전에서 개별적으로 구성해야 합니다. 위임된 관리자는 Security Hub, 기본 보안 표준 및 새 조직 계정의 기본 표준에 속하는 모든 제어를 자동으로 활성화하도록 선택할 수 있습니다. 기본 보안 표준은 AWS 기본 보안 모범 사례(FSBP) 표준과 CIS(인터넷 보안 센터) AWS 파운데이션 벤치마크 v1.2.0입니다. 이러한 설정은 현재 리전에만 적용되며 새 조직 계정에만 영향을 미칩니다. 위임된 관리자는

기본값인 표준을 변경할 수 없습니다. 로컬 구성에서는 구성 정책 또는 OU 수준의 구성 사용을 지원하지 않습니다.

중앙 구성 사용을 중지해도 위임된 관리자 계정의 ID는 동일하게 유지됩니다. 홈 리전과 연결된 리전도 동일하게 유지됩니다(홈 리전은 이제 집계 영역이라고 하며 결과 집계에 사용할 수 있음).

원하는 방법을 선택하고 단계에 따라 중앙 구성 사용을 중단하고 로컬 구성으로 전환하세요.

Security Hub console

중앙 구성 사용을 중지하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 개요 섹션에서 편집을 선택합니다.
4. 조직 구성 편집 상자에서 로컬 구성을 선택합니다. 아직 연결을 해제하지 않은 경우 중앙 구성을 중지하려면 먼저 현재 구성 정책을 연결 해제하고 삭제하라는 메시지가 표시됩니다. 자체 관리형으로 지정된 계정 또는 OU는 자체 관리형 구성과의 연결을 해제해야 합니다. 콘솔에서 각 자체 관리형 계정 또는 OU의 관리 유형을 중앙 관리형 및 내 조직에서 상속으로 변경하여 이 작업을 수행할 수 있습니다.
5. 필요에 따라 새 조직 계정의 로컬 구성 기본 설정을 선택합니다.
6. 확인을 선택합니다.

Security Hub API

중앙 구성 사용을 중지하려면

1. UpdateOrganizationConfiguration API를 호출합니다.
2. `OrganizationConfiguration` 객체의 `ConfigurationType` 필드를 `LOCAL`로 설정합니다. 기존 구성 정책 또는 정책 연결이 있는 경우 API는 오류를 반환합니다. 구성 정책을 연결 해제하려면 `StartConfigurationPolicyDisassociation` API를 호출합니다. 구성 정책을 삭제하려면 `DeleteConfigurationPolicy` API를 호출합니다.
3. 새 조직 계정에서 Security Hub를 자동으로 활성화하려면 `AutoEnable` 필드를 `true`로 설정합니다. 기본적으로 이 필드의 값은 `false`이며 Security Hub는 새 조직 계정에서 자동으로 활성화되지 않습니다. 필요에 따라 새 조직 계정에서 기본 보안 표준을 자동으로 활성화하려

면 AutoEnableStandards 필드를 DEFAULT로 설정합니다. 이것이 기본값입니다. 새 조직 계정에서 기본 보안 표준을 자동으로 활성화하지 않으려면 AutoEnableStandards 필드를 NONE로 설정합니다.

API 요청 예시:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

중앙 구성 사용을 중지하려면

1. update-organization-configuration 명령을 실행합니다.
2. organization-configuration 객체의 ConfigurationType 필드를 LOCAL로 설정합니다. 기존 구성 정책 또는 정책 연결이 있는 경우 이 명령은 오류를 반환합니다. 구성 정책을 연결 해제하려면 start-configuration-policy-disassociation 명령을 실행합니다. 구성 정책을 삭제하려면 delete-configuration-policy 명령을 실행합니다.
3. 새 조직 계정에서 Security Hub를 자동으로 활성화하려면 auto-enable 파라미터를 포함합니다. 기본적으로 이 파라미터의 값은 no-auto-enable이며 Security Hub는 새 조직 계정에서 자동으로 활성화되지 않습니다. 필요에 따라 새 조직 계정에서 기본 보안 표준을 자동으로 활성화하려면 auto-enable-standards 필드를 DEFAULT로 설정합니다. 이것이 기본값입니다. 새 조직 계정에서 기본 보안 표준을 자동으로 활성화하지 않으려면 auto-enable-standards 필드를 NONE로 설정합니다.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

관리자 및 구성원 계정 관리

AWS 환경에 계정이 여러 개 있는 경우 AWS Security Hub를 사용하는 계정을 구성원 계정으로 취급하여 단일 관리자 계정에 연결할 수 있습니다. 관리자는 전반적인 보안 태세를 모니터링하고 구성원 계정에 대해 허용된 작업을 수행할 수 있습니다. 또한 관리자는 예상 사용 비용 모니터링 및 계정 할당량 평가와 같은 다양한 계정 관리 및 관리 작업을 대규모로 수행할 수 있습니다.

Security Hub를 AWS Organizations와 통합하거나 Security Hub에서 구성원 초대를 수동으로 보내고 수락하는 두 가지 방법으로 구성원 계정을 관리자와 연결할 수 있습니다.

AWS Organizations를 사용하여 계정 관리

AWS Organizations는 AWS 관리자가 여러 AWS 계정을 통합하고 관리할 수 있는 글로벌 계정 관리 서비스입니다. 예산, 보안 및 규정 준수 요구 사항을 지원하도록 설계된 계정 관리 및 통합 결제 기능을 제공합니다. 추가 비용 없이 제공되며 AWS Security Hub, Amazon Macie 및 Amazon GuardDuty를 포함한 여러 AWS 서비스와 통합됩니다. 자세한 내용은 AWS Organizations 사용 설명서를 참조하세요.

Security Hub를 AWS Organizations와 통합할 때 Organizations 관리 계정은 Security Hub 위임된 관리자를 지정합니다. Security Hub는 지정된 AWS 리전의 위임된 관리자 계정에서 자동으로 활성화됩니다.

위임된 관리자를 지정한 후에는 중앙 구성을 사용하여 Security Hub에서 계정을 관리하는 것이 좋습니다. 이는 Security Hub를 사용자 지정하고 조직에 적절한 보안 범위를 보장하는 가장 효율적인 방법입니다.

중앙 구성을 사용하면 위임된 관리자가 리전별로 구성하는 대신 여러 조직 계정 및 리전에서 Security Hub를 사용자 지정할 수 있습니다. 전체 조직에 대한 구성 정책을 만들거나 계정 및 OU별로 다른 구성 정책을 만들 수 있습니다. 정책은 관련 계정에서 Security Hub를 활성화 또는 비활성화할지 여부와 활성화되는 보안 표준 및 제어를 지정합니다.

위임된 관리자는 계정을 중앙 관리형 계정 또는 자체 관리형 계정으로 지정할 수 있습니다. 중앙 관리형 계정은 위임된 관리자만 구성할 수 있습니다. 자체 관리형 계정은 자체 설정을 지정할 수 있습니다.

중앙 구성을 선택하지 않으면 위임된 관리자가 Security Hub를 구성할 수 있는 권한이 더 제한되며, 이를 로컬 구성이라고 합니다. 로컬 구성에서 위임된 관리자는 현재 리전의 새 조직 계정에서 Security Hub 및 기본 보안 표준을 자동으로 활성화할 수 있습니다. 하지만 기존 계정에서는 이러한 설정을 사용하지 않으므로 계정이 조직에 가입한 후에 구성 드리프트가 발생할 수 있습니다.

이러한 새 계정 설정 외에도 로컬 구성은 계정별 및 리전별로 다릅니다. 각 조직 계정은 각 리전에서 Security Hub 서비스, 표준 및 제어를 개별적으로 구성해야 합니다. 또한 로컬 구성에서는 구성 정책 사용을 지원하지 않습니다.

초대를 통한 수동 계정 관리

독립형 계정이 있는 경우 또는 Organizations와 통합하지 않는 경우 Security Hub에서 초대를 받아 구성원 계정을 수동으로 관리해야 합니다. 독립형 계정은 Organizations와 통합할 수 없으므로 수동으로 관리해야 합니다. 나중에 계정을 추가할 경우 AWS Organizations와 통합하고 중앙 구성을 사용하는 것이 좋습니다.

수동 계정 관리를 사용하는 경우 계정을 Security Hub 관리자로 지정합니다. 관리자 계정은 구성원 계정의 데이터를 보고 구성원 계정 결과에 대해 특정 작업을 수행할 수 있습니다. Security Hub 관리자는 다른 계정을 구성원 계정으로 초대하며, 예비 구성원 계정이 초대를 수락하면 관리자-구성원 관계가 성립됩니다.

수동 계정 관리는 구성 정책 사용을 지원하지 않습니다. 구성 정책이 없으면 관리자는 여러 계정에 대한 변수 설정을 구성하여 Security Hub를 중앙에서 사용자 지정할 수 없습니다. 대신 각 조직 계정은 각 리전에서 개별적으로 Security Hub를 활성화하고 구성해야 합니다. 이로 인해 Security Hub를 사용하는 모든 계정 및 리전에서 적절한 보안 범위를 보장하는 것이 더 어려워지고 시간이 많이 소요될 수 있습니다. 또한 구성원 계정이 관리자의 입력 없이 자체 설정을 지정할 수 있기 때문에 구성 드리프트가 발생할 수 있습니다.

초대를 통해 계정을 관리하려면 초대를 통한 계정 관리 섹션을 참조하세요.

를 통한 계정 관리 AWS Organizations

Security Hub를 조직 내 AWS Security Hub 계정과 AWS Organizations통합한 다음 해당 계정의 Security Hub를 관리할 수 있습니다.

Security Hub를 AWS Organizations통합하려면 에서 조직을 만들어야 AWS Organizations합니다. Organizations 관리 계정은 계정 하나를 해당 조직에 대해 Security Hub 위임된 관리자로 지정합니다. 그러면 위임된 관리자는 조직의 다른 계정에 대해 Security Hub를 활성화하고, 해당 계정을 Security Hub 구성원 계정으로 추가하고, 구성원 계정에 대해 허용된 작업을 수행할 수 있습니다. Security Hub 위임된 관리자는 최대 10,000개의 구성원 계정에 대해 Security Hub를 활성화하고 관리할 수 있습니다.

위임된 관리자의 구성 기능 범위는 중앙 구성을 사용하는지 여부에 따라 달라집니다. 중앙 구성을 사용하면 각 구성원 계정 및 AWS 리전에서 개별적으로 Security Hub를 구성할 필요가 없습니다. 위임된 관

리자는 여러 리전의 지정된 구성원 계정 및 OU(조직 단위)에서 특정 Security Hub 설정을 적용할 수 있습니다.

Security Hub 관리자 계정은 구성원 계정에 대해 다음 작업을 수행할 수 있습니다.

- 중앙 구성을 사용하는 경우 Security Hub 구성 정책을 생성하여 구성원 계정 및 OU에 대한 Security Hub를 중앙에서 구성하세요. 구성 정책을 사용하여 Security Hub를 활성화 및 비활성화하고, 표준을 활성화 및 비활성화하고, 제어를 활성화 및 비활성화할 수 있습니다.
- 새 계정이 조직에 추가될 때 자동으로 새 계정을 Security Hub 구성원 계정으로 취급합니다. 중앙 구성을 사용하는 경우 OU와 관련된 구성 정책에는 OU에 속한 기존 계정 및 새 계정이 포함됩니다.
- 기존 조직 계정을 Security Hub 구성원 계정으로 취급합니다. 이는 중앙 구성을 사용하면 자동으로 이루어집니다.
- 조직에 속한 구성원 계정을 연결 해제하세요. 중앙 구성을 사용하는 경우 구성원 계정을 자체 관리형으로 지정한 후에만 구성원 계정을 연결 해제할 수 있습니다. 또는 Security Hub를 비활성화하는 구성 정책을 특정한 중앙 관리형 구성원 계정과 연결할 수 있습니다.

위임된 관리자가 구성원 계정에 대해 수행할 수 있는 전체 작업 목록은 계정에 허용된 작업 섹션을 참조하세요.

이 섹션의 항목에서는 Security Hub를 조직 내 계정과 통합하는 방법 AWS Organizations 및 Security Hub를 관리하는 방법을 설명합니다. 관련된 경우, 각 섹션에서는 중앙 구성 사용자를 위한 관리상의 이점과 차이점을 설명합니다.

주제

- Security Hub와 통합 AWS Organizations
- 새 조직 계정에서 Security Hub 자동 활성화
- 새 조직 계정에서 Security Hub를 수동으로 활성화하기
- 조직에서 구성원 계정 연결 해제

Security Hub와 통합 AWS Organizations

AWS Security Hub 통합하려면 AWS Organizations Organizations에서 조직을 만들고 조직 관리 계정을 사용하여 위임된 Security Hub 관리자 계정을 지정합니다. 이를 통해 Security Hub는 Organizations에서 신뢰할 수 있는 서비스가 될 수 있습니다. 또한 위임된 관리자 계정에 AWS 리전 대해 현재 Security Hub를 활성화하고, 위임된 관리자는 구성원 계정에 대해 Security Hub를 활성화하고, 구성원 계정의 데이터를 보고, 구성원 계정에 대해 허용된 기타 작업을 수행할 수 있습니다.

중앙 구성을 사용하는 경우 위임된 관리자는 Security Hub 서비스, 표준 및 제어를 조직 계정에서 어떻게 구성하는지 지정하는 Security Hub 구성 정책을 만들 수도 있습니다.

조직 생성

조직은 단일 단위로 관리할 수 AWS 계정 있도록 통합하기 위해 만든 엔티티입니다.

AWS Organizations 콘솔을 사용하거나 SDK API 중 하나 AWS CLI 또는 하나의 명령을 사용하여 조직을 만들 수 있습니다. 자세한 지침은 AWS Organizations 사용 설명서의 조직 생성을 참조하세요.

를 AWS Organizations 사용하여 조직 내 모든 계정을 중앙에서 보고 관리할 수 있습니다. 조직은 관리 계정 하나와 0개 이상의 구성원 계정을 갖습니다. 위에는 루트, 아래에는 조직 단위(OU)가 있는 나무형 계층 구조로 계정을 조직할 수 있습니다. 각 계정은 루트 아래 바로 배치하거나, 계층 구조 내의 OU 중 하나에 배치할 수 있습니다. OU는 특정 계정을 담는 컨테이너입니다. 예를 들어 재무 운영과 관련된 모든 계정이 포함된 재무 OU를 만들 수 있습니다.

위임된 Security Hub 관리자 선택을 위한 권장 사항

수동 초대 프로세스에서 가져온 관리자 계정을 사용하여 계정 관리로 AWS Organizations전환하려는 경우 해당 계정을 위임된 Security Hub 관리자로 지정하는 것이 좋습니다.

Security Hub API와 콘솔에서는 조직 관리 계정을 위임된 Security Hub 관리자로 사용할 수 있지만 두 개의 다른 계정을 선택하는 것이 좋습니다. 이를 권장하는 이유는 청구 내용을 관리하기 위해 조직 관리 계정에 액세스할 수 있는 사용자는 보안 관리를 위해 Security Hub에 액세스해야 하는 사용자와 다를 수 있기 때문입니다.

여러 리전에서 동일한 위임된 관리자를 사용하는 것이 좋습니다. 중앙 구성을 선택하는 경우 Security Hub는 홈 리전 및 연결된 모든 리전에서 동일한 위임된 관리자를 자동으로 지정합니다.

위임된 관리자를 구성할 수 있는 권한을 확인하십시오.

위임된 Security Hub 관리자 계정을 지정하고 제거하려면 조직 관리 계정에 Security Hub에서의 `DisableOrganizationAdminAccount` 작업 `EnableOrganizationAdminAccount` 및 작업에 대한 권한이 있어야 합니다. Organizations 관리 계정은 Organizations에 대한 관리자 권한도 가지고 있어야 합니다.

필요한 모든 권한을 부여하려면 다음 Security Hub 관리형 정책을 조직 관리 계정의 IAM 보안 주체에 연결하십시오.

- AWSSecurityHubFullAccess

- AWSSecurityHubOrganizationsAccess

위임된 관리자 지정

위임된 Security Hub 관리자 계정을 지정하려면 Security Hub 콘솔, Security Hub API 또는 을 사용할 수 있습니다. AWS CLI Security Hub는 위임된 관리자를 현재 AWS 리전 관리자로만 설정하므로 다른 지역에서도 이 작업을 반복해야 합니다. 중앙 구성을 사용하기 시작하면 Security Hub는 홈 리전 및 연결된 리전에 동일한 위임된 관리자를 자동으로 설정합니다.

조직 관리 계정에서 Security Hub를 활성화하지 않아도 위임된 Security Hub 관리자 계정을 지정할 수 있습니다.

조직 관리 계정은 위임된 Security Hub 관리자 계정이 아닌 것이 좋습니다. 하지만 조직 관리 계정을 Security Hub 위임 관리자로 선택하는 경우 관리 계정에 Security Hub가 활성화되어 있어야 합니다. 관리 계정에 Security Hub가 활성화되어 있지 않은 경우 Security Hub를 수동으로 활성화해야 합니다. Security Hub는 조직 관리 계정에 자동으로 사용하도록 설정할 수 없습니다.

> **Note**
>
> 다음 방법 중 하나를 사용하여 위임된 Security Hub 관리자를 지정해야 합니다. Organizations API를 사용하여 위임된 Security Hub 관리자를 지정하는 것은 Security Hub에 반영되지 않습니다.
> 원하는 방법을 선택하고 단계에 따라 위임된 Security Hub 관리자 계정을 지정합니다.

Security Hub console

온보딩 중에 위임된 Security Hub 관리자를 지정하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. Security Hub로 이동하기를 선택합니다. 조직 관리 계정에 로그인하라는 메시지가 표시됩니다.
3. 위임된 관리자 지정 페이지의 위임된 관리자 계정 섹션에서 위임된 관리자 계정을 지정합니다. 다른 AWS 보안 및 규정 준수 서비스에 설정한 것과 동일한 위임된 관리자를 선택하는 것이 좋습니다.
4. 위임된 관리자 설정을 선택합니다. 중앙 구성으로 온보딩을 계속하려면 위임된 관리자 계정(아직 로그인하지 않은 경우)에 로그인하라는 메시지가 표시됩니다. 중앙 구성을 시작하지 않으려는 경우 취소를 선택하세요. 위임된 관리자가 설정되었지만 아직 중앙 구성을 사용하고 있지 않습니다.

설정 페이지에서 위임된 Security Hub 관리자를 지정하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. Security Hub 탐색 창에서 설정을 선택합니다. 그리고 일반을 선택합니다.
3. Security Hub 관리자 계정이 현재 할당되어 있는 경우 새 계정을 지정하려면 먼저 현재 계정을 제거해야 합니다.

   현재 계정을 제거하려면 위임된 관리자에서 제거를 선택합니다.
4. Security Hub 관리자 계정으로 지정할 계정의 계정 ID를 입력합니다.

   모든 리전에 동일한 Security Hub 관리자 계정을 지정해야 합니다. 다른 리전에서 지정된 계정과 다른 계정을 지정하는 경우 콘솔이 오류를 반환합니다.
5. 위임을 선택합니다.

Security Hub API, AWS CLI

조직 관리 계정에서 Security Hub API의 EnableOrganizationAdminAccount작업을 사용하십시오. 를 사용하는 경우 enable-organization-admin-account명령을 실행하십시오. AWS CLI위임된 Security Hub 관리자의 AWS 계정 ID를 입력합니다.

다음 예에서는 위임된 Security Hub 관리자를 지정합니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

위임된 관리자 제거 또는 변경

> **Warning**
>
> 중앙 구성을 사용하는 경우 Security Hub 콘솔 또는 Security Hub API를 사용하여 위임된 관리자 계정을 변경하거나 제거할 수 없습니다. 조직 관리 계정이 AWS Organizations 콘솔 또는 AWS Organizations API를 사용하여 위임된 Security Hub 관리자를 변경하거나 제거하는 경우 Security Hub는 자동으로 중앙 구성을 중지하고 구성 정책 및 정책 연결을 삭제합니다. 구성원 계정은 위임된 관리자가 변경되거나 제거되기 전의 구성을 유지합니다.

조직 관리 계정만 위임된 Security Hub 관리자 계정을 제거할 수 있습니다.

위임된 Security Hub 관리자를 변경하려면 먼저 현재 위임된 관리자 계정을 제거한 다음 새 계정을 지정해야 합니다.

Security Hub 콘솔을 사용하여 한 리전에서 위임된 관리자를 제거하면 모든 리전에서 자동으로 제거됩니다.

Security Hub API는 API 호출 또는 명령이 실행된 지역에서 위임된 Security Hub 관리자 계정만 제거합니다. 다른 리전에서도 이 작업을 반복해야 합니다.

Organizations API를 사용하여 위임된 Security Hub 관리자 계정을 제거하는 경우 모든 지역에서 자동으로 제거됩니다.

위임된 관리자 제거 (조직 API, AWS CLI)

Organizations를 사용하여 모든 지역에서 위임된 Security Hub 관리자를 제거할 수 있습니다.

중앙 구성을 사용하여 계정을 관리하는 경우 위임된 관리자 계정을 제거하면 구성 정책과 정책 연결이 삭제됩니다. 구성원 계정은 위임된 관리자가 변경되거나 제거되기 전의 구성을 유지합니다. 하지만 제거된 위임된 관리자 계정으로는 더 이상 이러한 계정을 관리할 수 없습니다. 이러한 계정은 각 리전에서 별도로 구성해야 하는 자체 관리형 계정이 됩니다.

원하는 방법을 선택하고 지침에 따라 위임된 Security Hub 관리자 계정을 제거합니다. AWS Organizations

Organizations API, AWS CLI

위임된 Security Hub 관리자를 제거하려면

조직 관리 계정에서 Organizations API의 DeregisterDelegatedAdministrator작업을 사용하십시오. 를 사용하는 경우 deregister-delegated-administrator명령을 실행하세요. AWS CLI위임된 관리자의 계정 ID와 Security Hub의 서비스 주체 () 를 입력합니다. `securityhub.amazonaws.com`

다음 예에서는 위임된 Security Hub 관리자를 제거합니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

위임된 관리자 제거 (Security Hub 콘솔)

Security Hub 콘솔을 사용하여 모든 지역에서 위임된 Security Hub 관리자를 제거할 수 있습니다.

위임된 Security Hub 관리자 계정이 제거되면 구성원 계정과 제거된 위임된 Security Hub 관리자 계정의 연결이 끊어집니다.

구성원 계정에는 여전히 Security Hub가 활성화되어 있습니다. 새 Security Hub 관리자가 구성원 계정으로 활성화하기 전까지는 독립형 계정이 됩니다.

조직 관리 계정이 Security Hub에서 사용하도록 설정된 계정이 아닌 경우 Security Hub 시작 페이지의 옵션을 사용하십시오.

Security Hub 시작 페이지에서 위임된 Security Hub 관리자 계정을 제거하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. Security Hub로 이동하기를 선택합니다.
3. 위임된 관리자에서 제거를 선택합니다.

조직 관리 계정이 Security Hub에서 사용하도록 설정된 계정인 경우 설정 페이지의 일반 탭에 있는 옵션을 사용하십시오.

설정 페이지에서 위임된 Security Hub 관리자 계정을 제거하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. Security Hub 탐색 창에서 설정을 선택합니다. 그리고 일반을 선택합니다.
3. 위임된 관리자에서 제거를 선택합니다.

위임된 관리자 제거 (Security Hub API, AWS CLI)

Security Hub API 또는 Security Hub 작업을 사용하여 위임된 보안 허브 관리자를 제거할 수 있습니다. AWS CLI 이러한 방법 중 하나를 사용하여 위임된 관리자를 제거하면 API 호출 또는 명령이 실행된 리전에서만 제거됩니다. Security Hub는 다른 지역을 업데이트하지 않으며, 에서 AWS Organizations위임된 관리자 계정을 제거하지도 않습니다.

원하는 방법을 선택하고 다음 단계에 따라 Security Hub에서 위임된 Security Hub 관리자 계정을 제거하십시오.

Security Hub API, AWS CLI

위임된 Security Hub 관리자를 제거하려면

조직 관리 계정에서 Security Hub API의 DisableOrganizationAdminAccount작업을 사용하십시오. 를 사용하는 경우 disable-organization-admin-account명령을 실행하십시오. AWS CLI위임된 Security Hub 관리자의 계정 ID를 입력합니다.

다음 예에서는 위임된 Security Hub 관리자를 제거합니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Security Hub 통합 비활성화 AWS Organizations

AWS Organizations 조직이 통합된 후에는 AWS Security Hub Organizations 관리 계정을 사용하여 통합을 비활성화할 수 있습니다. Organizations 관리 계정의 사용자는 AWS Organizations에서 Security Hub에 대한 신뢰할 수 있는 액세스를 비활성화하여 이를 수행할 수 있습니다.

Security Hub에 대한 신뢰할 수 있는 액세스를 비활성화하면 다음과 같은 상황이 발생합니다.

- Security Hub는 에서 신뢰할 수 있는 서비스로서의 지위를 AWS Organizations상실합니다.
- Security Hub 위임된 관리자 계정은 모든 AWS 리전의 모든 Security Hub 구성원 계정의 Security Hub 설정, 데이터 및 리소스에 대한 액세스 권한을 상실합니다.
- 중앙 구성을 사용하고 있었다면 Security Hub는 조직에서 중앙 구성 사용을 자동으로 중지합니다. 구성 정책 및 정책 연결이 삭제됩니다. 계정은 신뢰할 수 있는 액세스를 비활성화하기 전에 사용했던 구성을 유지합니다.
- 모든 Security Hub 구성원 계정은 독립형 계정이 되며 현재 설정을 유지합니다. Security Hub가 하나 이상의 리전에서 구성원 계정에 대해 활성화된 경우, Security Hub는 해당 리전에서 해당 계정을 계속 사용할 수 있습니다. 활성화된 표준 및 제어 역시 변경되지 않습니다. 이러한 설정은 각 계정 및 리전에서 개별적으로 변경할 수 있습니다. 하지만 계정은 더 이상 어떤 리전의 위임된 관리자와도 연결되지 않습니다.

신뢰할 수 있는 서비스 액세스를 비활성화한 결과에 대한 자세한 내용은 사용 설명서의AWS Organizations 다른 AWS OrganizationsAWS 서비스사람과 함께 사용을 참조하십시오.

신뢰할 수 있는 액세스를 비활성화하려면 AWS Organizations 콘솔, Organizations API 또는 를 사용할 수 AWS CLI있습니다. Organizations 관리 계정의 사용자만 Security Hub에 대한 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다. 필요한 권한에 대한 자세한 내용은 AWS Organizations 사용 설명서의 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한을 참조하세요.

신뢰할 수 있는 액세스를 비활성화하기 전에 조직의 위임된 관리자와 협력하여 구성원 계정에서 Security Hub를 비활성화하고 해당 계정에서 Security Hub 리소스를 정리하는 것이 좋습니다.

원하는 방법을 선택하고 단계에 따라 Security Hub에 대한 신뢰할 수 있는 액세스를 비활성화하세요.

Organizations console

Security Hub에 대한 신뢰할 수 있는 액세스를 비활성화하려면

1. AWS Organizations 관리 계정의 자격 증명을 AWS Management Console 사용하여 에 로그인합니다.
2. https://console.aws.amazon.com/organizations/에서 Organizations 콘솔을 엽니다.
3. 탐색 창에서 서비스를 선택합니다.
4. 통합 서비스에서 AWS Security Hub를 선택합니다.
5. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 신뢰할 수 있는 액세스를 비활성화할지 확인합니다.

Organizations API

Security Hub에 대한 신뢰할 수 있는 액세스를 비활성화하려면

AWS Organizations API의 비활성화 AWSServiceAccess 작업을 호출합니다. `ServicePrincipal` 파라미터에서 Security Hub 서비스 주체(`securityhub.amazonaws.com`)를 지정합니다.

AWS CLI

Security Hub에 대한 신뢰할 수 있는 액세스를 비활성화하려면

AWS Organizations API의 disable-aws-service-access명령을 실행합니다. `service-principal` 파라미터에서 Security Hub 서비스 주체(`securityhub.amazonaws.com`)를 지정합니다.

예:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

새 조직 계정에서 Security Hub 자동 활성화

새 계정이 조직에 가입하면 AWS Security Hub 콘솔의 계정 페이지에 있는 목록에 해당 계정이 추가됩니다. 조직 계정의 경우 유형은 조직별입니다. 기본적으로 새 계정은 조직에 가입할 때 Security Hub 구성원이 되지 않습니다. 해당 구성원의 상태는 구성원이 아님입니다. 위임된 관리자 계정은 새 계정을 구성원으로 자동으로 추가하고 해당 계정이 기관에 가입할 때 Security Hub를 활성화할 수 있습니다.

> **Note**
>
> 많은 지역이 기본적으로 AWS 리전 활성화되어 있지만 특정 지역은 수동으로 활성화해야 합니다. AWS 계정이 문서에서는 이러한 지역을 옵트인 지역이라고 합니다. 옵트인 지역의 새 계정에서 Security Hub를 자동으로 활성화하려면 먼저 해당 지역을 활성화해야 합니다. 계정 소유자만 옵트인 지역을 활성화할 수 있습니다. 옵트인 지역에 대한 자세한 내용은 AWS 리전 계정에서 사용할 수 있는 지역 지정을 참조하십시오.

이 프로세스는 중앙 구성(권장)을 사용하는지 로컬 구성을 사용하는지에 따라 달라집니다.

새 조직 계정 자동 활성화(중앙 구성)

중앙 구성을 사용하는 경우 Security Hub를 사용하도록 설정하는 구성 정책을 만들어 새 조직 계정과 기존 조직 계정에서 Security Hub를 자동으로 사용하도록 설정할 수 있습니다. 그런 다음 정책을 조직 루트 또는 특정 조직 단위 (OU) 에 연결할 수 있습니다.

Security Hub가 활성화된 구성 정책을 특정 OU와 연결하면 해당 OU에 속하는 모든 계정(기존 및 신규)에서 Security Hub가 자동으로 활성화됩니다. OU에 속하지 않는 새 계정은 자체 관리하며 Security Hub를 자동으로 활성화하지 않습니다. Security Hub가 활성화된 구성 정책을 루트와 연결하면 조직에 가입한 모든 계정(기존 및 신규)에서 Security Hub가 자동으로 활성화됩니다. 단, 계정이 적용 또는 상속을 통해 다른 정책을 사용하거나 자체 관리하는 경우는 예외입니다.

구성 정책에서는 OU에서 활성화해야 하는 보안 표준 및 제어를 정의할 수도 있습니다. 활성화된 표준에 대한 제어 결과를 생성하려면 OU의 계정이 필수 리소스를 기록하도록 AWS Config 활성화하고 구성해야 합니다. AWS Config 기록에 대한 자세한 내용은 활성화 및 구성을 참조하십시오 AWS Config.

구성 정책 생성에 대한 지침은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요.

새 조직 계정 자동 활성화(로컬 구성)

로컬 구성을 사용하고 자동 활성화를 켜면 Security Hub는 새 조직 계정을 구성원로 추가하고 현재 리전의 Security Hub를 활성화합니다. 다른 리전은 영향을 받지 않습니다. 또한 자동 활성화 기능을 켜도

이미 구성원 계정으로 추가된 경우를 제외하고 기존 조직 계정에서 Security Hub가 활성화되지 않습니다.

자동 활성화 기능을 켜면 현재 리전의 새 계정이 조직에 가입할 때 기본 보안 표준도 자동으로 활성화됩니다. 기본 표준은 기본 보안 모범 사례 (FSBP) 및 인터넷 보안 센터 (CIS) AWS 재단 벤치마크 v1.2.0입니다. AWS 기본 표준은 변경할 수 없습니다. 조직 전체에서 다른 표준을 사용하거나 일부 계정 및 OU에 표준을 적용하려면 중앙 구성을 사용하는 것이 좋습니다.

기본 표준 (및 기타 사용 표준) 에 대한 제어 결과를 생성하려면 조직의 계정이 필수 리소스를 기록하도록 활성화하고 구성해야 합니다. AWS Config AWS Config 기록에 대한 자세한 내용은 활성화 및 구성을 참조하십시오 AWS Config.

원하는 방법을 선택하고 단계에 따라 새 조직 계정에서 Security Hub를 자동으로 활성화하세요. 이 지침은 로컬 구성을 사용하는 경우에만 적용됩니다.

Security Hub console

새 조직 계정을 구성원 계정으로 자동으로 활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. Security Hub 탐색 창의 설정에서 구성를 선택합니다.
3. 계정 섹션에서 계정 자동 활성화를 켭니다.

Security Hub API

새 조직 계정을 구성원 계정으로 자동으로 활성화하려면

위임된 관리자 계정에서 `UpdateOrganizationConfiguration` API를 호출합니다. 새 조직 계정에서 Security Hub를 자동으로 활성화하려면 `AutoEnable` 필드를 `true`로 설정합니다.

AWS CLI

새 조직 계정을 구성원 계정으로 자동으로 활성화하려면

위임된 관리자 계정에서 `update-organization-configuration` 명령을 실행합니다. 새 조직 계정에서 Security Hub를 자동으로 활성화하는 `auto-enable` 파라미터를 포함합니다.

```
aws securityhub update-organization-configuration --auto-enable
```

새 조직 계정에서 Security Hub를 수동으로 활성화하기

새 조직 계정이 조직에 가입할 때 자동으로 Security Hub를 사용하도록 설정하지 않으면 해당 계정을 구성원으로 추가하고 조직에 가입한 후 해당 계정에서 Security Hub를 수동으로 활성화할 수 있습니다. 또한 이전에 조직과의 연결을 끊은 Security Hub를 수동으로 활성화해야 합니다. AWS 계정

> **Note**
>
> 중앙 구성을 사용하는 경우에는 이 섹션이 적용되지 않습니다. 중앙 구성을 사용하는 경우 지정된 구성원 계정 및 OU(조직 단위)에서 Security Hub를 활성화하는 구성 정책을 만들 수 있습니다. 또한 해당 계정과 OU에서 특정 표준 및 제어를 활성화할 수 있습니다.

이미 다른 조직의 구성원 계정인 경우 해당 계정에서 Security Hub를 활성화할 수 없습니다.

또한 현재 일시 중지된 계정에서는 Security Hub를 활성화할 수 없습니다. 일시 중지된 계정의 서비스를 활성화하려고 하면 계정 상태가 계정 일시 중단됨로 변경됩니다.

- 계정에 Security Hub가 활성화되지 않은 경우 해당 계정에서 Security Hub가 활성화됩니다. AWS 기본 보안 표준을 해제하지 않는 한 기본 보안 모범 사례 (FSBP) 표준 및 CIS AWS 재단 벤치마크 v1.2.0도 계정에서 활성화됩니다.

  이에 대한 예외는 Organizations 관리 계정입니다. Organizations 관리 계정에서는 Security Hub를 자동으로 활성화할 수 없습니다. Organizations 관리 계정을 구성원 계정으로 활성화하려면 먼저 Organizations 관리 계정에서 수동으로 Security Hub를 활성화해야 합니다.
- 계정에 이미 Security Hub가 활성화되어 있는 경우 Security Hub는 계정에 다른 변경 사항을 적용하지 않습니다. 멤버십만 활성화합니다.

Security Hub에서 제어 결과를 생성하려면 구성원 계정이 필수 리소스를 기록하도록 AWS Config 활성화하고 구성해야 합니다. 자세한 내용은 AWS Config설정 및 구성을 참조하세요.

원하는 방법을 선택하고 단계에 따라 조직 계정을 Security Hub 구성원 계정으로 활성화하세요.

Security Hub console

조직 계정을 Security Hub 구성원로 수동으로 활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.

2. Security Hub 탐색 창의 설정에서 구성를 선택합니다.
3. 계정 목록에서 활성화할 각 조직 계정을 선택합니다.
4. 작업을 선택하고 구성원 추가를 선택합니다.

Security Hub API

조직 계정을 Security Hub 구성원로 수동으로 활성화하려면

위임된 관리자 계정에서 `CreateMembers` API를 호출합니다. 활성화할 각 계정의 계정 ID를 입력합니다.

수동 초대 프로세스와 달리 조직 계정을 활성화하는 데 `CreateMembers`을 호출하는 경우 초대를 보낼 필요가 없습니다.

AWS CLI

조직 계정을 Security Hub 구성원로 수동으로 활성화하려면

위임된 관리자 계정에서 `create-members` 명령을 실행합니다. 활성화할 각 계정의 계정 ID를 입력합니다.

수동 초대 프로세스와 달리 조직 계정을 활성화하는 데 `create-members`을 실행하는 경우 초대를 보낼 필요가 없습니다.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

예

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

조직에서 구성원 계정 연결 해제

AWS Security Hub 구성원 계정으로부터 결과를 받거나 보는 것을 중단하려면 조직에서 구성원 계정을 분리하면 됩니다.

> **Note**
>
> 중앙 구성을 사용하는 경우 연결 해제가 다르게 작동합니다. 중앙에서 관리되는 하나 이상의 구성원 계정에서 Security Hub를 비활성화하는 구성 정책을 만들 수 있습니다. 그 이후에도 이

러한 계정은 여전히 조직의 일부이지만 Security Hub 결과를 생성하지는 않습니다. 중앙 구성을 사용하지만 수동으로 초대된 구성원 계정이 있는 경우 수동으로 초대된 계정을 하나 이상 연결 해제할 수 있습니다.

를 사용하여 관리하는 구성원 계정은 관리자 계정과의 계정 연결을 AWS Organizations 해제할 수 없습니다. 관리자 계정만 구성원 계정 연결을 해제할 수 있습니다.

구성원 계정을 연결 해제해도 계정은 해지되지 않습니다. 대신 조직에서 구성원 계정을 제거합니다. 연결이 끊긴 구성원 계정은 Security Hub 통합을 통해 더 이상 관리되지 AWS 계정 않는 독립형 계정이 됩니다. AWS Organizations

원하는 방법을 선택하고 단계에 따라 조직에서 구성원 계정을 연결 해제하세요.

Security Hub console

조직에서 구성원 계정을 연결 해제하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창의 설정에서 구성을 선택합니다.
3. 계정 섹션에서 연결을 해제하려는 계정을 선택합니다. 중앙 구성을 사용하는 경우 수동으로 초대된 계정을 선택하여 `Invitation accounts` 탭에서 연결을 해제할 수 있습니다. 이 탭은 중앙 구성을 사용하는 경우에만 표시됩니다.
4. 작업을 선택한 다음 계정 연결 해제를 선택합니다.

Security Hub API

조직에서 구성원 계정을 연결 해제하려면

위임된 관리자 계정에서 `DisassociateMembers` API를 호출합니다. 연결을 해제하려면 회원 계정의 AWS 계정 ID를 제공해야 합니다. 구성원 계정 목록을 보려면 `ListMembers` API를 호출합니다.

AWS CLI

조직에서 구성원 계정을 연결 해제하려면

위임된 관리자 계정에서 `>disassociate-members` 명령을 실행합니다. 연결을 끊을 회원 계정의 AWS 계정 ID를 제공해야 합니다. 구성원 계정 목록을 보려면 `>list-members` 명령을 실행합니다.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

예

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

AWS Organizations 콘솔 또는 AWS SDK를 사용하여 조직에서 멤버 계정을 분리할 수도 있습니다. AWS CLI자세한 내용은 AWS Organizations 사용 설명서의 조직에서 구성원 계정 제거를 참조하세요.

초대를 통한 계정 관리

Security Hub를 AWS Organizations 통합하거나 멤버십 초대를 수동으로 보내고 수락하는 두 가지 방법으로 여러 AWS Security Hub 계정을 중앙에서 관리할 수 있습니다. 독립형 계정이 있는 경우 또는 Organizations와 통합하지 않는 경우 수동 프로세스를 사용해야 합니다. 수동 계정 관리에서는 Security Hub 관리자가 계정을 구성원으로 초대합니다. 예비 구성원이 초대를 수락하면 관리자-구성원 관계가 성립됩니다. Security Hub 관리자 계정은 최대 1,000개의 초대 기반 구성원 계정에 대한 Security Hub를 관리할 수 있습니다.

> **Tip**
>
> Security Hub에서 초대 기반 조직을 만든 경우, 나중에 AWS Organizations을 대신 사용하도록 전환할 수 있습니다. 멤버 계정이 두 개 이상인 경우 를 통해 계정을 관리하는 것이 좋습니다. AWS Organizations

수동 초대 프로세스를 통해 초대하는 계정에 대해 결과와 기타 데이터에 대한 크로스 리전 집계를 사용할 수 있습니다. 하지만 교차 지역 집계가 제대로 작동하려면 관리자가 집계 지역 및 모든 연결 지역에서 회원 계정을 초대해야 합니다. 또한 관리자가 구성원 계정의 조사 결과를 볼 수 있도록 하려면 구성원 계정의 집계 지역 및 모든 연결 지역에서 Security Hub를 활성화해야 합니다.

수동으로 초대된 멤버 계정에는 구성 정책이 지원되지 않습니다. 대신 각 구성원 계정에서 그리고 수동 초대 프로세스를 사용할 AWS 리전 때 Security Hub 설정을 개별적으로 구성해야 합니다.

또한 조직에 속하지 않은 계정에 대해서는 수동 초대 기반 프로세스를 사용해야 합니다. 예를 들어, 조직에 테스트 계정을 포함하지 않을 수도 있습니다. 또는 여러 조직의 계정을 하나의 Security Hub 관리자 계정으로 통합할 수도 있습니다. Security Hub 관리자 계정은 다른 조직에 속한 계정으로 초대를 보내야 합니다.

Security Hub 콘솔의 구성 페이지에서 초대를 통해 추가된 계정이 초대 계정 탭에 나열됩니다. 중앙 구성 작동 방식을 사용하지만 조직 외부 계정을 초대하는 경우 이 탭에서 초대 기반 계정의 결과를 볼 수 있습니다. 하지만 Security Hub 관리자는 구성 정책을 사용하여 여러 리전의 초대 기반 계정을 구성할 수 없습니다.

이 섹션의 주제에서는 초대를 통해 구성원 계정을 관리하는 방법을 설명합니다.

주제

구성원 계정 추가 및 초대

사용자 계정은 초대를 수락하는 계정의 AWS Security Hub 관리자가 됩니다.

다른 계정으로부터 온 초대를 수락하면 사용자 계정이 구성원 계정이 되고 해당 계정이 귀하의 관리자가 됩니다.

사용자 계정이 관리자 계정인 경우, 구성원 계정이 되기 위한 초대를 수락할 수 없습니다.

구성원 계정 추가는 다음과 같은 단계로 구성됩니다.

1. 관리자 계정이 멤버 계정 목록에 멤버 계정을 추가합니다.
2. 관리자 계정이 멤버 계정에 초대를 보냅니다.
3. 구성원 계정이 초대를 수락합니다.

구성원 계정 추가

Security Hub 콘솔에서 구성원 계정 목록에 계정을 추가할 수 있습니다. Security Hub 콘솔에서 계정을 개별적으로 선택하거나 계정 정보가 포함된 .csv 파일을 업로드할 수 있습니다.

계정마다 계정 ID와 이메일 주소를 제공해야 합니다. 이메일 주소는 계정의 보안 문제에 대해 문의할 수 있는 이메일 주소여야 합니다. 이 이메일 주소는 계정 인증에 사용되지 않습니다.

원하는 방법을 선택하고 단계에 따라 구성원 계정을 추가하세요.

Security Hub console

구성원 계정 목록에 계정을 추가하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   관리자 계정의 보안 인증을 사용하여 로그인합니다.
2. 왼쪽 창에서 설정을 선택합니다.
3. 설정 페이지에서 계정을 선택하고 계정 추가를 선택합니다. 그런 다음에는 계정을 개별적으로 추가하거나 계정 목록이 포함된 .csv 파일을 업로드할 수 있습니다.
4. 이 계정을 선택하려면 다음 중 하나를 수행하십시오.

   - 개별로 계정을 추가하려면 계정 입력에서 추가할 계정의 계정 ID 및 이메일 주소를 입력하고 추가를 선택합니다.

     각 계정마다 이 절차를 반복합니다.
   - 쉼표로 구분된 값(.csv) 파일을 사용하여 복수 계정을 추가하려면 먼저 파일을 생성해야 합니다. 파일에는 추가할 각 계정의 계정 ID와 이메일 주소가 포함되어야 합니다.

     .csv 목록에는 계정이 한 줄에 하나씩 표시되어야 합니다. .csv 파일의 첫 번째 줄에는 헤더가 포함되어야 합니다. 헤더에서 첫 번째 열은 **Account ID**이고, 두 번째 열은 **Email**입니다.

     이어지는 각 줄에는 추가하려는 계정에 대한 계정 ID 및 유효한 이메일 주소가 포함되어야 합니다.

     다음은 텍스트 편집기에서 보는 .csv 파일의 예입니다.

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

스프레드시트 프로그램에서는 필드가 별도의 열에 표시됩니다. 기본 형식은 여전히 쉼표로 구분됩니다. 계정 ID의 형식은 소수점이 없는 숫자로 지정해야 합니다. 예를 들어, 계정 ID 444455556666은 444455556666.0으로 형식을 지정할 수 없습니다. 또한, 숫자 형식으로 인해 계정 ID에서 앞에 오는 0이 제거되지 않도록 해야 합니다.

파일을 선택하려면 콘솔에서 목록 업로드(.csv)를 선택합니다. 그런 다음 찾아보기를 선택합니다.

파일을 선택한 후 계정 추가를 선택합니다.

5. 계정 추가를 완료한 후 추가할 계정에서 다음을 선택합니다.

Security Hub API

구성원 계정 목록에 계정을 추가하려면

관리자 계정에서 `CreateMembers` API를 호출합니다. 추가할 각 멤버 계정에 대해 AWS 계정 ID를 제공해야 합니다.

AWS CLI

구성원 계정 목록에 계정을 추가하려면

관리자 계정에서 `create-members` 명령을 실행합니다. 추가할 각 회원 계정에 대해 AWS 계정 ID를 제공해야 합니다.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

예

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

구성원 계정 초대

구성원 계정을 추가한 후 구성원 계정에 초대를 전송합니다. 관리자와의 연결이 해제된 계정에 초대를 다시 보낼 수도 있습니다.

Security Hub console

예비 구성원 계정을 초대하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   관리자 계정의 보안 인증을 사용하여 로그인합니다.
2. 탐색 창에서 Settings(설정)를 선택한 다음 Accounts(계정)를 선택합니다.
3. 초대한 계정의 상태 열 값에서 초대를 선택합니다.
4. 확인하라는 메시지가 나타나면 초대를 선택합니다.

> **Note**
>
> 연결이 해제된 계정에 초대를 다시 보내려면 계정 페이지에서 연결이 해제된 각 계정을 선택합니다. 작업에서 초대 재전송을 선택합니다.

Security Hub API

예비 구성원 계정을 초대하려면

관리자 계정에서 `InviteMembers` API를 호출합니다. 초대할 각 계정의 AWS 계정 ID를 제공해야 합니다.

AWS CLI

예비 구성원 계정을 초대하려면

관리자 계정에서 `invite-members` 명령을 실행합니다. 초대할 각 계정의 AWS 계정 ID를 제공해야 합니다.

```
aws securityhub invite-members --account-ids <accountIDs>
```

예

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

멤버 계정 가입 초대에 응답

에서 구성원 계정으로 가입하라는 초대를 수락하거나 거절할 수 있습니다.

초대를 수락하면 계정이 AWS Security Hub 회원 계정이 됩니다. 초대를 보낸 계정이 Security Hub 관리자 계정이 됩니다. 관리자 계정 사용자는 Security Hub에서 멤버 계정에 대한 조사 결과를 볼 수 있습니다.

초대를 거부하면 관리자 계정의 구성원 계정 목록에 계정이 탈퇴로 표시됩니다.

멤버 계정으로 가입하라는 초대를 수락하거나 거절할 수만 있습니다.

초대를 수락하거나 거절하려면 Security Hub를 활성화해야 합니다.

모든 Security Hub 계정이 모든 리소스를 기록하도록 AWS Config 활성화하고 구성해야 한다는 점을 기억하십시오. 요구 사항에 대한 AWS Config자세한 내용은 활성화 및 구성을 참조하십시오 AWS Config.

초대 수락

원하는 방법을 선택하고 단계에 따라 구성원 계정 초대를 수락하세요.

Security Hub console

멤버십 초대를 수락하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 계정을 선택합니다.
3. 관리자 계정에서 수락을 켠 다음 초대 수락을 선택합니다.

Security Hub API

멤버십 초대를 수락하려면

`AcceptAdministratorInvitation` API를 호출합니다. 초대 식별자와 관리자 계정의 AWS 계정 ID를 제공해야 합니다. 초대에 대한 세부 정보를 검색하려면 `ListInvitations` 작업을 사용하세요.

AWS CLI

멤버십 초대를 수락하려면

accept-administrator-invitation 명령을 실행합니다. 초대 식별자와 관리자 계정의 AWS 계정 ID를 제공해야 합니다. 초대에 대한 세부 정보를 검색하려면 list-invitations 명령을 실행합니다.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

예

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> Security Hub 콘솔이 AcceptInvitation을 계속 사용합니다. 결국에는 AcceptAdministratorInvitation을 사용하도록 변경됩니다. 이 기능에 대한 액세스를 구체적으로 제어하는 모든 IAM 정책은 계속 AcceptInvitation을 사용해야 합니다. 또한, 콘솔이 AcceptAdministratorInvitation을 사용하기 시작하면 올바른 권한이 적용되도록 AcceptAdministratorInvitation을 정책에 추가해야 합니다.

초대 거부

구성원 계정으로 가입하라는 초대를 수락하거나 거절할 수 있습니다. Security Hub 콘솔에서 초대를 거부하면 관리자 계정의 구성원 계정 목록에 계정이 탈퇴로 표시됩니다.

초대를 거부할 때는 초대를 받은 구성원 계정으로 로그인해야 합니다.

원하는 방법을 선택하고 단계에 따라 구성원 계정 초대를 거부하세요.

Security Hub console

멤버십 초대를 거부하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 계정을 선택합니다.
3. 관리자 계정 섹션에서 초대 거부를 선택합니다.

Security Hub API

멤버십 초대를 거부하려면

DeclineInvitations API를 호출합니다. 초대를 발행한 관리자 계정의 AWS 계정 ID를 제공해야 합니다. 초대에 대한 정보를 보려면 ListInvitations 작업을 사용하세요.

AWS CLI

멤버십 초대를 거부하려면

decline-invitations 명령을 실행합니다. 초대를 발행한 관리자 계정의 AWS 계정 ID를 제공해야 합니다. 초대에 대한 정보를 보려면 list-invitations 명령을 실행합니다.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

예

```
aws securityhub decline-invitations --account-ids "123456789012"
```

멤버 계정 연결 해제

AWS Security Hub 관리자 계정은 구성원 계정을 연결 해제하여 해당 계정의 결과를 수신하고 보는 것을 중단할 수 있습니다. 구성원 계정을 삭제하기 전에는 구성원 계정 연결을 해제해야 합니다.

멤버 계정을 연결 해제해도 멤버 계정 목록에는 해당 계정이 제거됨(연결 해제됨) 상태인 상태로 남아 있습니다. 멤버 계정의 관리자 계정 정보에서 계정이 제거됩니다.

계정에 대한 조사 결과를 다시 받으려면 초대를 다시 보내면 됩니다. 구성원 계정을 완전히 삭제하려면 구성원 계정을 삭제하면 됩니다.

원하는 방법을 선택하고 단계에 따라 관리자 계정에서 수동으로 초대된 구성원 계정을 연결 해제하세요.

Security Hub console

수동으로 초대된 구성원 계정을 연결 해제하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   관리자 계정의 보안 인증을 사용하여 로그인합니다.

2. 탐색 창의 설정에서 구성을 선택합니다.
3. 계정 섹션에서 연결을 해제하려는 계정을 선택합니다.
4. 작업을 선택한 다음 계정 연결 해제를 선택합니다.

Security Hub API

수동으로 초대된 구성원 계정을 연결 해제하려면

관리자 계정에서 `DisassociateMembers` API를 호출합니다. 연결을 해제하려는 회원 계정의 AWS 계정 ID를 제공해야 합니다. 구성원 계정 목록을 보려면 `ListMembers` 작업을 사용하세요.

AWS CLI

수동으로 초대된 구성원 계정을 연결 해제하려면

관리자 계정에서 `disassociate-members` 명령을 실행합니다. 연결을 끊으려는 회원 계정의 AWS 계정 ID를 제공해야 합니다. 구성원 계정 목록을 보려면 `list-members` 명령을 실행합니다.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

예

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

멤버 계정 삭제

AWS Security Hub 관리자 계정은 초대를 통해 추가된 구성원 계정을 삭제할 수 있습니다. 멤버 계정을 삭제하기 전에는 멤버 계정 연결을 해제해야 합니다.

구성원 계정을 삭제하면 목록에서 완전히 제거됩니다. 계정의 멤버십을 복원하려면 계정을 추가하고 완전히 새로운 구성원 계정인 것처럼 다시 초대해야 합니다.

조직에 속해 있고 와의 통합을 사용하여 관리되는 계정은 삭제할 수 없습니다 AWS Organizations.

원하는 방법을 선택하고 단계에 따라 수동으로 초대된 구성원 계정을 삭제하세요.

Security Hub console

수동으로 초대된 구성원 계정을 삭제하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

관리자 계정을 사용하여 로그인합니다.

2. 탐색 창에서 설정을 선택한 다음 구성을 선택합니다.
3. 초대 계정 탭을 선택합니다. 그런 다음 삭제할 계정을 선택합니다.
4. 작업을 선택한 후 삭제를 선택합니다. 이 옵션은 계정 연결을 해제한 경우에만 사용할 수 있습니다. 구성원 계정을 삭제하려면 먼저 구성원 계정 연결을 해제해야 합니다.

Security Hub API

수동으로 초대된 구성원 계정을 삭제하려면

관리자 계정에서 `DeleteMembers` API를 호출합니다. 삭제하려는 구성원 계정의 AWS 계정 ID를 제공해야 합니다. 구성원 계정 목록을 검색하려면 `ListMembers` API를 호출합니다.

AWS CLI

수동으로 초대된 구성원 계정을 삭제하려면

관리자 계정에서 `delete-members` 명령을 실행합니다. 삭제하려는 구성원 계정의 AWS 계정 ID를 제공해야 합니다. 구성원 계정 목록을 검색하려면 `list-members` 명령을 실행합니다.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

예

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

관리자 계정과의 연결 해제

초대를 통해 계정을 AWS Security Hub 회원 계정으로 추가한 경우 관리자 계정에서 회원 계정을 분리할 수 있습니다. 구성원 계정을 연결 해제하면, Security Hub는 계정의 조사 결과를 관리자 계정으로 보내지 않습니다.

통합을 사용하여 관리하는 구성원 계정은 관리자 계정과의 계정 연결을 AWS Organizations 해제할 수 없습니다. Security Hub 위임된 관리자만 Organizations로 관리하는 구성원 계정의 연결을 해제할 수 있습니다.

관리자 계정과의 연결을 끊어도 해당 계정은 관리자 계정의 구성원 목록에 탈퇴 상태로 남아 있습니다. 하지만, 관리자 계정은 사용자의 계정에 대한 조사 결과를 받을 수 없습니다.

관리자 계정과의 연결을 해제한 후에도 구성원로 가입하라는 초대는 아직 남아 있습니다. 나중에 다시 초대를 수락할 수 있습니다.

Security Hub console

관리자 계정과의 연결을 해제하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 계정을 선택합니다.
3. 관리자 계정 섹션에서 수락을 끄고 업데이트를 선택합니다.

Security Hub API

관리자 계정과의 연결을 해제하려면

`DisassociateFromAdministratorAccount` API를 호출합니다.

AWS CLI

관리자 계정과의 연결을 해제하려면

`disassociate-from-administrator-account` 명령을 실행합니다.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> Security Hub 콘솔이 `DisassociateFromMasterAccount`을 계속 사용합니다. 결국에는 `DisassociateFromAdministratorAccount`을 사용하도록 변경됩니다. 이 기능에 대한 액세스를 구체적으로 제어하는 모든 IAM 정책은 계속 `DisassociateFromMasterAccount`을 사용해야 합니다. 또한, 콘솔이 `DisassociateFromAdministratorAccount`을 사용하기 시작하면 올바른 권한이 적용되도록 `DisassociateFromAdministratorAccount`을 정책에 추가해야 합니다.

계정 관리를 위해 AWS Organizations으로 전환하기

AWS Security Hub에서 계정을 수동으로 관리하는 경우 예비 구성원 계정을 초대하고 각 AWS 리전에서 구성원 계정을 개별적으로 구성해야 합니다.

Security Hub 및 AWS Organizations를 통합하면 초대를 보낼 필요가 없으며 조직에서 Security Hub를 구성하고 사용자 지정되는 방식을 더 잘 제어할 수 있습니다.

AWS Organizations 통합을 사용하는 결합된 접근 방식을 사용할 수도 있지만 조직 외부의 계정을 수동으로 초대할 수도 있습니다. 하지만 Organizations 통합만 사용하는 것이 좋습니다. 여러 계정 및 리전에서 Security Hub를 관리하는 데 도움이 되는 기능인 중앙 구성은 Organizations와 통합할 때만 사용할 수 있습니다.

이 섹션에서는 AWS Organizations를 통해 수동 초대 기반 계정 관리에서 계정 관리로 전환하는 방법을 설명합니다.

Security Hub와 AWS Organizations의 통합

먼저 Security Hub 및 AWS Organizations를 통합해야 합니다.

다음 단계를 완료하면 이러한 서비스를 통합할 수 있습니다.

- AWS Organizations에서 조직을 생성합니다. 지침은 AWS Organizations 사용 설명서의 조직 생성을 참조하세요.
- Organizations 관리 계정에서 Security Hub 위임된 관리자 계정을 지정합니다.

> **Note**
>
> Organizations 관리 계정은 DA 계정으로 사용할 수 없습니다.

자세한 지침은 Security Hub와 통합 AWS Organizations 섹션을 참조하세요.

이전 단계를 완료하면 AWS Organizations의 Security Hub에 대한 신뢰할 수 있는 액세스 권한을 부여하게 됩니다. 또한 위임된 관리자 계정에 대해 현재 AWS 리전의 Security Hub를 활성화합니다.

위임된 관리자는 주로 조직의 계정을 Security Hub 구성원 계정으로 추가하여 Security Hub에서 조직을 관리할 수 있습니다. 관리자는 해당 계정에 대한 특정 Security Hub 설정, 데이터 및 리소스에 액세스할 수도 있습니다.

Organizations를 사용하여 계정 관리로 전환해도 초대 기반 계정이 자동으로 Security Hub 구성원이 되지는 않습니다. 새 조직에 추가하는 계정만 Security Hub 구성원이 될 수 있습니다.

중앙 구성과 로컬 구성 비교

통합을 활성화한 후에는 Organizations를 사용하여 계정을 관리할 수 있습니다. 자세한 내용은 를 통한 계정 관리 AWS Organizations 섹션을 참조하세요. 계정 관리는 조직의 구성 유형에 따라 달라집니다.

조직에 사용할 수 있는 구성 유형은 로컬과 중앙의 두 가지입니다. 기본 구성 유형은 로컬 구성입니다. 현재 구성 유형을 보려면 Security Hub 콘솔의 탐색 창에서 설정을 선택한 다음 구성을 선택합니다. `DescribeOrganizationConfiguration` API를 호출하여 구성 유형을 볼 수도 있습니다.

로컬 구성에서 위임된 관리자 계정은 새 계정이 조직에 가입할 때 새 계정에서 Security Hub 및 기본 보안 표준을 자동으로 활성화하도록 선택할 수 있습니다. 이러한 새 계정 설정은 현재 리전에 적용됩니다. 기타 Security Hub 설정은 각 리전의 각 구성원 계정별로 개별적으로 구성해야 합니다.

로컬 구성 대신 중앙 구성을 사용하는 것이 좋습니다. 중앙 구성에서 위임된 관리자 계정은 여러 리전에 적용되는 Security Hub 구성 정책을 생성하고 조직의 다양한 계정 및 OU(조직 단위)에 Security Hub 기능을 지정할 수 있습니다. 단일 구성 정책을 전체 조직에 적용하거나 다른 구성 정책을 여러 계정 및 OU에 적용할 수 있습니다. 예를 들어 프로덕션 계정에서는 한 세트의 표준 및 제어를 활성화하고 테스트 계정에서는 다른 표준 및 제어 세트를 활성화할 수 있습니다. DA는 필요에 따라 구성 정책을 편집할 수 있습니다.

중앙 구성의 작동 방식에 대한 자세한 내용은 중앙 구성 작동 방식 섹션을 참조하세요.

로컬 구성에서 중앙 구성으로 전환하는 방법에 대한 지침은 중앙 구성 사용 시작 섹션을 참조하세요.

계정에 허용된 작업

관리자 및 구성원 계정은 다음 표에 나온 AWS Security Hub 작업에 액세스할 수 있습니다. 표에서 값의 의미는 다음과 같습니다.

- 임의 – 이 계정은 동일한 관리자에 속한 모든 계정에 대해 작업을 수행할 수 있습니다.
- 현재 – 이 계정은 해당 계정(현재 로그인되어 있는 계정)에 대해서만 작업을 수행할 수 있습니다.
- 대시(-) – 해당 계정에서 작업을 수행할 수 없음을 나타냅니다.

표에 나와 있듯이 허용되는 작업은 AWS Organizations와의 통합 및 조직에서 사용하는 구성 유형에 따라 다릅니다. 중앙 구성과 로컬 구성의 차이에 대한 자세한 내용은 AWS Organizations를 사용하여 계정 관리 섹션을 참조하세요.

Security Hub는 구성원 계정의 조사 결과를 관리자 계정에 복사하지 않습니다. Security Hub에서는 모든 조사 결과가 특정 계정의 특정 리전에 수집됩니다. 각 리전에서 관리자 계정은 해당 리전의 구성원 계정에 대한 조사 결과를 보고 관리할 수 있습니다.

집계 영역을 설정하는 경우 관리자 계정은 집계 영역에 복제된 연결된 리전의 구성원 계정에 대한 조사 결과를 보고 관리할 수 있습니다. 크로스 리전 집계에 대한 자세한 내용은 크로스 리전 집계 활성화를 참조하세요.

이 표에는 관리자 및 구성원 계정의 기본 권한이 반영되어 있습니다. 사용자 지정 IAM 정책을 사용하여 Security Hub 특징 및 기능에 대한 액세스를 추가로 제한할 수 있습니다. 지침과 예시는 AWS Security Hub의 사용자 페르소나에 맞게 IAM 정책 조정하기라는 블로그 게시물을 참고하세요.

Organizations와 통합하고 중앙 구성을 사용하는 경우 허용되는 작업

Organizations와 통합하고 중앙 구성을 사용하는 경우 관리자 및 구성원 계정은 다음과 같이 Security Hub 작업에 액세스할 수 있습니다.

작업	Security Hub 위임된 관리자 계정	중앙 관리형 구성원 계정	자체 관리형 구성원 계정
Security Hub 구성 정책 생성 및 관리	자체 관리형 및 중앙 관리형 계정의 경우	–	–
조직 세부 정보 보기	모두	–	–
구성원 계정 연결 해지	모두	–	–
구성원 계정 삭제	모든 비조직 계정	–	–
Security Hub 비활성화	현재 계정 및 중앙 관리형 계정의 경우	–	Current
조사 결과 및 조사 결과 기록 보기	모두	Current	Current
조사 결과 업데이트	모두	Current	Current
인사이트 결과 보기	모두	Current	Current

작업	Security Hub 위임된 관리자 계정	중앙 관리형 구성원 계정	자체 관리형 구성원 계정
제어 기능 세부 정보 보기	모두	Current	Current
통합 제어 기능에 대한 조사 결과 켜기 또는 끄기	모두	–	–
표준 활성화 및 비활성화	현재 계정 및 중앙 관리형 계정의 경우	–	Current
제어 기능 활성화 및 비활성화	현재 계정 및 중앙 관리형 계정의 경우	–	Current
통합 활성화 및 비활성화	Current	Current	Current
크로스 리전 집계 활성화 구성	모두	–	–
홈 리전 및 연결된 리전 선택	임의(홈 리전을 변경하려면 중앙 구성을 중지했다가 다시 시작해야 함)	–	–
사용자 지정 작업 구성	Current	Current	Current
자동화 규칙 구성	모두	–	–
사용자 지정 인사이트 구성	Current	Current	Current

Organizations와 통합하고 로컬 구성을 사용하는 경우 허용되는 작업

Organizations와 통합하고 로컬 구성을 사용하는 경우 관리자 및 구성원 계정은 다음과 같이 Security Hub 작업에 액세스할 수 있습니다.

작업	Security Hub 위임된 관리자 계정	구성원 계정
Security Hub 구성 정책 생성 및 관리	–	–
조직 세부 정보 보기	모두	–
구성원 계정 연결 해지	모두	–
구성원 계정 삭제	–	–
Security Hub 비활성화	–	현재(계정이 위임된 관리자와 연결 해제된 경우)
조사 결과 및 조사 결과 기록 보기	모두	Current
조사 결과 업데이트	모두	Current
인사이트 결과 보기	모두	Current
제어 기능 세부 정보 보기	모두	Current
통합 제어 기능에 대한 조사 결과 켜기 또는 끄기	모두	–
표준 활성화 및 비활성화	Current	Current
새 조직 계정에서 Security Hub 및 기본 표준을 자동으로 활성화	현재 계정 및 새 조직 계정의 경우	–
제어 기능 활성화 및 비활성화	Current	Current
통합 활성화 및 비활성화	Current	Current
크로스 리전 집계 활성화 구성	모두	–
사용자 지정 작업 구성	Current	Current

작업	Security Hub 위임된 관리자 계정	구성원 계정
자동화 규칙 구성	모두	–
사용자 지정 인사이트 구성	Current	Current

초대 기반 계정에 허용된 작업

AWS Organizations와 통합하는 대신 초대 기반 방법을 사용하여 계정을 수동으로 관리하는 경우 관리자 및 구성원 계정은 다음과 같이 Security Hub 작업에 액세스할 수 있습니다.

작업	Security Hub 관리자 계정	구성원 계정
Security Hub 구성 정책 생성 및 관리	–	–
조직 세부 정보 보기	모두	–
구성원 계정 연결 해지	모두	Current
구성원 계정 삭제	모두	–
Security Hub 비활성화	현재(활성화된 구성원 계정이 없는 경우)	현재(계정이 관리자 계정과 연결 해제된 경우)
조사 결과 및 조사 결과 기록 보기	모두	Current
조사 결과 업데이트	모두	Current
인사이트 결과 보기	모두	Current
제어 기능 세부 정보 보기	모두	Current
통합 제어 기능에 대한 조사 결과 켜기 또는 끄기	모두	–
표준 활성화 및 비활성화	Current	Current

작업	Security Hub 관리자 계정	구성원 계정
새 조직 계정에서 Security Hub 및 기본 표준을 자동으로 활성화	–	–
제어 기능 활성화 및 비활성화	Current	Current
통합 활성화 및 비활성화	Current	Current
크로스 리전 집계 활성화 구성	모두	–
사용자 지정 작업 구성	Current	Current
자동화 규칙 구성	모두	–
사용자 지정 인사이트 구성	Current	Current

계정 관리에 대한 제한 및 권장 사항

다음 섹션에는 AWS Security Hub에서 구성원 계정을 관리할 때 염두에 두어야 할 몇 가지 제한 및 권장 사항이 요약되어 있습니다.

구성원 계정 최대 수

와의 AWS Organizations통합을 사용하는 경우 Security Hub는 각 AWS 리전계정에서 위임된 관리자 계정당 최대 10,000개의 구성원 계정을 지원합니다. Security Hub를 수동으로 활성화하고 관리하는 경우 Security Hub는 각 지역의 관리자 계정당 최대 1,000개의 구성원 계정 초대를 지원합니다.

계정 및 리전

조직을 통한 멤버십

Security Hub를 와 AWS Organizations통합하면 조직 관리 계정이 Security Hub의 위임된 관리자 (DA) 계정을 지정할 수 있습니다. 조직 관리 계정은 Organizations에서 DA로 설정할 수 없습니다. Security Hub에서는 허용되지만 Organizations 관리 계정은 DA가 아닌 것이 좋습니다.

모든 리전에 DA 계정을 동일하게 선택하는 것을 권장합니다. 중앙 구성을 사용하는 경우 Security Hub는 조직의 Security Hub를 구성하는 모든 리전에서 동일한 DA 계정을 설정합니다.

또한 AWS 보안 및 규정 준수 서비스 전반에서 동일한 DA 계정을 선택하여 보안 관련 문제를 단일 창에서 관리하는 것이 좋습니다.

초대를 통한 멤버십

초대를 통해 생성된 구성원 계정의 경우 초대를 보낸 리전에서만 관리자-구성원 계정 연결이 생성됩니다. 관리자 계정은 Security Hub를 사용하려는 각 리전에서 Security Hub를 활성화해야 합니다. 그러면 관리자 계정이 각 계정을 해당 리전의 구성원 계정이 되도록 초대합니다.

관리자-구성원 관계에 대한 제한 사항

> **Note**
>
> Security Hub 통합을 사용하고 회원 계정을 수동으로 초대하지 않은 경우에는 이 섹션이 적용되지 않습니다. AWS Organizations

한 계정이 관리자 계정이면서 구성원 계정일 수 없습니다.

멤버 계정은 한 번에 하나의 관리자 계정만 연결할 수 있습니다. Security Hub 관리자 계정이 조직 계정을 활성화한 경우 해당 계정은 다른 계정의 초대를 수락할 수 없습니다. 계정이 이미 초대를 수락한 경우 조직의 Security Hub 관리자 계정에서 해당 계정을 활성화할 수 없습니다. 또한, 다른 계정의 초대를 받을 수 없습니다.

수동 초대 프로세스의 경우 멤버십 초대를 수락하는 것은 선택 사항입니다.

서비스 전반에서 관리자 계정 조정하기

Security Hub는 아마존, 아마존 인스펙터 GuardDuty, 아마존 메이시와 같은 다양한 AWS 서비스의 조사 결과를 집계합니다. 또한 Security Hub를 사용하면 사용자가 GuardDuty 발견한 내용을 토대로 Amazon Detective에서 조사를 시작할 수 있습니다.

하지만, 이러한 다른 서비스에서 설정한 관리자-구성원 관계는 Security Hub에 자동으로 적용되지 않습니다. Security Hub는 이러한 모든 서비스에 관리자 계정과 동일한 계정을 사용할 것을 권장합니다. 이 관리자 계정은 보안 도구를 담당하는 계정이어야 합니다. 또한, 동일한 계정이 AWS Config에 대한 집계 계정이어야 합니다.

예를 들어 GuardDuty 관리자 계정 A의 사용자는 콘솔에서 GuardDuty 구성원 계정 B와 C의 조사 결과를 볼 수 있습니다. GuardDuty 계정 A가 Security Hub를 활성화한 경우 계정 A의 사용자는 Security

Hub에서 계정 B와 C의 GuardDuty 검색 결과를 자동으로 볼 수 없습니다. 이러한 계정에는 Security Hub 관리자-구성원 관계도 필요합니다.

이를 수행하려면, 계정 A를 Security Hub 관리자 계정으로 만들고 계정 B와 C가 Security Hub 구성원 계정이 되도록 활성화하십시오.

계정 작업이 Security Hub 데이터에 미치는 영향

이러한 계정 작업은 AWS Security Hub 데이터에 다음과 같은 영향을 미칩니다.

Security Hub 비활성화됨

중앙 구성을 사용하는 경우 위임된 관리자(DA)는 특정 계정 및 OU(조직 단위)에서 AWS Security Hub를 비활성화하는 Security Hub 구성 정책을 만들 수 있습니다. 이 경우 홈 리전 및 연결된 리전의 지정된 계정 및 OU에서 Security Hub가 비활성화됩니다.

중앙 구성을 사용하지 않는 경우 Security Hub를 활성화한 각 계정 및 리전에서 개별적으로 Security Hub를 비활성화해야 합니다.

관리자 계정에서 Security Hub가 비활성화된 경우 관리자 계정에 대해 새 결과가 생성되지 않습니다. DA 계정에서 Security Hub가 비활성화된 경우에도 중앙 구성을 사용할 수 없습니다. 기존 결과는 90일 후에 삭제됩니다.

다른 AWS 서비스와의 통합이 제거되었습니다.

활성화된 보안 표준 및 제어가 비활성화됩니다.

구성원 계정 연결, 사용자 지정 작업, 인사이트 및 타사 제품 구독을 포함한 기타 데이터 및 설정은 유지됩니다.

구성원 계정이 관리자 계정에서 연결 해제됨

구성원 계정이 관리자 계정에서 연결이 해제되면 관리자 계정은 구성원 계정의 결과를 볼 수 있는 권한을 잃습니다. 그러나 Security Hub는 두 계정 모두에서 여전히 활성화되어 있습니다.

중앙 구성을 사용하는 경우 DA는 DA 계정과 연결이 끊긴 구성원 계정에 대해 Security Hub를 구성할 수 없습니다.

관리자 계정에 정의된 사용자 지정 설정 또는 통합은 이전 구성원 계정에서 얻은 결과에 적용되지 않습니다. 예를 들어, 계정 연결이 끊긴 후 Amazon EventBridge 규칙의 이벤트 패턴으로 사용되는 관리자

계정에 사용자 지정 작업이 있을 수 있습니다. 하지만, 구성원 계정에서는 이 사용자 지정 작업을 사용할 수 없습니다.

Security Hub 관리자 계정의 계정 목록에서 제거된 계정은 연결 해제됨 상태입니다.

구성원 계정이 조직에서 제거

구성원 계정이 조직에서 제거되면 Security Hub 관리자 계정은 구성원 계정의 조사 결과를 볼 수 있는 권한을 잃게 됩니다. 하지만 Security Hub는 제거 전과 동일한 설정으로 두 계정 모두에서 계속 활성화됩니다.

중앙 구성을 사용하는 경우 위임된 관리자가 속한 조직에서 제거된 후에는 구성원 계정에 대해 Security Hub를 구성할 수 없습니다. 하지만 수동으로 변경하지 않는 한 계정은 제거 이전의 설정을 그대로 유지합니다.

Security Hub 관리자 계정의 계정 목록에서 제거된 계정은 삭제됨 상태입니다.

계정이 일시 중지되었습니다.

계정이 AWS에서 일시 중단되면 해당 계정은 Security Hub에서 조사 결과를 볼 수 있는 권한을 잃게 됩니다. 해당 계정에 대한 새로운 조사 결과는 생성되지 않습니다. 일시 중지된 계정의 관리자 계정은 기존 계정의 조사 결과를 볼 수 있습니다.

조직 계정의 경우 구성원 계정 상태가 계정 일시 중단됨으로 변경될 수도 있습니다. 관리자 계정이 계정을 활성화하려고 시도하는 동시에 계정이 일시 중지되면 이런 상황이 발생합니다. 계정 일시 중지됨 계정의 관리자 계정은 해당 계정의 조사 결과를 볼 수 없습니다. 그 외에는 일시 중지됨 상태는 구성원 계정 상태에 영향을 주지 않습니다.

중앙 구성을 사용하는 경우 위임된 관리자가 구성 정책을 일시 중지된 계정과 연결하려고 하면 정책 연결이 실패합니다.

90일이 지나면 계정이 해지되거나 다시 활성화됩니다. 계정이 다시 활성화되면 Security Hub 권한이 복원됩니다. 구성원 계정 상태가 계정 일시 중단됨인 경우 관리자 계정이 이 계정을 수동으로 활성화해야 합니다.

계정이 폐쇄되었습니다.

AWS 계정가 폐쇄되면 Security Hub는 다음과 같이 폐쇄에 응답합니다.

Security Hub는 계정 해지 발효일로부터 90일 동안 계정에 대한 조사 결과를 유지합니다. 90일의 기간이 종료되는 시점에 Security Hub는 계정의 모든 조사 결과를 영구적으로 삭제합니다.

- 90일 이상 조사 결과를 유지하려면 EventBridge 규칙에 사용자 지정 작업을 사용하여 조사 결과를 Amazon S3 버킷에 저장할 수 있습니다. Security Hub가 조사 결과를 보관하는 한, 폐쇄된 계정을 다시 열면 Security Hub는 계정에 대한 조사 결과를 복원합니다.
- 계정이 Security Hub 관리자 계정인 경우, 관리자로서 제거되고 모든 구성원 계정이 제거됩니다. 계정이 구성원 계정인 경우 Security Hub 관리자 계정에서 구성원으로서 연결이 해제되고 제거됩니다.
- 자세한 내용은 AWS 과금 정보 및 비용 관리 사용 설명서의 계정 해지를 참조하세요.

Important

AWS GovCloud (US) 리전의 고객인 경우:

- 계정을 해지하기 전에 정책 데이터 및 기타 계정 리소스를 백업한 다음 삭제합니다. 계정을 해지한 뒤에는 더 이상 해당 계정에 액세스할 수 없습니다.

크로스 리전 집계 활성화

크로스 리전 집계 활성화를 사용하면 여러 리전의 조사 결과, 조사 결과 업데이트, 인사이트, 제어 규정 준수 상태 및 보안 점수를 단일 집계 영역으로 집계할 수 있습니다. 그러면 집계 영역에서 이 모든 데이터를 관리할 수 있습니다.

> **Note**
>
> 에서는 AWS GovCloud (US)지역 간 집계가 검색 결과, 업데이트 찾기 및 전체 인사이트에 대해서만 지원됩니다. AWS GovCloud (US)특히 AWS GovCloud (미국 동부) 와 (미국 서부) 간의 결과, 업데이트 검색 결과 및 인사이트만 집계할 수 있습니다. AWS GovCloud 중국 리전에서는 중국 리전 전반의 조사 결과, 조사 결과 업데이트 및 인사이트에 대해서만 크로스 리전 집계 활성화가 지원됩니다. 특히 중국(베이징) 및 중국(닝샤) 간에는 조사 결과, 조사 결과 업데이트, 인사이트만 집계할 수 있습니다.

미국 동부(버지니아 북부)를 집계 영역으로 설정하고 미국 서부(오레곤) 및 미국 서부(캘리포니아 북부)를 연결 리전으로 설정한다고 가정해 보겠습니다. 미국 동부(버지니아 북부) 의 조사 결과 페이지를 보면 세 리전 모두의 조사 결과를 볼 수 있습니다. 이러한 조사 결과에 대한 업데이트도 세 리전 모두에 반영됩니다.

제어의 활성화 상태는 각 리전에서 수정해야 합니다. 연결된 리전에서는 제어가 활성화되었지만 집계 영역에서는 비활성화된 경우 집계 영역에서 제어의 규정 준수 상태를 볼 수 있지만 집계 영역에서는 해당 제어를 활성화하거나 비활성화할 수 없습니다.

리전 간 보안 점수 및 규정 준수 상태를 보려면 Security Hub를 사용하는 IAM 역할에 다음 권한을 추가하십시오.

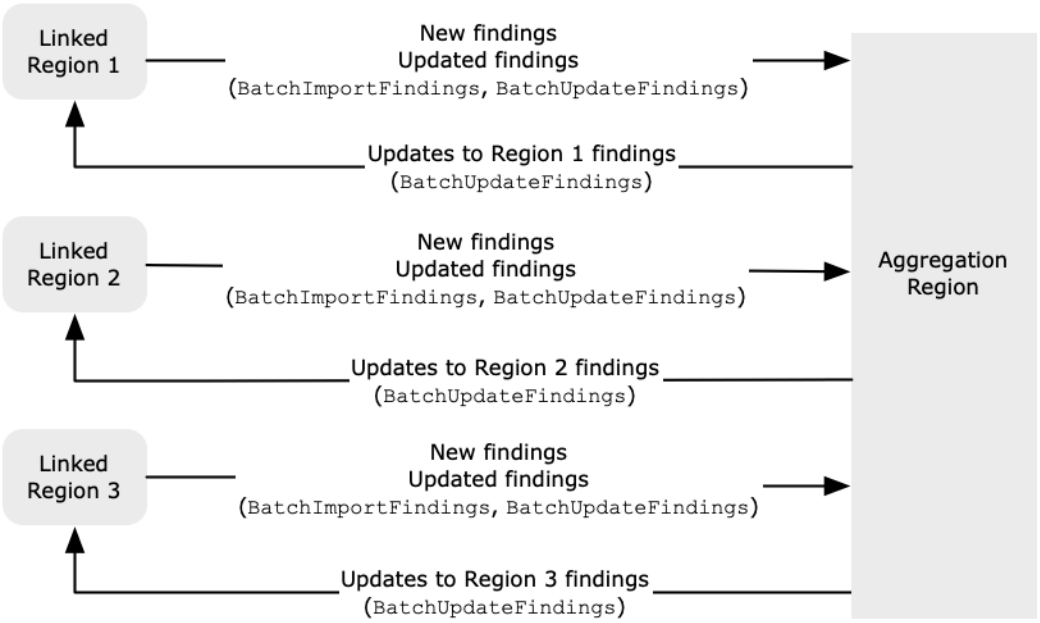
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

크로스 리전 집계 활성화 작동 방법

지역 간 집계가 활성화된 경우 Security Hub는 연결된 지역의 다음 데이터를 집계 지역으로 복제합니다. 이는 지역 간 집계가 활성화된 모든 계정에서 발생합니다.

- 조사 결과
- 인사이트
- 제어 규정 준수 상태
- 보안 점수

이전 목록의 새 데이터 외에 Security Hub는 연결된 리전과 집계 영역 간에 이 데이터에 대한 업데이트를 복제합니다. 연결된 리전에서 발생한 업데이트는 집계 영역에 복제됩니다. 집계 영역에서 발생한 업데이트는 연결된 리전에 다시 복제됩니다.



집계 영역과 연결 리전의 업데이트가 충돌하는 경우 가장 최근 업데이트가 사용됩니다.

크로스 리전 집계 활성화는 Security Hub 비용에 추가되지 않습니다. Security Hub에서 새 데이터나 업데이트를 복제할 때는 요금이 부과되지 않습니다.

집계 영역의 요약 페이지에서는 연결된 리전 전반의 활성 조사 결과를 볼 수 있습니다. 자세한 내용은 심각도별 결과에 대한 크로스 리전 요약 보기를 참조하세요. 조사 결과를 분석하는 기타 요약 페이지 패널에는 연결된 리전 전반의 정보도 표시됩니다.

집계 영역의 보안 점수는 전달된 제어의 수를 연결된 모든 리전에서 활성화된 제어의 수와 비교하여 계산됩니다. 또한 하나 이상의 연결된 리전에서 제어가 활성화된 경우 집계 영역의 보안 표준 세부 정보 페이지에서 해당 제어를 볼 수 있습니다. 표준 세부 정보 페이지의 규제 준수 상태는 연결 리전 전반의 조사 결과를 반영합니다. 하나 이상의 연결된 리전에서 제어와 관련된 보안 검사에 실패하는 경우 집계

영역의 표준 세부 정보 페이지에 해당 제어의 규정 준수 상태가 실패로 표시됩니다. 보안 검사 수에는 연결된 모든 리전의 조사 결과가 포함됩니다.

Security Hub는 계정에 Security Hub가 활성화된 리전의 데이터만 집계합니다. Security Hub는 크로스 리전 집계 활성화 구성을 기반으로 하는 계정에 대해 자동으로 활성화되지 않습니다.

관리자 및 구성원 계정 집계

독립형 계정, 구성원 계정, 관리자 계정은 지역 간 집계를 구성할 수 있습니다. 관리자가 구성한 경우 관리자 계정에서 지역 간 집계가 작동하려면 관리자 계정이 있어야 합니다. 관리자 계정이 제거되거나 구성원 계정과의 연결이 끊어지면 해당 구성원 계정의 지역 간 집계가 중지됩니다. 관리자-구성원 관계가 시작되기 전에 계정에 지역 간 집계가 활성화된 경우에도 마찬가지입니다.

관리자 계정이 지역 간 집계를 활성화하면 Security Hub는 관리자 계정이 연결된 모든 지역에서 생성한 데이터를 집계 지역에 복제합니다. 또한 Security Hub는 해당 관리자와 연결된 구성원 계정을 식별하며 각 구성원 계정은 관리자의 지역 간 집계 설정을 상속합니다. Security Hub는 멤버 계정이 모든 연결 지역에서 생성하는 데이터를 집계 지역에 복제합니다.

관리자는 관리 지역 내의 모든 구성원 계정에서 보안 결과에 액세스하고 이를 관리할 수 있습니다. 하지만 Security Hub 관리자는 집계 지역에 로그인해야 모든 구성원 계정 및 연결된 지역의 집계된 데이터를 볼 수 있습니다.

Security Hub 회원 계정으로서 모든 연결 지역의 계정에서 집계된 데이터를 보려면 집계 지역에 로그인해야 합니다. 멤버 계정에는 다른 멤버 계정의 데이터를 볼 권한이 없습니다.

관리자 계정은 구성원 계정을 수동으로 초대하거나 통합된 AWS Organizations조직의 위임 관리자 역할을 할 수 있습니다. 수동으로 초대된 회원 계정의 경우 관리자가 통합 지역 및 모든 연결 지역에서 계정을 초대해야 지역 간 집계가 제대로 작동할 수 있습니다. 또한 관리자가 구성원 계정의 조사 결과를 볼 수 있도록 하려면 구성원 계정의 집계 지역 및 모든 연결 지역에서 Security Hub를 활성화해야 합니다. 집계 지역을 다른 용도로 사용하지 않는 경우 해당 지역의 Security Hub 표준 및 통합을 비활성화하여 요금이 부과되지 않도록 할 수 있습니다.

지역 간 집계를 사용할 계획이고 관리자 계정이 여러 명인 경우 다음 모범 사례를 따르는 것이 좋습니다.

- 각 관리자 계정에는 서로 다른 구성원 계정이 있습니다.
- 각 관리자 계정은 여러 리전에서 동일한 구성원 계정을 가집니다.
- 각 관리자 계정은 서로 다른 집계 영역을 사용합니다.

> **Note**
>
> 지역 간 집계가 중앙 구성에 미치는 영향을 이해하려면 을 참조하십시오. 중앙 구성 및 크로스 리전 집계 활성화

중앙 구성 및 크로스 리전 집계 활성화

중앙 구성은 Security Hub의 옵트인 기능으로, 통합할 경우 사용할 수 있습니다. AWS Organizations중앙 구성을 사용하는 경우 위임된 관리자 계정으로 조직의 계정 및 조직 단위(OU)에 대한 Security Hub 서비스, 표준 및 제어를 구성할 수 있습니다. 계정 및 OU를 구성하기 위해 위임된 관리자는 Security Hub 구성 정책을 생성합니다. 구성 정책을 사용하여 Security Hub의 활성화 또는 비활성화 여부와 활성화되는 표준 및 제어를 정의할 수 있습니다. 위임된 관리자는 구성 정책을 특정 계정, OU 또는 루트(전체 조직)와 연결합니다.

위임된 관리자는 집계 영역에서만 조직에 대한 구성 정책을 만들고 관리할 수 있습니다. 또한 구성 정책은 집계 영역 및 연결된 모든 리전에 적용됩니다. 일부 연결된 리전에만 적용되고 다른 리전에는 적용되지 않는 구성 정책을 만들 수 없습니다. 중앙 구성에서는 집계 영역을 홈 리전이라고 합니다. 동일한 리전이 중앙 구성를 위한 홈 리전 역할을 하고 크로스 리전 집계를 위한 집계 영역 역할을 해야 합니다. 크로스 리전 집계 활성화에 대한 자세한 내용은 크로스 리전 집계 활성화를 참조하세요.

중앙 구성을 사용하려면 홈 지역과 하나 이상의 연결된 지역을 지정해야 합니다.

크로스 리전 집계 활성화 설정을 변경하면 구성 정책에 영향을 미칠 수 있습니다. 연결된 리전을 추가하면 구성 정책이 해당 리전에 적용됩니다. 리전이 옵트인 리전인 경우 해당 리전에 구성 정책이 적용되려면 해당 리전을 활성화해야 합니다. 반대로 연결된 리전을 제거하면 해당 리전에는 구성 정책이 더 이상 적용되지 않습니다. 해당 리전의 계정은 연결된 리전이 제거되었을 때의 설정을 유지합니다. 이러한 설정을 변경할 수 있지만 각 계정 및 리전에서 개별적으로 변경해야 합니다.

홈 리전을 제거하거나 변경하면 구성 정책 및 정책 연결이 삭제됩니다. 더 이상 어떤 리전에서도 중앙 구성을 사용하거나 구성 정책을 만들 수 없습니다. 계정은 홈 리전이 변경되거나 제거되기 전의 설정을 유지합니다. 이러한 설정은 언제든지 변경할 수 있지만 더 이상 중앙 구성을 사용하지 않으므로 각 계정 및 리전에서 설정을 개별적으로 수정해야 합니다. 새 홈 리전을 지정하는 경우 중앙 구성을 사용하고 구성 정책을 다시 만들 수 있습니다.

중앙 구성에 대한 자세한 내용은 중앙 구성 작동 방식 섹션을 참조하세요.

크로스 리전 집계 활성화 활성화하기

집계 지역으로 지정하려는 지역에서 지역 간 집계를 활성화해야 합니다. AWS 리전

기본적으로 비활성화된 리전을 집계 영역으로 사용할 수 없습니다. 기본적으로 비활성화되는 리전 목록은 AWS 일반 참조에서 리전 활성화를 참조하십시오.

크로스 리전 집계 활성화 활성화하기(콘솔)

크로스 리전 집계 활성화를 활성화할 때는 연결된 리전을 선택합니다. 또한 Security Hub에서 새 리전을 지원하기 시작하고 선택한 경우 새 리전을 자동으로 연결할지 여부도 선택합니다.

크로스 리전 집계 활성화를 활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 콘솔을 엽니다. AWS Security Hub
2. AWS 리전 선택기를 사용하여 집계 지역으로 사용할 지역에 로그인합니다.
3. Security Hub 탐색 메뉴에서 설정을 선택한 다음 리전을 선택합니다.
4. 조사 결과 집계에서 조사 결과 집계 구성을 선택합니다.

   기본적으로 집계 영역은 집계 영역 없음으로 설정됩니다.
5. 집계 영역에서 옵션을 선택하여 현재 리전을 집계 영역으로 지정합니다.
6. 필요에 따라 연결된 리전에서 데이터를 집계할 리전을 선택합니다.
7. Security Hub에서 지원하므로 파티션에 있는 새 리전의 데이터를 자동으로 집계하고 사용자가 이를 선택하도록 하려면 미래 리전 연결을 선택합니다.
8. 저장을 선택합니다.

지역 간 집계 활성화 (Security Hub API,) AWS CLI

Security Hub API를 사용하여 크로스 리전 집계 활성화를 활성화할 수 있습니다.

Security Hub API에서 크로스 리전 집계 활성화를 활성화하려면 조사 결과 집계자를 생성합니다. 집계 영역으로 사용할 리전에서 조사 결과 집계자를 생성해야 합니다.

검색 결과 수집기 (Security Hub API,) 를 만들려면 AWS CLI

- Security Hub API: 집계 영역으로 사용하려는 리전에서 `CreateFindingAggregator` 작업을 사용합니다. `RegionLinkingMode`의 경우 다음 옵션 중 하나를 선택합니다.

- ALL_REGIONS- Security Hub는 모든 리전의 데이터를 집계합니다. 또한 Security Hub는 새로운 리전이 지원되고 사용자가 이를 선택할 때 해당 리전의 데이터도 집계합니다.
- ALL_REGIONS_EXCEPT_SPECIFIED- Security Hub는 제외하려는 리전을 제외한 모든 리전의 데이터를 집계합니다. 또한 Security Hub는 새로운 리전이 지원되고 사용자가 이를 선택할 때 해당 리전의 데이터도 집계합니다. 집계에서 제외할 리전 목록을 제공하는 데 Regions를 사용합니다.
- SPECIFIED_REGIONS- Security Hub는 선택된 리전 목록에서 데이터를 집계합니다. Security Hub는 새 리전의 데이터를 자동으로 집계하지 않습니다. 집계할 리전 목록을 제공하는 데 Regions를 사용합니다.

- AWS CLI: 명령줄에서 create-finding-aggregator 명령을 실행합니다. 각 리전을 공백으로 구분합니다.

```
aws securityhub create-finding-aggregator --region <aggregation Region> --region-
linking-mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --
regions <Region list>
```

다음 예시에서는 선택한 리전에 대해 크로스 리전 집계 활성화가 구성되어 있습니다. 집계 영역은 미국 동부(버지니아 북부) 입니다. 연결된 리전은 미국 서부(캘리포니아 북부) 및 미국 서부(오레곤)입니다.

```
aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

크로스 리전 집계 활성화 설정 보기

모든 리전의 현재 크로스 리전 집계 활성화 구성을 볼 수 있습니다. 구성에는 집계 영역, 연결된 리전, 새 리전과의 자동 연결 여부가 포함됩니다.

크로스 리전 집계 활성화 구성 보기(콘솔)

설정 페이지의 리전 탭에는 현재 크로스 리전 집계 활성화 구성이 표시됩니다. 모든 리전에서 구성을 볼 수 있습니다. 구성원 계정은 관리자 계정이 구성한 리전 간 구성도 볼 수 있습니다.

크로스 리전 집계 활성화가 활성화되지 않은 경우 리전 탭에 크로스 리전 집계 활성화를 활성화하는 옵션이 표시됩니다. the section called “크로스 리전 집계 활성화 활성화하기” 섹션을 참조하십시오. 관리자 계정 및 독립 실행형 계정만 크로스 리전 집계 활성화를 활성화할 수 있습니다.

크로스 리전 집계 활성화가 활성화된 경우 리전 탭에 다음 정보가 표시됩니다.

- 집계 영역
- Security Hub가 지원하고 사용자가 선택한 새 리전의 조사 결과, 인사이트, 제어 상태 및 보안 점수를 자동으로 집계할지 여부
- 연결 리전 목록

현재 지역 간 집계 구성 보기 (Security Hub API,) AWS CLI

Security Hub API를 사용하거나 AWS CLI 현재의 지역 간 집계 구성을 볼 수 있습니다. 모든 리전에서 크로스 리전 집계 활성화 구성을 볼 수 있습니다.

현재 크로스 리전 집계 활성화 구성(Security Hub API, AWS CLI)을 보려면

- Security Hub API: `GetFindingAggregator` API를 사용합니다. 요청할 때 조사 결과 집계 ARN을 제공해야 합니다. 조사 결과 집계 ARN을 구하려면 `ListFindingAggregators`를 사용합니다.
- AWS CLI: 명령줄에서 `get-finding-aggregator` 명령을 실행합니다. 조사 결과 집계 ARN을 구하려면 `list-finding-aggregators`를 사용합니다.

```
aws securityhub get-finding-aggregator --finding-aggregator-arn <finding aggregator
 ARN>
```

크로스 리전 집계 활성화 구성 업데이트

크로스 리전 집계 활성화 구성을 업데이트하여 현재 집계 영역의 연결된 AWS 리전 을(를) 변경할 수 있습니다. 또한 새 리전의 조사 결과, 인사이트, 제어 상태 및 보안 점수를 자동으로 집계할지 여부도 변경할 수 있습니다.

크로스 리전 집계 활성화에 대한 변경 사항은 AWS 계정에서 해당 리전이 활성화될 때까지 옵트인 리전에 대해 구현되지 않습니다. 2019년 3월 20일 또는 그 이후에 AWS 도입된 지역은 옵트인 지역입니다.

연결된 리전의 데이터 집계를 중지하면 Security Hub는 집계 영역에서 기존의 집계 데이터를 제거하지 않습니다.

업데이트 프로세스를 사용하여 집계 영역을 변경할 수는 없습니다. 집계 영역을 변경하려면 다음을 수행해야 합니다.

1. 크로스 리전 집계 활성화 중지 the section called “크로스 리전 집계 활성화 중지” 섹션을 참조하십시오.

2. 새 집계 영역으로 설정하려는 리전으로 변경합니다.
3. 크로스 리전 집계 활성화를 활성화 the section called “크로스 리전 집계 활성화 활성화하기” 섹션을 참조하십시오.

크로스 리전 집계 활성화 구성 업데이트(콘솔)

현재 집계 영역에서 크로스 리전 집계 활성화 구성을 업데이트해야 합니다.

집계 영역 AWS 리전 이외의 경우 집계 결과 패널에 집계 영역의 구성을 편집해야 한다는 메시지가 표시됩니다. 이 메시지를 선택하면 집계 영역으로 이동할 수 있는 링크가 표시됩니다.

현재 집계 영역의 연결된 리전을 변경하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 현재 집계 영역으로 변경합니다.
3. Security Hub 탐색 메뉴에서 설정을 선택한 다음 리전을 선택합니다.
4. 조사 결과 집계에서 편집을 선택합니다.
5. 연결 리전에서 선택한 연결 리전을 업데이트합니다.
6. 필요한 경우 미래 리전 연결 선택 여부를 변경합니다. 이 설정은 Security Hub가 새 리전에 대한 지원을 추가하고 사용자가 선택할 때 새 리전을 자동으로 연결할지 여부를 결정합니다.
7. 저장을 선택합니다.

지역 간 집계 구성 업데이트 (Security Hub API,) AWS CLI

Security Hub API를 사용하거나 AWS CLI 지역 간 집계 구성을 업데이트할 수 있습니다. 현재 집계 영역에서 크로스 리전 집계 활성화를 업데이트해야 합니다.

리전 연결 모드를 변경할 수 있습니다. 연결 모드가 `ALL_REGIONS_EXCEPT_SPECIFIED`또는 `SPECIFIED_REGIONS`인 경우 제외 또는 포함된 리전 목록을 변경할 수 있습니다.

제외 또는 포함된 리전 목록을 변경할 때는 업데이트와 함께 전체 목록을 제공해야 합니다. 예를 들어 현재 미국 동부(오하이오) 의 조사 결과를 집계하고 있고 미국 서부(오레곤) 의 조사 결과도 집계하려는 경우를 가정해 보겠습니다. `UpdateFindingAggregator`을 직접적으로 호출하면 미국 동부(오하이오) 와 미국 서부(오레곤) 가 모두 포함된 `Regions` 목록을 제공합니다.

지역 간 집계를 업데이트하려면 (Security Hub API,) AWS CLI

- Security Hub API: `UpdateFindingAggregator` API 작업을 사용합니다. 조사 결과 집계자를 식별하려면 조사 결과 집계자 ARN을 제공해야 합니다. 조사 결과 집계 ARN을 구하려면 `ListFindingAggregators`를 사용합니다.

  리전 연결 모드와 제외되거나 포함된 리전의 업데이트된 목록을 제공합니다.

- AWS CLI: 명령줄에서 `update-finding-aggregator` 명령을 실행합니다. 각 리전을 공백으로 구분합니다.

```
aws securityhub update-finding-aggregator --region <aggregation Region> --finding-
aggregator-arn <finding aggregator ARN> --region-linking-mode ALL_REGIONS |
 ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region list>
```

  다음 예시에서는 크로스 리전 집계 활성화 구성이 선택한 리전에 대한 집계로 변경되었습니다. 이 명령은 현재 집계 영역인 미국 동부(버지니아 북부)에서 실행됩니다. 연결된 리전은 미국 서부(캘리포니아 북부) 및 미국 서부(오레곤)입니다.

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-aggregator-arn
 arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-
a456-426652340000 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-
west-2
```

크로스 리전 집계 활성화 중지

더 이상 데이터를 집계하지 않거나 집계 영역을 변경하려는 경우 크로스 리전 집계 활성화를 중지합니다.

크로스 리전 집계 활성화를 중지하면 Security Hub는 데이터 집계를 중지합니다. 집계 영역에서 기존의 집계 데이터는 제거되지 않습니다.

크로스 리전 집계 활성화 중지하기(콘솔)

현재 집계 영역에서 크로스 리전 집계 활성화를 중지해야 합니다.

집계 영역이 아닌 리전의 경우 조사 결과 집계 패널에 집계 영역의 구성을 편집해야 한다는 메시지가 표시됩니다. 이 메시지를 선택하면 집계 영역으로 전환할 수 있는 링크가 표시됩니다.

크로스 리전 집계 활성화를 중지하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 현재 집계 영역으로 변경합니다.
3. Security Hub 탐색 메뉴에서 설정을 선택한 다음 리전을 선택합니다.
4. 조사 결과 집계에서 편집을 선택합니다.
5. 집계 영역에서 집계 영역 없음을 선택합니다.
6. 저장을 선택합니다.
7. 확인 필드의 확인 대화 상자에 **Confirm**을 입력합니다.
8. 확인을 선택합니다.

지역 간 집계 중지 (Security Hub API,) AWS CLI

Security Hub API를 사용하여 크로스 리전 집계 활성화를 중지할 수 있습니다. 집계 영역에서 크로스 리전 집계 활성화를 중지해야 합니다.

지역 간 집계를 중지하려면 (Security Hub API,) AWS CLI

- Security Hub API: `DeleteFindingAggregator` 작업을 사용합니다. 삭제할 조사 결과 집계자를 식별하려면 조사 결과 집계자 ARN을 제공합니다. 조사 결과 집계 ARN을 구하려면 `ListFindingAggregators`를 사용합니다.
- AWS CLI: 명령줄에서 `delete-finding-aggregator` 명령을 실행합니다.

```
aws securityhub delete-finding-aggregator <finding aggregator ARN> --
region <aggregation Region>
```

AWS Security Hub의 조사 결과

AWS Security Hub를 사용하면 여러 제공업체의 대량의 조사 결과를 처리하는 복잡성을 없앨 수 있습니다. 따라서 모든 AWS 계정, 리소스 및 워크로드의 보안을 관리하고 개선하는 데 필요한 노력을 줄일 수 있습니다.

Security Hub는 다음 소스에서 조사 결과를 수신합니다.

- 활성화된 제어에 대한 Security Hub 검사입니다. the section called “제어 조사 결과 생성 및 업데이트”을 참조하십시오.
- AWS 서비스 이를 통해 통합을 활성화할 수 있습니다. the section called “AWS 서비스 통합”을 참조하십시오.
- 사용자가 활성화하는 타사 제품과의 통합. the section called “타사 제품 통합”을 참조하십시오.
- 사용자가 구성하는 사용자 지정 통합. the section called “사용자 지정 제품 통합 사용”을 참조하십시오.

Security Hub는 보안 검색 결과 형식이라는 표준 검색 결과 형식을 사용하여 검색 결과를 사용합니다. AWS 결과 형식에 대한 자세한 내용은 the section called “결과 형식”을 참조하십시오.

Security Hub는 가장 중요한 제품을 우선 순위로 지정할 수 있도록 모든 통합 제품 간의 조사 결과를 상호 연관시킵니다.

조사 결과 공급자는 조사 결과의 추가 인스턴스를 반영하도록 조사 결과를 업데이트할 수 있습니다. 조사 결과를 업데이트하여 조사 및 결과에 대한 세부 정보를 입력할 수 있습니다.

또한 Security Hub를 사용하면 리전 간 조사 결과를 집계하여 모든 조사 결과를 한 곳에서 볼 수 있습니다. 크로스 리전 집계 활성화을 참조하십시오.

주제

- AWS Security Hub에서 조사 결과 생성 및 업데이트
- 검색 결과 세부 정보 및 기록 관리 및 검토
- 조사 결과에 대한 조치 취하기 AWS Security Hub
- AWS 보안 검색 형식 (ASFF)

AWS Security Hub에서 조사 결과 생성 및 업데이트

에서 AWS Security Hub검색 결과는 다음 유형의 검색 공급자 중 하나에서 생성될 수 있습니다.

- Security Hub에서 활성화된 보안 제어
- 다른 회사와의 통합이 활성화되었습니다. AWS 서비스
- 타사 제품과의 활성화된 통합

결과가 생성된 후에는 결과 공급자 또는 고객이 업데이트할 수 있습니다.

- 결과 공급자는 `BatchImportFindings` API 작업을 사용하여 결과에 대한 일반 정보를 업데이트합니다. 조사 결과 공급자는 자신이 생성한 조사 결과만 업데이트할 수 있습니다.
- 고객은 `BatchUpdateFindings`API 작업을 사용하여 조사 결과를 업데이트합니다. `BatchUpdateFindings`고객을 대신하여 티켓팅, 사고 관리, 오케스트레이션, 수정 또는 SIEM 도구에서 사용할 수도 있습니다.

  Security Hub 콘솔에서 고객은 조사 결과의 워크플로 상태를 관리하고 조사 결과를 사용자 지정 작업으로 전송할 수 있습니다. the section called “조사 결과에 대한 조치 수행”을 참조하십시오.

Security Hub는 조사 결과를 자동으로 업데이트하고 삭제합니다. 지난 90일 동안 업데이트되지 않은 모든 조사 결과는 자동으로 삭제됩니다.

크로스 리전 집계 활성화 시 Security Hub는 연결된 리전의 새 조사 결과를 집계 영역으로 자동 집계합니다. 또한 Security Hub는 조사 결과에 대한 업데이트를 복제합니다. 연결된 리전에서 발생한 업데이트는 집계 영역에 복제됩니다. 집계 지역에서 발생하는 업데이트는 연결된 지역에 복제됩니다. 크로스 리전 집계 활성화에 대한 자세한 내용은 크로스 리전 집계 활성화을 참조하십시오.

주제

- 조사 결과 생성 및 업데이트에 BatchImportFindings 사용
- 결과를 업데이트하기 위한 BatchUpdateFindings 사용

조사 결과 생성 및 업데이트에 BatchImportFindings 사용

조사 결과 공급자는 `BatchImportFindings` API 작업을 사용하여 새 조사 결과를 생성하고 생성한 조사 결과에 대한 정보를 업데이트합니다. 작성하지 않은 조사 결과는 업데이트할 수 없습니다.

고객, SIEM, 티켓팅 도구 및 SOAR 도구는 제공업체 검색 결과 조사와 관련된 업데이트를 만드는 BatchUpdateFindings데 사용합니다. the section called “BatchUpdateFindings 사용하기” 섹션을 참조하십시오.

결과 생성 또는 업데이트 BatchImportFindings 요청을 AWS Security Hub 받을 때마다 Amazon 에서 Security Hub Findings - Imported이벤트가 자동으로 생성됩니다 EventBridge. the section called “자동 응답 및 해결”을 참조하십시오.

계정 및 배치 크기에 대한 요구 사항

BatchImportFindings는 다음 중 하나에 의해 호출되어야 합니다.

- 조사 결과와 연결된 계정. 관련 계정의 식별자는 검색 결과에 대한 AwsAccountId 속성 값입니다.
- 공식 Security Hub 파트너 통합을 위해 연동 허용 목록에 있는 계정.

Security Hub에서는 Security Hub가 활성화된 계정에 대한 결과 업데이트만 수락할 수 있습니다. 결과 공급자도 활성화해야 합니다. Security Hub가 비활성화되거나 조사 결과 공급자 통합이 활성화되지 않은 경우, 조사 결과가 InvalidAccess 오류와 함께 FailedFindings 목록에 반환됩니다.

BatchImportFindings는 조사 결과를 배치당 최대 100개, 조사 결과당 최대 240KB, 배치당 최대 6MB를 허용합니다. 스로틀 속도 제한은 리전당 계정당 10TPS이며, 버스트는 30TPS입니다.

결과 생성 또는 갱신 여부 결정

결과를 생성할지 또는 업데이트할지 여부를 결정하려면 Security Hub는 ID 필드를 확인합니다. ID의 값이 기존 결과와 일치하지 않으면 새 결과가 생성됩니다.

ID가 기존 결과와 일치하는 경우, Security Hub는 UpdatedAt 필드의 업데이트를 확인합니다.

- 업데이트의 UpdatedAt이 일치하거나 기존 결과의 UpdatedAt 이전에 발생하면 업데이트가 무시됩니다.
- 업데이트의 UpdatedAt이 기존 결과의 UpdatedAt 이후에 발생하면 기존 결과가 업데이트됩니다.

BatchImportFindings에 대한 제한된 속성

기존 검색 결과의 경우 검색 제공자는 다음 속성 및 객체를 BatchImportFindings 업데이트하는 데 사용할 수 없습니다. 이 속성은 BatchUpdateFindings를 사용해서만 업데이트할 수 있습니다.

- Note

- UserDefinedFields
- VerificationState
- Workflow

Security Hub는 해당 속성 및 객체에 대한 BatchImportFindings 요청에 제공된 모든 콘텐츠를 무시합니다. 고객 또는 고객을 대신하여 활동하는 다른 공급자는 이를 업데이트하기 위해 BatchUpdateFindings을 사용합니다.

FindingProviderFields 사용하기

또한 검색 제공자는 다음 속성을 BatchImportFindings 업데이트하는 데 사용해서는 안 됩니다.

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

대신 결과 공급자는 FindingProviderFields 객체를 사용하여 이러한 속성에 대한 값을 제공합니다.

예

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

BatchImportFindings 요청의 경우 Security Hub는 최상위 속성 및 FindingProviderFields의 값을 다음과 같이 처리합니다.

(선호) **BatchImportFindings**은 **FindingProviderFields**의 속성 값을 제공하지만 해당하는 최상위 속성에 대한 값은 제공하지 않습니다.

예를 들어 BatchImportFindings는 FindingProviderFields.Confidence을 제공하지만 Confidence을 제공하지는 않습니다. BatchImportFindings 요청에는 이 옵션을 사용하는 것이 좋습니다.

Security Hub는 FindingProviderFields의 속성 값을 업데이트합니다.

에서 속성을 아직 업데이트하지 않은 경우에만 최상위 속성에 값을 복제합니다. BatchUpdateFindings

BatchImportFindings은 최상위 속성에 대한 값을 제공하지만 **FindingProviderFields**에서 해당하는 속성의 값은 제공하지 않습니다.

예를 들어 BatchImportFindings는 FindingProviderFields.Confidence을 제공하지만 Confidence을 제공하지는 않습니다.

Security Hub는 이 값을 사용하여 FindingProviderFields의 속성을 업데이트합니다. 이는 기존 값을 모두 덮어씁니다.

Security Hub는 속성이 BatchUpdateFindings에 의해 아직 업데이트되지 않은 경우에만 최상위 속성을 업데이트합니다.

BatchImportFindings은 최상위 속성과 **FindingProviderFields**의 해당 속성 모두에 대한 값을 제공합니다.

예를 들어, BatchImportFindings는 Confidence 및 FindingProviderFields.Confidence을 모두 제공합니다.

새로운 결과의 경우 Security Hub는 FindingProviderFields의 값을 사용하여 최상위 속성과 FindingProviderFields의 해당 속성을 모두 채웁니다. 제공된 최상위 속성 값은 사용하지 않습니다.

기존 검색 결과에 대해 Security Hub는 두 값을 모두 사용합니다. 하지만 BatchUpdateFindings에서 속성을 아직 업데이트하지 않은 경우에만 최상위 속성 값을 업데이트합니다.

에서 제공하는 batch-import-findings 명령 사용 AWS CLI

AWS Command Line Interface에서는 batch-import-findings명령을 사용하여 결과를 만들거나 업데이트합니다.

사용자는 각 결과를 JSON 객체로 입력합니다.

예

```
aws securityhub batch-import-findings --findings
    [{
        "AwsAccountId": "123456789012",
        "CreatedAt": "2019-08-07T17:05:54.832Z",
        "Description": "Vulnerability in a CloudTrail trail",
        "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0/rule/2.2",
        "Id": "Id1",
        "ProductArn": "arn:aws:securityhub:us-west-1:123456789012:product/123456789012/
default",
        "Resources": [
            {
                "Id": "arn:aws:cloudtrail:us-west-1:123456789012:trail/TrailName",
                "Partition": "aws",
                "Region": "us-west-1",
                "Type": "AwsCloudTrailTrail"
            }
        ],
        "SchemaVersion": "2018-10-08",
        "Title": "CloudTrail trail vulnerability",
        "UpdatedAt": "2020-06-02T16:05:54.832Z",
        "Types": [
            "Software and Configuration Checks/Vulnerabilities/CVE"
        ],
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "0"
        }
    }]'
```

결과를 업데이트하기 위한 BatchUpdateFindings 사용

이 BatchUpdateFindings 작업은 조사 결과 공급자의 조사 결과에 대한 고객의 처리와 관련된 정보를 업데이트하는 데 사용됩니다. 이는 고객이 사용할 수도 있고 또는 고객을 대신하여 작동하는 SIEM,

티켓팅, 인시던트 관리 또는 SOAR 도구에서 사용할 수 있습니다. 를 BatchUpdateFindings 사용하여 AWS 보안 검색 형식 (ASFF) 의 특정 필드를 업데이트할 수 있습니다.

새 조사 결과를 만드는 데는 BatchUpdateFindings을 사용할 수 없습니다. 한 번에 최대 100개의 조사 결과를 업데이트하는 데 사용할 수 있습니다.

Security Hub는 결과 업데이트 BatchUpdateFindings 요청을 받을 때마다 Amazon에서 자동으로 Security Hub Findings - Imported이벤트를 생성합니다 EventBridge. the section called “자동 응답 및 해결” 섹션을 참조하십시오.

BatchUpdateFindings검색 결과 UpdatedAt 필드를 변경하지 않습니다. UpdatedAt검색 제공자의 최신 업데이트만 반영합니다.

BatchUpdateFindings에 사용 가능한 필드

관리자 계정은 자체 계정이나 멤버 계정에 대한 조사 결과를 업데이트하는 데 >BatchUpdateFindings를 사용할 수 있습니다. 멤버 계정은 멤버 계정에 대한 조사 결과를 업데이트하는 데 >BatchUpdateFindings를 사용할 수 있습니다.

고객은 >BatchUpdateFindings만 사용하여 다음 필드와 객체를 업데이트할 수 있습니다.

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

기본적으로 관리자 및 멤버 계정은 위의 모든 필드와 필드 값에 액세스할 수 있습니다. 또한 Security Hub는 필드 및 필드 값에 대한 액세스를 제한할 수 있는 컨텍스트 키를 제공합니다.

예를 들어 멤버 계정만 Workflow.Status를 RESOLVED로 설정하도록 허용할 수 있습니다. 또는 멤버 계정을 Severity.Label로 변경하는 것을 허용하지 않을 수도 있습니다.

BatchUpdateFindings에 대한 액세스 구성

필드 및 필드 값을 업데이트하기 위해 BatchUpdateFindings을 사용하도록 액세스를 제한하도록 IAM 정책을 구성할 수 있습니다.

액세스를 BatchUpdateFindings로 제한하는 문에는 다음 값을 사용하십시오.

- Action는 securityhub:BatchUpdateFindings
- Effect는 Deny
- Condition의 경우, 다음을 기준으로 BatchUpdateFindings 요청을 거부할 수 있습니다.
  - 결과에 특정 필드가 포함됩니다.
  - 결과에 특정 필드 값이 포함됩니다.

조건 키

액세스를 BatchUpdateFindings로 제한하기 위한 조건 키입니다.

ASFF 필드

ASFF 필드의 조건 키는 다음과 같습니다.

```
securityhub:ASFFSyntaxPath/<fieldName>
```

*<fieldName>*를 ASFF 필드로 바꾸십시오. BatchUpdateFindings에 대한 액세스를 구성할 때는 상위 수준 필드 대신 IAM 정책에 하나 이상의 특정 ASFF 필드를 포함하십시오. 예를 들어 Workflow.Status 필드에 대한 액세스를 제한하려면 Workflow 상위 수준 필드 대신 정책에 securityhub:ASFFSyntaxPath/Workflow.Status을 포함해야 합니다.

필드에 대한 모든 업데이트 허용 안 함

사용자가 특정 필드를 업데이트하지 못하게 하려면 다음과 같은 조건을 사용하십시오.

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
                }
}
```

예를 들어 다음 문장은 워크플로 상태를 업데이트하는 데 BatchUpdateFindings를 사용할 수 없음을 나타냅니다.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

특정 필드 값 허용 안 함

사용자가 필드를 특정 값으로 설정하는 것을 방지하려면 다음과 같은 조건을 사용하십시오.

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
               }
}
```

예를 들어, 다음 명령문은 Workflow.Status을 SUPPRESSED로 설정하는 데 BatchUpdateFindings를 사용할 수 없음을 나타냅니다.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

허용되지 않는 값 목록을 입력할 수도 있습니다.

```
 "Condition": {
```

```
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

예를 들어, 다음 문은 `Workflow.Status`를 `RESOLVED` 또는 `SUPPRESSED` 중 하나로 설정하는 데 `BatchUpdateFindings`를 사용할 수 없음을 나타냅니다.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

의 batch-update-findings 명령 사용 AWS CLI

AWS Command Line Interface에서는 [batch-update-findings](#)명령을 사용하여 결과를 업데이트합니다.

업데이트할 각 결과에 대해 결과 ID와 결과를 생성한 제품의 ARN을 모두 입력합니다.

```
--finding-identifiers ID="<findingID1>",ProductArn="<productARN>"
 ID="<findingID2>",ProductArn="<productARN2>"
```

업데이트할 속성을 입력할 때는 JSON 형식 또는 바로가기 형식을 사용할 수 있습니다.

다음은 JSON 형식을 사용하는 `Note` 객체에 대한 업데이트의 예입니다.

```
--note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}'
```

다음은 바로가기 형식을 사용하는 것과 동일한 업데이트입니다.

```
--note Text="Known issue that is not a risk.",UpdatedBy="user1"
```

AWS CLI 명령 참조는 각 필드에 대한 JSON과 단축키 구문을 제공합니다.

다음 >batch-update-findings 예제는 두 가지 조사 결과를 업데이트하여 메모를 추가하고, 심각도 레이블을 변경하고, 문제를 해결합니다.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note '{"Text": "Known issue that is not a
 risk.", "UpdatedBy": "user1"}' --severity '{"Label": "LOW"}' --workflow '{"Status":
 "RESOLVED"}'
```

이는 동일한 예이지만 JSON 대신 바로가기를 사용합니다.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note Text="Known issue that is not a
 risk.",UpdatedBy="user1" --severity Label="LOW" --workflow Status="RESOLVED"
```

검색 결과 세부 정보 및 기록 관리 및 검토

AWS Security Hub 콘솔에서 검색 결과 목록을 보는 방법은 여러 가지가 있습니다.

- 결과 페이지 - 활성화된 모든 컨트롤 및 제품 통합에서 얻은 포괄적인 결과 목록을 표시합니다. 기본적으로 NEW 또는 NOTIFIED 워크플로 상태의 활성 검색 결과가 표시됩니다.
- 제어 세부 정보 페이지 - 특정 컨트롤에 대해 지난 24시간 동안 생성된 결과 목록을 표시합니다.
- 인사이트 페이지 - 일치하는 인사이트에 대한 검색 결과 목록을 표시합니다. 인사이트는 컬렉션별 검색 결과입니다. 자세한 정보는 the section called “인사이트 결과 및 조사 결과 보기”을 참조하세요.
- 통합 페이지 - 통합 AWS 서비스 또는 타사 제품에서 생성된 결과 목록을 표시합니다.

이러한 목록의 결과를 필터링하고 그룹화하여 특정 유형의 검색 결과에 초점을 맞출 수 있습니다. 이전 페이지에서 특정 결과를 선택하여 해당 결과에 대한 세부 정보를 볼 수도 있습니다.

검색 결과 목록을 프로그래밍 방식으로 보려면 Security Hub API의 `GetFindings`작업을 사용하십시오. 필터를 포함하여 특정 유형의 검색 결과를 검색할 수 있습니다.

지역 간 집계를 활성화하면 여러 지역의 통제 상태, 보안 점수, 통찰력 및 조사 결과를 검색할 수 있습니다. 집계 영역에서 데이터 찾기에는 집계 지역 및 연결 지역의 데이터가 포함됩니다. 다른 지역의 경우 데이터 검색은 해당 지역에만 해당됩니다. 지역 간 집계 구성에 대한 자세한 내용은 을 참조하십시오. 크로스 리전 집계 활성화

조사 결과 필터링 및 그룹화(콘솔)

Security Hub 콘솔의 조사 결과 페이지, 통합 페이지 또는 Insights 페이지에 결과 목록을 표시하면 레코드 상태 및 워크플로 상태를 기반으로 목록이 사전 필터링됩니다. 이는 인사이트 또는 통합을 위한 필터에 추가됩니다.

기록 상태는 검색 결과가 활성 상태인지 보관되었는지를 나타냅니다. 기본적으로 검색 결과 목록에는 활성 검색 결과만 표시됩니다. 검색 결과 제공자가 검색 결과를 보관할 수 있습니다. AWS Security Hub 또한 관련 리소스가 삭제되는 경우 제어 결과를 자동으로 보관합니다.

워크플로 상태는 결과에 대한 조사 상태를 나타냅니다. 기본적으로 조사 결과 목록에는 워크플로 상태가 `NEW` 또는 `NOTIFIED`인 조사 결과만 표시됩니다. 검색 결과의 워크플로 상태를 업데이트할 수 있습니다.

검색결과 집계를 활성화하고 집계 영역에 로그인한 경우 검색결과 및 인사이트 페이지에서 지역별로 검색결과를 필터링할 수 있습니다.

통제 결과 작업에 대한 자세한 내용은 을 참조하십시오. the section called “조사 결과 필터링 및 정렬” 이 페이지의 정보는 검색 결과, 인사이트 및 통합 페이지의 검색 결과 목록에 적용됩니다.

필터 추가

목록 범위를 변경하려면 필터를 추가할 수 있습니다.

최대 10개의 속성으로 필터링할 수 있습니다. 각 속성에 대해 최대 20개의 필터 값을 입력할 수 있습니다.

결과 목록을 필터링할 때 Security Hub는 필터 집합에 AND 논리를 적용합니다. 즉, 결과는 입력된 모든 필터와 일치해야 합니다. 예를 들어 제품 이름에 대한 GuardDuty 필터로 추가하고 리소스 유형에 대한 `AwsS3Bucket` 필터로 추가하는 경우 일치하는 결과가 이 두 기준과 일치해야 합니다.

그러나 Security Hub에서는 속성은 동일하지만 다른 값을 사용하는 필터에 OR 로직을 적용합니다. 예를 들어 둘 다 Amazon GuardDuty Inspector를 제품 이름의 필터 값으로 추가합니다. 이 경우 검색 결과가 둘 중 하나 GuardDuty 또는 Amazon Inspector에서 생성된 경우 일치하는 결과를 얻을 수 있습니다.

결과 목록에 필터를 추가하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 결과 목록을 표시하려면 다음 중 하나를 수행하십시오.
   - Security Hub 탐색 창에서 조사 결과를 선택합니다.
   - Security Hub 탐색 창에서 인사이트를 선택합니다. 인사이트를 선택합니다. 그런 다음 결과 목록에서 인사이트 결과를 선택합니다.
   - Security Hub 탐색 창에서 통합을 선택합니다. 통합에 대해 조사 결과 보기를 선택합니다.
3. 필터 추가 상자에서 필터에 대해 필터를 선택합니다.

   회사 이름 또는 제품 이름을 기준으로 필터링하는 경우 콘솔은 최상위 `CompanyName` 및 `ProductName` 필드를 사용합니다. API는 `ProductFields`에 있는 값을 사용합니다.
4. 필터 일치 유형을 선택합니다.

   문자열 필터의 경우 다음 비교 옵션 중에서 선택할 수 있습니다.

   - is - 필터 값과 정확히 일치하는 값을 찾습니다.
   - starts with - 필터 값으로 시작하는 값을 찾습니다.
   - is not - 필터 값과 일치하지 않는 값을 찾습니다.
   - does not start with - 필터 값으로 시작하지 않는 값을 찾습니다.

   숫자 필터의 경우 단일 숫자(단일) 또는 숫자 범위(범위) 중에서 어느 것을 입력할지 선택할 수 있습니다.

   날짜 또는 시간 필터의 경우 현재 날짜 시간(롤링 윈도우) 또는 날짜 범위(고정 범위) 중 어느 기간을 입력할지 선택할 수 있습니다.

   필터를 여러 개 추가하면 다음과 같은 상호 작용이 발생합니다.

   - is 및 with start 필터는 OR로 조인됩니다. 필터 값이 하나라도 포함되어 있으면 값이 일치합니다. 예를 들어 심각도 레이블을 중요로 지정하고 심각도 레이블을 높음으로 지정하면 결과에는 심각도 중요와 심각도 높음 조사 결과가 모두 포함됩니다.

- is not 및 does not start with 필터는 AND로 조인됩니다. 값은 해당 필터 값을 포함하지 않는 경우에만 일치합니다. 예를 들어 심각도 레이블을 낮음으로 지정하고 심각도 레이블을 보통이 아닌 경우 결과에는 심각도가 낮거나 중간 정도인 결과가 포함되지 않습니다.

필드에 is 필터가 있는 경우 동일한 필드에서 is not 또는 a가 필터로 시작되지 않도록 설정할 수 없습니다.

5. 필터 값을 지정합니다.

   문자열 필터의 경우 필터 값은 대소문자를 구분합니다.

   예를 들어, Security Hub 조사 결과의 경우 제품 이름은 Security Hub입니다. EQUALS 연산자를 사용하여 Security Hub의 조사 결과를 보는 경우 필터 값에 **`Security Hub`**를 입력해야 합니다. **`security hub`**를 입력하면 조사 결과가 표시되지 않습니다.

   마찬가지로 PREFIX 연산자를 사용하고 **`Sec`**를 입력하면 Security Hub 조사 결과가 표시됩니다. **`sec`**만 입력하면 Security Hub 조사 결과가 표시되지 않습니다.

6. 적용을 선택합니다.

조사 결과 그룹화

필터를 변경하는 것 외에도 선택한 속성의 값을 기준으로 조사 결과를 그룹화할 수 있습니다.

조사 결과를 그룹화하면 조사 결과 목록이 일치하는 조사 결과에서 선택한 속성의 값 목록으로 바뀝니다. 각 값의 경우 다른 필터 기준과 일치하는 조사 결과 수가 목록에 표시됩니다.

예를 들어 결과를 AWS 계정 ID별로 그룹화하면 각 계정의 일치하는 결과 수가 포함된 계정 식별자 목록이 표시됩니다.

참고로 Security Hub는 100개의 값만 표시할 수 있습니다. 그룹화 값이 100개를 초과하는 경우 처음 100개만 표시됩니다.

속성 값을 선택하면 해당 값과 일치하는 조사 결과 목록이 표시됩니다.

조사 결과 목록에서 조사 결과를 그룹화하려면

1. 결과 목록에서 필터 추가 상자를 선택합니다.
2. 그룹화에서 그룹화 기준을 선택합니다.
3. 목록에서 그룹화에 사용할 속성을 선택합니다.

4. 적용을 선택합니다.

필터 값 또는 그룹화 속성 변경

기존 필터의 경우 필터 값을 변경할 수 있습니다. 그룹화 속성을 변경할 수도 있습니다.

예를 들어, ARCHIVED 조사 결과 대신 ACTIVE 조사 결과를 찾도록 레코드 상태 필터를 변경할 수 있습니다.

필터 또는 그룹화 속성을 편집하려면

1. 필터링된 결과 목록에서 필터 또는 그룹화 속성을 선택합니다.
2. 그룹화 기준에서 새 속성을 선택한 다음 적용을 선택합니다.
3. 필터에서 새 값을 선택한 다음 적용을 선택합니다.

필터 또는 그룹화 속성 삭제

필터 또는 그룹화 속성을 삭제하려면 x 아이콘을 선택합니다.

목록이 자동으로 업데이트되어 변경 사항을 반영합니다. 그룹화 속성을 제거하면 목록이 필드 값 목록에서 조사 결과 목록으로 변경됩니다.

사용 가능한 검색 정보

Security Hub 콘솔에서 또는 Security Hub API의 GetFindings작업을 호출하여 다양한 결과 세부 정보를 얻을 수 있습니다. 다음은 얻을 수 있는 검색 결과 세부 정보 유형의 일부 목록입니다.

- 애플리케이션 메타데이터 — 애플리케이션을 생성하고 AWS 애플리케이션 태그를 추가했는지 확인하는 데 관련된 애플리케이션의 이름 및 Amazon Resource Name (ARN) 을 제공합니다. 에서 애플리케이션을 생성하는 것이 좋습니다. AWS Service Catalog AppRegistry
- 검색 기록 - 지난 90일 동안의 검색 기록을 제공합니다.
- Detective에서 조사 결과 검색 (콘솔만 해당) - 자동 로그 수집, 보안 분석 및 AWS 서비스 리소스 탐색 도구를 사용하여 Detective의 조사 결과를 자세히 조사할 수 있는 링크를 제공합니다. 이 정보는 Detective를 활성화한 AWS 서비스 경우 다른 사람으로부터 받은 Security Hub 검색 결과에만 포함됩니다.
- 공급자 검색 필드 - 신뢰도, 중요도, 관련 검색 결과, 심각도, 검색 결과 유형에 대한 검색 결과 제공자의 값을 표시합니다.

- 매개 변수 - 보안 제어의 현재 매개 변수 값을 표시합니다. Security Hub는 제어 기능의 보안 검사를 수행할 때 이러한 파라미터 값을 사용합니다.
- 수정 - 실패한 제어 결과를 수정하기 위한 지침으로 연결되는 링크를 제공합니다.
- 리소스 - 검색 결과와 관련된 AWS 리소스에 대한 정보를 제공합니다.
- 리소스 태그 - 검색 결과와 관련된 리소스의 태그 키 및 값 정보를 제공합니다. AWS Resource Groups Tagging API의 `GetResources` 작동으로 지원되는 리소스에 태그를 지정할 수 있습니다. Security Hub는 서비스 연결 역할을 통해 이 작업을 호출하고, AWS 보안 검색 결과 형식 (ASFF) `Resource.Id` 필드가 리소스 ARN으로 채워지면 리소스 태그를 검색합니다. AWS 잘못된 리소스 ID는 무시됩니다. 결과에 리소스 태그를 포함하는 방법에 대한 자세한 내용은 을 참조하십시오Tags.
- 유형 및 관련 검색 결과 - 검색 결과 유형에 대한 정보가 들어 있습니다.
- 취약성 세부 정보 — 발견 결과 및 영향을 받는 패키지에서 탐지된 취약성에 대한 정보입니다. Amazon Inspector가 Security Hub로 보내는 결과에 대해 Amazon Inspector를 활성화하면 이러한 세부 정보를 확인할 수 있습니다.

다음 섹션을 검토하여 이러한 세부 정보에 액세스하여 결과를 얻는 방법을 알아보십시오.

검색 결과 기록 검토

결과 기록은 지난 90일 동안 결과에 대한 변경 사항을 추적할 수 있는 Security Hub 기능입니다. 이는 활성 및 보관된 조사 결과에 사용할 수 있습니다. 결과 기록은 변경 내용, 발생 시기, 어떤 사용자에 의해 이루어졌는지를 포함하여 시간이 지남에 따라 결과에 적용된 변경 사항에 대한 불변의 추적을 제공합니다.

특히, AWS 보안 검색 형식 (ASFF) 필드의 변경 사항을 추적할 수 있습니다. Security Hub는 자동화 규칙을 사용하여 수동으로 수행한 변경 사항을 추적합니다.

검색 기록은 Security Hub 콘솔, API 및 에서 사용할 수 AWS CLI있습니다.

Security Hub 관리자 계정으로 로그인한 경우 관리자 계정 및 모든 구성원 계정의 검색 기록을 가져올 수 있습니다.

원하는 방법을 선택하고 단계에 따라 검색 기록을 검토하십시오.

Security Hub console

검색 기록 검토

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

2. 왼쪽 탐색 창에서 조사 결과를 선택합니다.
3. 결과를 선택합니다. 표시되는 패널에서 기록 탭을 선택합니다.

Security Hub API

검색 기록 검토

1. 명령을 GetFindings실행하거나 를 AWS CLI사용하는 경우 get-findings명령을 실행합니다. 필요에 따라 적절한 필터를 사용하여 기록을 보려는 결과를 식별합니다. API 응답은 결과에 대한 `ProductArn` 및 `Id`를 제공합니다. 세 번째 단계에서 이러한 필드의 값이 필요합니다.
2. 명령을 GetFindingHistory실행하거나 를 AWS CLI사용하는 경우 get-finding-history명령을 실행합니다.
3. `ProductArn` 및 `Id` 필드를 사용하여 기록을 가져오려는 결과를 식별합니다. 필드에 대한 자세한 내용은 AwsSecurityFindingIdentifier 섹션을 참조하세요. 요청당 하나의 결과에 대한 기록만 가져올 수 있습니다.
4. `StartTime`. 에 대한 값을 `EndTime` 입력하고 검색 기록을 특정 기간으로 제한하십시오.
5. 결과 기록을 특정 수의 결과로 제한하려면 `MaxResults`에 값을 입력하십시오. 입력하지 않을 경우 API 응답은 검색 기록의 첫 100개 결과를 반환합니다.
6. 결과에 대한 다음 100개의 결과(해당하는 경우)를 보려면 `NextToken`에 값을 입력하십시오. 초기 API 요청에서 `NextToken`의 값은 `NULL`여야 합니다.

다음 CLI 명령은 지정된 검색 결과에 대한 기록을 검색합니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

검색 결과 세부 정보 검토

원하는 방법을 선택하고 단계에 따라 Security Hub에서 검색 결과 세부 정보를 확인하십시오.

Security Hub console

검색 결과 세부 정보 검토

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 검색 결과 목록을 표시하려면 다음 조치 중 하나를 수행하십시오.
   - Security Hub 탐색 창에서 조사 결과를 선택합니다. 필요에 따라 검색 필터를 추가하여 검색 결과 목록의 범위를 좁힐 수 있습니다.
   - Security Hub 탐색 창에서 인사이트를 선택합니다. 인사이트를 선택합니다. 그런 다음 결과 목록에서 인사이트 결과를 선택합니다.
   - Security Hub 탐색 창에서 통합을 선택합니다. 통합에 대해 조사 결과 보기를 선택합니다.
3. 결과 제목을 선택합니다.
4. 검색 결과 세부 정보 패널에서 다음과 같이 추가 조치를 취할 수 있습니다.
   - 결과에 대한 전체 JSON을 표시하려면 결과 ID를 선택합니다. JSON 찾기에서 검색 JSON을 다운로드하십시오.
   - AWS Config 규칙을 기반으로 한 검색 결과를 보려면 해당 규칙 목록을 표시하려면 규칙을 선택합니다.
   - Macie 콘솔의 검색 결과에서 발견된 민감한 데이터를 조사하려면 Macie와 함께 조사를 선택하십시오. 이 옵션은 Amazon Macie와 민감한 데이터 자동 검색 기능을 활성화한 경우에만 사용할 수 있습니다.
   - 검색과 관련된 리소스에 대한 정보를 보려면 [리소스] 를 선택합니다.
   - Detective 콘솔에서 검색 결과를 조사하려면 Amazon Detective에서 조사를 선택하십시오. 이 옵션은 Amazon Detective를 활성화한 경우에만 사용할 수 있습니다.
   - 기록 탭을 선택하면 최대 90일간의 검색 기록을 볼 수 있습니다.

> **Note**
>
> 결과 세부 정보 패널 상단에는 계정, 심각도, 날짜, 상태 등 결과에 대한 개요 정보가 표시됩니다. AWS Organizations 통합하고 로그인한 계정이 기관 구성원 계정인 경우 세부 정보 패널에 계정 이름이 포함됩니다. Organizations 통합을 통하지 않고 수동으로 초대된 구성원 계정의 경우 세부 정보 패널에 계정 ID만 포함됩니다.

Security Hub API

검색 결과 세부 정보 검토

Security Hub API의 `GetFindings`작업을 사용하거나 를 사용하는 경우 get-find 명령을 실행하십시오. AWS CLI

`Filters`매개 변수에 하나 이상의 값을 제공하여 검색하려는 검색 결과의 범위를 좁힐 수 있습니다.

결과 양이 너무 많으면 매개 변수를 사용하여 검색 결과를 지정된 수로 제한하고 `MaxResults` 매개 변수를 사용하여 검색 결과를 페이지별로 `NextToken` 나눌 수 있습니다. `SortCriteria`매개 변수를 사용하여 검색 결과를 특정 필드를 기준으로 정렬할 수 있습니다.

지역 간 집계를 활성화하고 집계 지역에서 이 작업을 호출한 경우 집계 및 연결 지역의 검색 결과가 결과에 포함됩니다.

다음 CLI 명령은 제공된 필터와 일치하는 결과를 검색하고 필드의 내림차순으로 정렬합니다. `LastObservedAt` 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

PowerShell

검색 결과 세부 정보 검토

1. `Get-SHUBFinding` cmdlet을 사용하십시오.
2. 선택적으로 `Filter` 파라미터를 채워 검색하려는 조사 결과의 범위를 좁힙니다.

예

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> CompanyName또는 ProductName 를 기준으로 검색 결과를 필터링하면 Security Hub 는 ProductFields ASFF 개체의 일부인 값을 사용합니다. Security Hub는 최상위 수준 CompanyName 및 ProductName 필드를 사용하지 않습니다.

조사 결과에 대한 조치 취하기 AWS Security Hub

AWS Security Hub 결과에 대한 조사의 현재 상태를 추적할 수 있습니다.

조사 결과를 사용자 지정 작업에 전송하여 처리할 수도 있습니다.

주제

조사 결과에 대한 워크플로 상태 설정

워크플로 상태는 결과에 대한 조사 진행 상황을 추적합니다. 워크플로 상태는 개별 결과에 따라 다릅니다. 새로운 조사 결과 생성에는 영향을 주지 않습니다. 예를 들어, 검색 결과의 워크플로 상태를 SUPPRESSED 설정하거나 설정해도 동일한 문제에 대해 새 검색 결과가 생성되는 AWS Security Hub 것을 막지는 RESOLVED 못합니다.

워크플로 상태는 다음 값이 있을 수 있습니다.

NEW

검토하기 전 결과의 초기 상태입니다.

AWS 서비스통합에서 수집된 결과 (예:) 는 초기 상태로 유지됩니다. AWS ConfigNEW

또한 Security Hub는 다음과 같은 경우 워크플로 상태를 NOTIFIED 또는 RESOLVED에서 NEW로 재설정합니다.

- RecordState는 ARCHIVED에서 ACTIVE로 바뀝니다.
- Compliance.Status는 PASSED에서 FAILED, WARNING 또는 NOT_AVAILABLE로 바뀝니다.

이러한 변경은 추가 조사가 필요하다는 것을 의미합니다.

NOTIFIED

리소스 소유자에게 보안 문제에 대해 통지했음을 나타냅니다. 리소스 소유자가 아닌 경우 이 상태를 사용할 수 있으며 보안 문제를 해결하기 위해 리소스 소유자의 개입이 필요합니다.

다음 중 하나가 발생하면 워크플로우 상태가 자동으로 NOTIFIED에서 NEW로 변경됩니다.

- RecordState는 ARCHIVED에서 ACTIVE로 바뀝니다.
- Compliance.Status는 PASSED에서 FAILED, WARNING 또는 NOT_AVAILABLE로 바뀝니다.

SUPPRESSED

결과를 검토한 결과 조치가 필요하지 않다고 생각함을 나타냅니다.

RecordState가 ARCHIVED에서 ACTIVE으로 변경되더라도 SUPPRESSED 결과의 워크플로 상태는 변경되지 않습니다.

RESOLVED

결과가 검토 및 수정되었으며 이제 해결된 것으로 간주됩니다.

다음 중 하나가 발생하지 않는 한 결과는 RESOLVED로 유지됩니다.

- RecordState는 ARCHIVED에서 ACTIVE로 바뀝니다.
- Compliance.Status는 PASSED에서 FAILED, WARNING 또는 NOT_AVAILABLE로 바뀝니다.

이 경우 워크플로 상태는 자동으로 NEW로 재설정됩니다.

제어 조사 결과의 경우, Compliance.Status이 PASSED이면 Security Hub는 자동으로 워크플로 상태를 RESOLVED로 설정합니다.

조사 결과에 대한 워크플로 상태 설정

원하는 방법을 선택하고 단계에 따라 하나 이상의 조사 결과에 대한 워크플로 상태를 설정합니다.

특정 조사 결과의 워크플로 상태를 자동으로 업데이트하려면 자동화 규칙을 참조하십시오.

Security Hub console

조사 결과의 워크플로 상태 설정

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 결과 목록을 표시하려면 다음 중 하나를 수행하십시오.

- Security Hub 탐색 창에서 조사 결과를 선택합니다.
- Security Hub 탐색 창에서 인사이트를 선택합니다. 인사이트를 선택합니다. 그런 다음 결과 목록에서 인사이트 결과를 선택합니다.
- Security Hub 탐색 창에서 통합을 선택합니다. 통합에 대해 조사 결과 보기를 선택합니다.
- Security Hub 탐색 창에서 보안 표준을 선택합니다. 결과 보기를 선택하여 제어 목록을 표시합니다. 그런 다음 제어를 선택하고 해당 제어에 대한 조사 결과 목록을 확인합니다.

3. 결과 목록에서 업데이트할 각 결과의 확인란을 선택합니다.
4. 목록 상단의 워크플로 상태에서 상태를 선택합니다.
5. 워크플로 상태 설정 대화 상자에서 워크플로 상태를 업데이트하는 이유를 자세히 설명하는 선택적 메모를 제공합니다. 상태 설정을 선택합니다.

Security Hub API

BatchUpdateFindings API를 호출합니다. 결과 ID와 결과를 생성한 제품의 ARN을 모두 입력합니다. GetFindings API를 호출하여 이러한 세부 정보를 얻을 수 있습니다.

AWS CLI

batch-update-findings 명령을 실행합니다. 결과 ID와 결과를 생성한 제품의 ARN을 모두 입력합니다. get-findings 명령을 실행하여 이 세부 정보를 가져올 수 있습니다.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

예

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

사용자 지정 작업에 조사 결과 전송

Amazon에서 Security Hub를 자동화하는 AWS Security Hub 사용자 지정 작업을 생성할 수 EventBridge 있습니다. 사용자 지정 작업의 경우 이벤트 유형은 Security Hub Findings - Custom Action입니다.

사용자 지정 작업을 만드는 방법에 대한 자세한 내용과 단계는 the section called “자동 응답 및 해결”을 참조하십시오.

사용자 지정 작업을 설정한 후 조사 결과를 해당 작업에 전송할 수 있습니다.

조사 결과를 사용자 지정 작업으로 전송하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 결과 목록을 표시하려면 다음 중 하나를 수행하십시오.
   - Security Hub 탐색 창에서 조사 결과를 선택합니다.
   - Security Hub 탐색 창에서 인사이트를 선택합니다. 인사이트를 선택합니다. 그런 다음 결과 목록에서 인사이트 결과를 선택합니다.
   - Security Hub 탐색 창에서 통합을 선택합니다. 통합에 대해 조사 결과 보기를 선택합니다.
   - Security Hub 탐색 창에서 보안 표준을 선택합니다. 결과 보기를 선택하여 제어 목록을 표시합니다. 그런 다음 제어 이름을 선택합니다.
3. 결과 목록에서 사용자 지정 작업으로 전송할 각 결과의 확인란을 선택합니다.

   조사 결과를 한 번에 최대 20개까지 선택할 수 있습니다.
4. 작업에서 사용자 지정 작업을 선택합니다.

AWS 보안 검색 형식 (ASFF)

AWS Security Hub는 AWS 보안 서비스 및 타사 제품 통합에서 얻은 결과를 사용, 집계, 구성 및 우선 순위를 지정합니다. Security Hub는 보안 검색 결과 형식 (ASFF) 이라는 표준 검색 결과 형식을 사용하여 이러한 결과를 처리하므로 시간이 많이 걸리는 데이터 변환 작업이 필요하지 않습니다. AWS 그러면 가장 중요한 제품에 우선 순위를 부여하기 위해 제품 전반에 걸쳐 수집된 조사 결과를 상호 연관시킵니다.

주제

- AWS 보안 탐지 형식 (ASFF) 구문
- ASFF 필드 및 값에 대한 통합의 영향
- ASFF 예제

AWS 보안 탐지 형식 (ASFF) 구문

이 페이지는 AWS 보안 탐지 형식 (ASFF) 검색 결과에 대한 JSON의 전체 개요를 제공합니다. 형식은 JSON 스키마에서 파생됩니다. 연결된 객체 이름을 선택하면 해당 객체에 대한 예제 결과를 볼 수 있습니다. Security Hub 조사 결과를 여기에 표시된 리소스 및 예시와 비교하여 조사 결과를 해석하는 데 도움을 받을 수 있습니다.

필수 ASFF 속성에 대한 설명을 보려면 the section called “필수 최상위 속성”을 참조하십시오.

다른 최상위 ASFF 속성에 대한 설명을 보려면 the section called “선택적 최상위 속성”을 참조하십시오.

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
       "CallerType": "string",
       "DomainDetails": {
        "Domain": "string"
       },
       "FirstSeen": "string",
       "LastSeen": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
```

```
          "Isp": "string",
          "Org": "string"
         }
        },
        "ServiceName": "string"
       },
       "DnsRequestAction": {
        "Blocked": boolean,
        "Domain": "string",
        "Protocol": "string"
       },
       "NetworkConnectionAction": {
        "Blocked": boolean,
        "ConnectionDirection": "string",
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "Protocol": "string",
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "IpAddressV4": "string",
         "Geolocation": {
          "Lat": number,
          "Lon": number
         },
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        },
        "RemotePortDetails": {
         "Port": number,
         "PortName": "string"
        }
       },
```

```
      "PortProbeAction": {
       "Blocked": boolean,
       "PortProbeDetails": [{
        "LocalIpDetails": {
         "IpAddressV4": "string"
        },
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "GeoLocation": {
          "Lat": number,
          "Lon": number
         },
         "IpAddressV4": "string",
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        }
       }]
      }
     },
     "AwsAccountId": "string",
     "AwsAccountName": "string",
     "CompanyName": "string",
     "Compliance": {
      "AssociatedStandards": [{
       "StandardsId": "string"
      }],
      "RelatedRequirements": ["string"],
      "SecurityControlId": "string",
      "SecurityControlParameters": [
       {
```

```
        "Name": "string",
        "Value": ["string"]
       }
     ],
      "Status": "string",
      "StatusReasons": [
       {
        "Description": "string",
        "ReasonCode": "string"
       }
      ]
     },
     "Confidence": number,
     "CreatedAt": "string",
     "Criticality": number,
     "Description": "string",
     "FindingProviderFields": {
      "Confidence": number,
      "Criticality": number,
      "RelatedFindings": [{
       "ProductArn": "string",
       "Id": "string"
      }],
      "Severity": {
       "Label": "string",
       "Normalized": number,
       "Original": "string"
      },
      "Types": ["string"]
     },
     "FirstObservedAt": "string",
     "GeneratorId": "string",
     "Id": "string",
     "LastObservedAt": "string",
     "Malware": [{
      "Name": "string",
      "Path": "string",
      "State": "string",
      "Type": "string"
     }],
     "Network": {
      "DestinationDomain": "string",
      "DestinationIpV4": "string",
      "DestinationIpV6": "string",
```

```
      "DestinationPort": number,
      "Direction": "string",
      "OpenPortRange": {
       "Begin": integer,
       "End": integer
      },
      "Protocol": "string",
      "SourceDomain": "string",
      "SourceIpV4": "string",
      "SourceIpV6": "string",
      "SourceMac": "string",
      "SourcePort": number
     },
     "NetworkPath": [{
      "ComponentId": "string",
      "ComponentType": "string",
      "Egress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      },
      "Ingress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
```

```
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      }
     }],
     "Note": {
      "Text": "string",
      "UpdatedAt": "string",
      "UpdatedBy": "string"
     },
     "PatchSummary": {
      "FailedCount": number,
      "Id": "string",
      "InstalledCount": number,
      "InstalledOtherCount": number,
      "InstalledPendingReboot": number,
      "InstalledRejectedCount": number,
      "MissingCount": number,
      "Operation": "string",
      "OperationEndTime": "string",
      "OperationStartTime": "string",
      "RebootOption": "string"
     },
     "Process": {
      "LaunchedAt": "string",
      "Name": "string",
      "ParentPid": number,
      "Path": "string",
      "Pid": number,
      "TerminatedAt": "string"
     },
     "ProductArn": "string",
     "ProductFields": {
      "string": "string"
     },
     "ProductName": "string",
     "RecordState": "string",
     "Region": "string",
     "RelatedFindings": [{
      "Id": "string",
      "ProductArn": "string"
     }],
```

```
    "Remediation": {
     "Recommendation": {
      "Text": "string",
      "Url": "string"
     }
    },
    "Resources": [{
     "ApplicationArn": "string",
     "ApplicationName": "string",
     "DataClassification": {
      "DetailedResultsLocation": "string",
      "Result": {
       "AdditionalOccurrences": boolean,
       "CustomDataIdentifiers": {
        "Detections": [{
         "Arn": "string",
         "Count": integer,
         "Name": "string",
         "Occurrences": {
          "Cells": [{
           "CellReference": "string",
           "Column": integer,
           "ColumnName": "string",
           "Row": integer
          }],
          "LineRanges": [{
           "End": integer,
           "Start": integer,
           "StartColumn": integer
          }],
          "OffsetRanges": [{
           "End": integer,
           "Start": integer,
           "StartColumn": integer
          }],
          "Pages": [{
           "LineRange": {
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           },
           "OffsetRange": {
            "End": integer,
            "Start": integer,
```

```
            "StartColumn": integer
           },
           "PageNumber": integer
          }],
          "Records": [{
           "JsonPath": "string",
           "RecordIndex": integer
          }]
         }
        }],
        "TotalCount": integer
       },
       "MimeType": "string",
       "SensitiveData": [{
        "Category": "string",
        "Detections": [{
         "Count": integer,
         "Occurrences": {
          "Cells": [{
           "CellReference": "string",
           "Column": integer,
           "ColumnName": "string",
           "Row": integer
          }],
          "LineRanges": [{
           "End": integer,
           "Start": integer,
           "StartColumn": integer
          }],
          "OffsetRanges": [{
           "End": integer,
           "Start": integer,
           "StartColumn": integer
          }],
          "Pages": [{
           "LineRange": {
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           },
           "OffsetRange": {
            "End": integer,
            "Start": integer,
            "StartColumn": integer
```

```
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
        }
       }
      },
      "Details": {
       "AwsAmazonMQBroker": {
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
         "Id": "string",
         "Revision": integer
        },
        "DeploymentMode": "string",
        "EncryptionOptions": {
         "UseAwsOwnedKey": boolean
        },
        "EngineType": "string",
        "EngineVersion": "string",
        "HostInstanceType": "string",
        "Logs": {
         "Audit": boolean,
         "AuditLogGroup": "string",
         "General": boolean,
         "GeneralLogGroup": "string"
        },
        "MaintenanceWindowStartTime": {
         "DayOfWeek": "string",
```

```
          "TimeOfDay": "string",
          "TimeZone": "string"
         },
         "PubliclyAccessible": boolean,
         "SecurityGroups": [
          "string"
         ],
         "StorageType": "string",
         "SubnetIds": [
          "string",
          "string"
         ],
         "Users": [{
          "Username": "string"
         }]
        },
        "AwsApiGatewayRestApi": {
         "ApiKeySource": "string",
         "BinaryMediaTypes": [" string"],
         "CreatedDate": "string",
         "Description": "string",
         "EndpointConfiguration": {
          "Types": ["string"]
         },
         "Id": "string",
         "MinimumCompressionSize": number,
         "Name": "string",
         "Version": "string"
        },
        "AwsApiGatewayStage": {
         "AccessLogSettings": {
          "DestinationArn": "string",
          "Format": "string"
         },
         "CacheClusterEnabled": boolean,
         "CacheClusterSize": "string",
         "CacheClusterStatus": "string",
         "CanarySettings": {
          "DeploymentId": "string",
          "PercentTraffic": number,
          "StageVariableOverrides": [{
           "string": "string"
          }],
          "UseStageCache": boolean
```

```
        },
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DeploymentId": "string",
        "Description": "string",
        "DocumentationVersion": "string",
        "LastUpdatedDate": "string",
        "MethodSettings": [{
         "CacheDataEncrypted": boolean,
         "CachingEnabled": boolean,
         "CacheTtlInSeconds": number,
         "DataTraceEnabled": boolean,
         "HttpMethod": "string",
         "LoggingLevel": "string",
         "MetricsEnabled": boolean,
         "RequireAuthorizationForCacheControl": boolean,
         "ResourcePath": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number,
         "UnauthorizedCacheControlHeaderStrategy": "string"
        }],
        "StageName": "string",
        "TracingEnabled": boolean,
        "Variables": {
         "string": "string"
        },
        "WebAclArn": "string"
       },
       "AwsApiGatewayV2Api": {
        "ApiEndpoint": "string",
        "ApiId": "string",
        "ApiKeySelectionExpression": "string",
        "CorsConfiguration": {
         "AllowCredentials": boolean,
         "AllowHeaders": ["string"],
         "AllowMethods": ["string"],
         "AllowOrigins": ["string"],
         "ExposeHeaders": ["string"],
         "MaxAge": number
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
```

```
        "RouteSelectionExpression": "string",
        "Version": "string"
       },
       "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "ApiGatewayManaged": boolean,
        "AutoDeploy": boolean,
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DefaultRouteSettings": {
         "DataTraceEnabled": boolean,
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "DeploymentId": "string",
        "Description": "string",
        "LastDeploymentStatusMessage": "string",
        "LastUpdatedDate": "string",
        "RouteSettings": {
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "DataTraceEnabled": boolean,
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "StageName": "string",
        "StageVariables": [{
         "string": "string"
        }]
       },
       "AwsAppSyncGraphQLApi": {
        "AwsAppSyncGraphQlApi": {
         "AdditionalAuthenticationProviders": [
         {
          "AuthenticationType": "string",
          "LambdaAuthorizerConfig": {
           "AuthorizerResultTtlInSeconds": integer,
           "AuthorizerUri": "string"
          }
```

```
        },
        {
         "AuthenticationType": "string"
        }
        ],
        "ApiId": "string",
        "Arn": "string",
        "AuthenticationType": "string",
        "Id": "string",
        "LogConfig": {
         "CloudWatchLogsRoleArn": "string",
         "ExcludeVerboseContent": boolean,
         "FieldLogLevel": "string"
        },
        "Name": "string",
        "XrayEnabled": boolean
       }
      },
      "AwsAthenaWorkGroup": {
       "Description": "string",
       "Name": "string",
       "WorkgroupConfiguration": {
        "ResultConfiguration": {
         "EncryptionConfiguration": {
          "EncryptionOption": "string",
          "KmsKey": "string"
         }
        }
       },
       "State": "string"
      },
      "AwsAutoScalingAutoScalingGroup": {
       "AvailabilityZones": [{
        "Value": "string"
       }],
       "CreatedTime": "string",
       "HealthCheckGracePeriod": integer,
       "HealthCheckType": "string",
       "LaunchConfigurationName": "string",
       "LoadBalancerNames": ["string"],
       "LaunchTemplate": {
                      "LaunchTemplateId": "string",
                      "LaunchTemplateName": "string",
                      "Version": "string"
```

```
                },
        "MixedInstancesPolicy": {
         "InstancesDistribution": {
          "OnDemandAllocationStrategy": "string",
          "OnDemandBaseCapacity": number,
          "OnDemandPercentageAboveBaseCapacity": number,
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
           "LaunchTemplateId": "string",
           "LaunchTemplateName": "string",
           "Version": "string"
          },
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
          }]
         }
        }
       },
       "AwsAutoScalingLaunchConfiguration": {
        "AssociatePublicIpAddress": boolean,
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteOnTermination": boolean,
          "Encrypted": boolean,
          "Iops": number,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         },
         "NoDevice": boolean,
         "VirtualName": "string"
        }],
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
```

```
        },
        "ImageId": "string",
        "InstanceMonitoring": {
         "Enabled": boolean
        },
        "InstanceType": "string",
        "KernelId": "string",
        "KeyName": "string",
        "LaunchConfigurationName": "string",
        "MetadataOptions": {
         "HttpEndPoint": "string",
         "HttpPutReponseHopLimit": number,
         "HttpTokens": "string"
        },
        "PlacementTenancy": "string",
        "RamdiskId": "string",
        "SecurityGroups": ["string"],
        "SpotPrice": "string",
        "UserData": "string"
       },
       "AwsBackupBackupPlan": {
        "BackupPlan": {
         "AdvancedBackupSettings": [{
          "BackupOptions": {
           "WindowsVSS":"string"
          },
          "ResourceType":"string"
         }],
         "BackupPlanName": "string",
         "BackupPlanRule": [{
          "CompletionWindowMinutes": integer,
          "CopyActions": [{
           "DestinationBackupVaultArn": "string",
           "Lifecycle": {
            "DeleteAfterDays": integer,
            "MoveToColdStorageAfterDays": integer
           }
          }],
          "Lifecycle": {
           "DeleteAfterDays": integer
          },
          "RuleName": "string",
          "ScheduleExpression": "string",
          "StartWindowMinutes": integer,
```

```
          "TargetBackupVault": "string"
         }]
        },
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "VersionId": "string"
      },
       "AwsBackupBackupVault": {
        "AccessPolicy": {
         "Statement": [{
          "Action": ["string"],
          "Effect": "string",
          "Principal": {
           "AWS": "string"
          },
          "Resource": "string"
         }],
         "Version": "string"
        },
        "BackupVaultArn": "string",
        "BackupVaultName": "string",
        "EncryptionKeyArn": "string",
        "Notifications": {
         "BackupVaultEvents": ["string"],
         "SNSTopicArn": "string"
        }
       },
       "AwsBackupRecoveryPoint": {
        "BackupSizeInBytes": integer,
        "BackupVaultName": "string",
        "BackupVaultArn": "string",
        "CalculatedLifecycle": {
         "DeleteAt": "string",
         "MoveToColdStorageAt": "string"
        },
        "CompletionDate": "string",
        "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
        },
        "CreationDate": "string",
        "EncryptionKeyArn": "string",
```

```
        "IamRoleArn": "string",
        "IsEncrypted": boolean,
        "LastRestoreTime": "string",
        "Lifecycle": {
         "DeleteAfterDays": integer,
         "MoveToColdStorageAfterDays": integer
        },
        "RecoveryPointArn": "string",
        "ResourceArn": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "Status": "string",
        "StatusMessage": "string",
        "StorageClass": "string"
       },
       "AwsCertificateManagerCertificate": {
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
         "DomainName": "string",
         "ResourceRecord": {
          "Name": "string",
          "Type": "string",
          "Value": "string"
         },
         "ValidationDomain": "string",
         "ValidationEmails": ["string"],
         "ValidationMethod": "string",
         "ValidationStatus": "string"
        }],
        "ExtendedKeyUsages": [{
         "Name": "string",
         "OId": "string"
        }],
        "FailureReason": "string",
        "ImportedAt": "string",
        "InUseBy": ["string"],
        "IssuedAt": "string",
        "Issuer": "string",
        "KeyAlgorithm": "string",
        "KeyUsages": [{
         "Name": "string"
        }],
```

```
        "NotAfter": "string",
        "NotBefore": "string",
        "Options": {
         "CertificateTransparencyLoggingPreference": "string"
        },
        "RenewalEligibility": "string",
        "RenewalSummary": {
         "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
           "Name": "string",
           "Type": "string",
           "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
          "ValidationMethod": "string",
          "ValidationStatus": "string"
         }],
         "RenewalStatus": "string",
         "RenewalStatusReason": "string",
         "UpdatedAt": "string"
        },
        "Serial": "string",
        "SignatureAlgorithm": "string",
        "Status": "string",
        "Subject": "string",
        "SubjectAlternativeNames": ["string"],
        "Type": "string"
       },
       "AwsCloudFormationStack": {
        "Capabilities": ["string"],
        "CreationTime": "string",
        "Description": "string",
        "DisableRollback": boolean,
        "DriftInformation": {
         "StackDriftStatus": "string"
        },
        "EnableTerminationProtection": boolean,
        "LastUpdatedTime": "string",
        "NotificationArns": ["string"],
        "Outputs": [{
         "Description": "string",
         "OutputKey": "string",
```

```
        "OutputValue": "string"
       }],
       "RoleArn": "string",
       "StackId": "string",
       "StackName": "string",
       "StackStatus": "string",
       "StackStatusReason": "string",
       "TimeoutInMinutes": number
      },
      "AwsCloudFrontDistribution": {
       "CacheBehaviors": {
        "Items": [{
         "ViewerProtocolPolicy": "string"
        }]
       },
       "DefaultCacheBehavior": {
        "ViewerProtocolPolicy": "string"
       },
       "DefaultRootObject": "string",
       "DomainName": "string",
       "Etag": "string",
       "LastModifiedTime": "string",
       "Logging": {
        "Bucket": "string",
        "Enabled": boolean,
        "IncludeCookies": boolean,
        "Prefix": "string"
       },
       "OriginGroups": {
        "Items": [{
         "FailoverCriteria": {
          "StatusCodes": {
           "Items": [number],
           "Quantity": number
          }
         }
        }]
       },
       "Origins": {
        "Items": [{
         "CustomOriginConfig": {
          "HttpPort": number,
          "HttpsPort": number,
          "OriginKeepaliveTimeout": number,
```

```
          "OriginProtocolPolicy": "string",
          "OriginReadTimeout": number,
          "OriginSslProtocols": {
           "Items": ["string"],
           "Quantity": number
          }
         },
         "DomainName": "string",
         "Id": "string",
         "OriginPath": "string",
         "S3OriginConfig": {
          "OriginAccessIdentity": "string"
         }
        }]
       },
       "Status": "string",
       "ViewerCertificate": {
        "AcmCertificateArn": "string",
        "Certificate": "string",
        "CertificateSource": "string",
        "CloudFrontDefaultCertificate": boolean,
        "IamCertificateId": "string",
        "MinimumProtocolVersion": "string",
        "SslSupportMethod": "string"
       },
       "WebAclId": "string"
      },
      "AwsCloudTrailTrail": {
       "CloudWatchLogsLogGroupArn": "string",
       "CloudWatchLogsRoleArn": "string",
       "HasCustomEventSelectors": boolean,
       "HomeRegion": "string",
       "IncludeGlobalServiceEvents": boolean,
       "IsMultiRegionTrail": boolean,
       "IsOrganizationTrail": boolean,
       "KmsKeyId": "string",
       "LogFileValidationEnabled": boolean,
       "Name": "string",
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "SnsTopicArn": "string",
       "SnsTopicName": "string",
       "TrailArn": "string"
      },
```

```
      "AwsCloudWatchAlarm": {
       "ActionsEnabled": boolean,
       "AlarmActions": ["string"],
       "AlarmArn": "string",
       "AlarmConfigurationUpdatedTimestamp": "string",
       "AlarmDescription": "string",
       "AlarmName": "string",
       "ComparisonOperator": "string",
       "DatapointsToAlarm": number,
       "Dimensions": [{
        "Name": "string",
        "Value": "string"
       }],
       "EvaluateLowSampleCountPercentile": "string",
       "EvaluationPeriods": number,
       "ExtendedStatistic": "string",
       "InsufficientDataActions": ["string"],
       "MetricName": "string",
       "Namespace": "string",
       "OkActions": ["string"],
       "Period": number,
       "Statistic": "string",
       "Threshold": number,
       "ThresholdMetricId": "string",
       "TreatMissingData": "string",
       "Unit": "string"
      },
      "AwsCodeBuildProject": {
       "Artifacts": [{
        "ArtifactIdentifier": "string",
        "EncryptionDisabled": boolean,
        "Location": "string",
        "Name": "string",
        "NamespaceType": "string",
        "OverrideArtifactName": boolean,
        "Packaging": "string",
        "Path": "string",
        "Type": "string"
       }],
       "SecondaryArtifacts": [{
                   "ArtifactIdentifier": "string",
                   "Type": "string",
                   "Location": "string",
                   "Name": "string",
```

```
                "NamespaceType": "string",
                "Packaging": "string",
                "Path": "string",
                "EncryptionDisabled": boolean,
                "OverrideArtifactName": boolean
            }],
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
         "Certificate": "string",
         "EnvironmentVariables": [{
          "Name": "string",
          "Type": "string",
          "Value": "string"
         }],
         "ImagePullCredentialsType": "string",
         "PrivilegedMode": boolean,
         "RegistryCredential": {
          "Credential": "string",
          "CredentialProvider": "string"
         },
         "Type": "string"
        },
        "LogsConfig": {
         "CloudWatchLogs": {
          "GroupName": "string",
          "Status": "string",
          "StreamName": "string"
         },
         "S3Logs": {
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Status": "string"
         }
        },
        "Name": "string",
        "ServiceRole": "string",
        "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
        },
        "VpcConfig": {
         "VpcId": "string",
```

```
          "Subnets": ["string"],
          "SecurityGroupIds": ["string"]
        }
      },
      "AwsDmsEndpoint": {
        "CertificateArn": "string",
        "DatabaseName": "string",
        "EndpointArn": "string",
        "EndpointIdentifier": "string",
        "EndpointType": "string",
        "EngineName": "string",
        "KmsKeyId": "string",
        "Port": integer,
        "ServerName": "string",
        "SslMode": "string",
        "Username": "string"
      },
      "AwsDmsReplicationInstance": {
        "AllocatedStorage": integer,
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "EngineVersion": "string",
        "KmsKeyId": "string",
        "MultiAZ": boolean,
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ReplicationInstanceClass": "string",
        "ReplicationInstanceIdentifier": "string",
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "string"
        },
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "string"
            }
        ]
      },
      "AwsDmsReplicationTask": {
        "CdcStartPosition": "string",
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
```

```
        "string": "string"
       },
       "SourceEndpointArn": "string",
       "TableMappings": {
        "string": "string"
       },
       "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
       "AttributeDefinitions": [{
        "AttributeName": "string",
        "AttributeType": "string"
       }],
       "BillingModeSummary": {
        "BillingMode": "string",
        "LastUpdateToPayPerRequestDateTime": "string"
       },
       "CreationDateTime": "string",
       "DeletionProtectionEnabled": boolean,
       "GlobalSecondaryIndexes": [{
        "Backfilling": boolean,
        "IndexArn": "string",
        "IndexName": "string",
        "IndexSizeBytes": number,
        "IndexStatus": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "Projection": {
         "NonKeyAttributes": ["string"],
         "ProjectionType": "string"
        },
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        }
       }],
       "GlobalTableVersion": "string",
       "ItemCount": number,
```

```
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "LatestStreamArn": "string",
        "LatestStreamLabel": "string",
        "LocalSecondaryIndexes": [{
         "IndexArn": "string",
         "IndexName": "string",
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         }
        }],
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        },
        "Replicas": [{
         "GlobalSecondaryIndexes": [{
          "IndexName": "string",
          "ProvisionedThroughputOverride": {
           "ReadCapacityUnits": number
          }
         }],
         "KmsMasterKeyId": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         },
         "RegionName": "string",
         "ReplicaStatus": "string",
         "ReplicaStatusDescription": "string"
        }],
        "RestoreSummary": {
         "RestoreDateTime": "string",
         "RestoreInProgress": boolean,
         "SourceBackupArn": "string",
```

```
        "SourceTableArn": "string"
       },
       "SseDescription": {
        "InaccessibleEncryptionDateTime": "string",
        "KmsMasterKeyArn": "string",
        "SseType": "string",
        "Status": "string"
       },
       "StreamSpecification": {
        "StreamEnabled": boolean,
        "StreamViewType": "string"
       },
       "TableId": "string",
       "TableName": "string",
       "TableSizeBytes": number,
       "TableStatus": "string"
      },
      "AwsEc2ClientVpnEndpoint": {
       "AuthenticationOptions": [
        {
         "MutualAuthentication": {
          "ClientRootCertificateChainArn": "string"
         },
         "Type": "string"
        }
       ],
       "ClientCidrBlock": "string",
       "ClientConnectOptions": {
        "Enabled": boolean
       },
       "ClientLoginBannerOptions": {
        "Enabled": boolean
       },
       "ClientVpnEndpointId": "string",
       "ConnectionLogOptions": {
        "Enabled": boolean
       },
       "Description": "string",
       "DnsServer": ["string"],
       "ServerCertificateArn": "string",
       "SecurityGroupIdSet": [
        "string"
       ],
       "SelfServicePortalUrl": "string",
```

```
        "SessionTimeoutHours": "integer",
        "SplitTunnel": boolean,
        "TransportProtocol": "string",
        "VpcId": "string",
        "VpnPort": integer
      },
      "AwsEc2Eip": {
        "AllocationId": "string",
        "AssociationId": "string",
        "Domain": "string",
        "InstanceId": "string",
        "NetworkBorderGroup": "string",
        "NetworkInterfaceId": "string",
        "NetworkInterfaceOwnerId": "string",
        "PrivateIpAddress": "string",
        "PublicIp": "string",
        "PublicIpv4Pool": "string"
      },
      "AwsEc2Instance": {
        "IamInstanceProfileArn": "string",
        "ImageId": "string",
        "IpV4Addresses": ["string"],
        "IpV6Addresses": ["string"],
        "KeyName": "string",
        "LaunchedAt": "string",
        "MetadataOptions": {
          "HttpEndpoint": "string",
          "HttpProtocolIpv6": "string",
          "HttpPutResponseHopLimit": number,
          "HttpTokens": "string",
          "InstanceMetadataTags": "string"
        },
        "Monitoring": {
          "State": "string"
        },
        "NetworkInterfaces": [{
          "NetworkInterfaceId": "string"
        }],
        "SubnetId": "string",
        "Type": "string",
        "VirtualizationType": "string",
        "VpcId": "string"
      },
      "AwsEc2LaunchTemplate": {
```

```
        "DefaultVersionNumber": "string",
        "ElasticGpuSpecifications": ["string"],
        "ElasticInferenceAccelerators": ["string"],
        "Id": "string",
        "ImageId": "string",
        "LatestVersionNumber": "string",
        "LaunchTemplateData": {
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteonTermination": boolean,
           "Encrypted": boolean,
           "SnapshotId": "string",
           "VolumeSize": number,
           "VolumeType": "string"
          }
         }],
         "MetadataOptions": {
          "HttpTokens": "string",
          "HttpPutResponseHopLimit" : number
         },
         "Monitoring": {
          "Enabled": boolean
         },
         "NetworkInterfaces": [{
          "AssociatePublicIpAddress" : boolean
         }]
        },
        "LaunchTemplateName": "string",
        "LicenseSpecifications": ["string"],
        "SecurityGroupIds": ["string"],
        "SecurityGroups": ["string"],
        "TagSpecifications": ["string"]
       },
       "AwsEc2NetworkAcl": {
        "Associations": [{
         "NetworkAclAssociationId": "string",
         "NetworkAclId": "string",
         "SubnetId": "string"
        }],
        "Entries": [{
         "CidrBlock": "string",
         "Egress": boolean,
         "IcmpTypeCode": {
```

```
          "Code": number,
          "Type": number
         },
         "Ipv6CidrBlock": "string",
         "PortRange": {
          "From": number,
          "To": number
         },
         "Protocol": "string",
         "RuleAction": "string",
         "RuleNumber": number
        }],
        "IsDefault": boolean,
        "NetworkAclId": "string",
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2NetworkInterface": {
        "Attachment": {
         "AttachmentId": "string",
         "AttachTime": "string",
         "DeleteOnTermination": boolean,
         "DeviceIndex": number,
         "InstanceId": "string",
         "InstanceOwnerId": "string",
         "Status": "string"
        },
        "Ipv6Addresses": [{
         "Ipv6Address": "string"
        }],
        "NetworkInterfaceId": "string",
        "PrivateIpAddresses": [{
         "PrivateDnsName": "string",
         "PrivateIpAddress": "string"
        }],
        "PublicDnsName": "string",
        "PublicIp": "string",
        "SecurityGroups": [{
         "GroupId": "string",
         "GroupName": "string"
        }],
        "SourceDestCheck": boolean
       },
       "AwsEc2RouteTable": {
```

```
        "AssociationSet": [{
         "AssociationState": {
          "State": "string"
         },
         "Main": boolean,
         "RouteTableAssociationId": "string",
         "RouteTableId": "string"
        }],
        "PropogatingVgwSet": [],
        "RouteTableId": "string",
        "RouteSet": [
         {
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         },
         {
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         }
        ],
        "VpcId": "string"
       },
       "AwsEc2SecurityGroup": {
        "GroupId": "string",
        "GroupName": "string",
        "IpPermissions": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
```

```
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "IpPermissionsEgress": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2Subnet": {
        "AssignIpv6AddressOnCreation": boolean,
        "AvailabilityZone": "string",
        "AvailabilityZoneId": "string",
        "AvailableIpAddressCount": number,
        "CidrBlock": "string",
        "DefaultForAz": boolean,
        "Ipv6CidrBlockAssociationSet": [{
         "AssociationId": "string",
         "Ipv6CidrBlock": "string",
         "CidrBlockState": "string"
        }],
```

```
        "MapPublicIpOnLaunch": boolean,
        "OwnerId": "string",
        "State": "string",
        "SubnetArn": "string",
        "SubnetId": "string",
        "VpcId": "string"
      },
      "AwsEc2TransitGateway": {
        "AmazonSideAsn": number,
        "AssociationDefaultRouteTableId": "string",
        "AutoAcceptSharedAttachments": "string",
        "DefaultRouteTableAssociation": "string",
        "DefaultRouteTablePropagation": "string",
        "Description": "string",
        "DnsSupport": "string",
        "Id": "string",
        "MulticastSupport": "string",
        "PropagationDefaultRouteTableId": "string",
        "TransitGatewayCidrBlocks": ["string"],
        "VpnEcmpSupport": "string"
      },
      "AwsEc2Volume": {
        "Attachments": [{
          "AttachTime": "string",
          "DeleteOnTermination": boolean,
          "InstanceId": "string",
          "Status": "string"
        }],
        "CreateTime": "string",
        "DeviceName": "string",
        "Encrypted": boolean,
        "KmsKeyId": "string",
        "Size": number,
        "SnapshotId": "string",
        "Status": "string",
        "VolumeId": "string",
        "VolumeScanStatus": "string",
        "VolumeType": "string"
      },
      "AwsEc2Vpc": {
        "CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlock": "string",
          "CidrBlockState": "string"
```

```
        }],
        "DhcpOptionsId": "string",
        "Ipv6CidrBlockAssociationSet": [{
         "AssociationId": "string",
         "CidrBlockState": "string",
         "Ipv6CidrBlock": "string"
        }],
        "State": "string"
       },
       "AwsEc2VpcEndpointService": {
        "AcceptanceRequired": boolean,
        "AvailabilityZones": ["string"],
        "BaseEndpointDnsNames": ["string"],
        "ManagesVpcEndpoints": boolean,
        "GatewayLoadBalancerArns": ["string"],
        "NetworkLoadBalancerArns": ["string"],
        "PrivateDnsName": "string",
        "ServiceId": "string",
        "ServiceName": "string",
        "ServiceState": "string",
        "ServiceType": [{
         "ServiceType": "string"
        }]
       },
       "AwsEc2VpcPeeringConnection": {
        "AccepterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "ExpirationTime": "string",
        "RequesterVpcInfo": {
```

```
        "CidrBlock": "string",
        "CidrBlockSet": [{
         "CidrBlock": "string"
        }],
        "Ipv6CidrBlockSet": [{
         "Ipv6CidrBlock": "string"
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "Status": {
        "Code": "string",
        "Message": "string"
       },
       "VpcPeeringConnectionId": "string"
      },
      "AwsEc2VpnConnection": {
       "Category": "string",
       "CustomerGatewayConfiguration": "string",
       "CustomerGatewayId": "string",
       "Options": {
        "StaticRoutesOnly": boolean,
        "TunnelOptions": [{
         "DpdTimeoutSeconds": number,
         "IkeVersions": ["string"],
         "OutsideIpAddress": "string",
         "Phase1DhGroupNumbers": [number],
         "Phase1EncryptionAlgorithms": ["string"],
         "Phase1IntegrityAlgorithms": ["string"],
         "Phase1LifetimeSeconds": number,
         "Phase2DhGroupNumbers": [number],
         "Phase2EncryptionAlgorithms": ["string"],
         "Phase2IntegrityAlgorithms": ["string"],
         "Phase2LifetimeSeconds": number,
         "PreSharedKey": "string",
         "RekeyFuzzPercentage": number,
         "RekeyMarginTimeSeconds": number,
         "ReplayWindowSize": number,
```

```
          "TunnelInsideCidr": "string"
         }]
        },
        "Routes": [{
         "DestinationCidrBlock": "string",
         "State": "string"
        }],
        "State": "string",
        "TransitGatewayId": "string",
        "Type": "string",
        "VgwTelemetry": [{
         "AcceptedRouteCount": number,
         "CertificateArn": "string",
         "LastStatusChange": "string",
         "OutsideIpAddress": "string",
         "Status": "string",
         "StatusMessage": "string"
        }],
        "VpnConnectionId": "string",
        "VpnGatewayId": "string"
       },
       "AwsEcrContainerImage": {
        "Architecture": "string",
        "ImageDigest": "string",
        "ImagePublishedAt": "string",
        "ImageTags": ["string"],
        "RegistryId": "string",
        "RepositoryName": "string"
       },
       "AwsEcrRepository": {
        "Arn": "string",
        "ImageScanningConfiguration": {
         "ScanOnPush": boolean
        },
        "ImageTagMutability": "string",
        "LifecyclePolicy": {
         "LifecyclePolicyText": "string",
         "RegistryId": "string"
        },
        "RepositoryName": "string",
        "RepositoryPolicyText": "string"
       },
       "AwsEcsCluster": {
        "ActiveServicesCount": number,
```

```
        "CapacityProviders": ["string"],
        "ClusterArn": "string",
        "ClusterName": "string",
        "ClusterSettings": [{
         "Name": "string",
         "Value": "string"
        }],
        "Configuration": {
         "ExecuteCommandConfiguration": {
          "KmsKeyId": "string",
          "LogConfiguration": {
           "CloudWatchEncryptionEnabled": boolean,
           "CloudWatchLogGroupName": "string",
           "S3BucketName": "string",
           "S3EncryptionEnabled": boolean,
           "S3KeyPrefix": "string"
          },
          "Logging": "string"
         }
        },
        "DefaultCapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "RegisteredContainerInstancesCount": number,
        "RunningTasksCount": number,
        "Status": "string"
       },
       "AwsEcsContainer": {
        "Image": "string",
        "MountPoints": [{
         "ContainerPath": "string",
         "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
       },
       "AwsEcsService": {
        "CapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
```

```
        "Cluster": "string",
        "DeploymentConfiguration": {
         "DeploymentCircuitBreaker": {
          "Enable": boolean,
          "Rollback": boolean
         },
         "MaximumPercent": number,
         "MinimumHealthyPercent": number
        },
        "DeploymentController": {
         "Type": "string"
        },
        "DesiredCount": number,
        "EnableEcsManagedTags": boolean,
        "EnableExecuteCommand": boolean,
        "HealthCheckGracePeriodSeconds": number,
        "LaunchType": "string",
        "LoadBalancers": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "LoadBalancerName": "string",
         "TargetGroupArn": "string"
        }],
        "Name": "string",
        "NetworkConfiguration": {
         "AwsVpcConfiguration": {
          "AssignPublicIp": "string",
          "SecurityGroups": ["string"],
          "Subnets": ["string"]
         }
        },
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "PlacementStrategies": [{
         "Field": "string",
         "Type": "string"
        }],
        "PlatformVersion": "string",
        "PropagateTags": "string",
        "Role": "string",
        "SchedulingStrategy": "string",
        "ServiceArn": "string",
```

```
        "ServiceName": "string",
        "ServiceRegistries": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "Port": number,
         "RegistryArn": "string"
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
        "TaskDefinitionArn": "string",
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
          "Condition": "string",
          "ContainerName": "string"
         }],
         "DisableNetworking": boolean,
         "DnsSearchDomains": ["string"],
         "DnsServers": ["string"],
```

```
        "DockerLabels": {
         "string": "string"
        },
        "DockerSecurityOptions": ["string"],
        "EntryPoint": ["string"],
        "Environment": [{
         "Name": "string",
         "Value": "string"
        }],
        "EnvironmentFiles": [{
         "Type": "string",
         "Value": "string"
        }],
        "Essential": boolean,
        "ExtraHosts": [{
         "Hostname": "string",
         "IpAddress": "string"
        }],
        "FirelensConfiguration": {
         "Options": {
          "string": "string"
         },
         "Type": "string"
        },
        "HealthCheck": {
         "Command": ["string"],
         "Interval": number,
         "Retries": number,
         "StartPeriod": number,
         "Timeout": number
        },
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
         "Capabilities": {
          "Add": ["string"],
          "Drop": ["string"]
         },
         "Devices": [{
          "ContainerPath": "string",
          "HostPath": "string",
          "Permissions": ["string"]
```

```
          }],
          "InitProcessEnabled": boolean,
          "MaxSwap": number,
          "SharedMemorySize": number,
          "Swappiness": number,
          "Tmpfs": [{
           "ContainerPath": "string",
           "MountOptions": ["string"],
           "Size": number
          }]
         },
         "LogConfiguration": {
          "LogDriver": "string",
          "Options": {
           "string": "string"
          },
          "SecretOptions": [{
           "Name": "string",
           "ValueFrom": "string"
          }]
         },
         "Memory": number,
         "MemoryReservation": number,
         "MountPoints": [{
          "ContainerPath": "string",
          "ReadOnly": boolean,
          "SourceVolume": "string"
         }],
         "Name": "string",
         "PortMappings": [{
          "ContainerPort": number,
          "HostPort": number,
          "Protocol": "string"
         }],
         "Privileged": boolean,
         "PseudoTerminal": boolean,
         "ReadonlyRootFilesystem": boolean,
         "RepositoryCredentials": {
          "CredentialsParameter": "string"
         },
         "ResourceRequirements": [{
          "Type": "string",
          "Value": "string"
         }],
```

```
        "Secrets": [{
         "Name": "string",
         "ValueFrom": "string"
        }],
        "StartTimeout": number,
        "StopTimeout": number,
        "SystemControls": [{
         "Namespace": "string",
         "Value": "string"
        }],
        "Ulimits": [{
         "HardLimit": number,
         "Name": "string",
         "SoftLimit": number
        }],
        "User": "string",
        "VolumesFrom": [{
         "ReadOnly": boolean,
         "SourceContainer": "string"
        }],
        "WorkingDirectory": "string"
       }],
       "Cpu": "string",
       "ExecutionRoleArn": "string",
       "Family": "string",
       "InferenceAccelerators": [{
        "DeviceName": "string",
        "DeviceType": "string"
       }],
       "IpcMode": "string",
       "Memory": "string",
       "NetworkMode": "string",
       "PidMode": "string",
       "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
       }],
       "ProxyConfiguration": {
        "ContainerName": "string",
        "ProxyConfigurationProperties": [{
         "Name": "string",
         "Value": "string"
        }],
        "Type": "string"
```

```
        },
        "RequiresCompatibilities": ["string"],
        "Status": "string",
        "TaskRoleArn": "string",
        "Volumes": [{
         "DockerVolumeConfiguration": {
          "Autoprovision": boolean,
          "Driver": "string",
          "DriverOpts": {
           "string": "string"
          },
          "Labels": {
           "string": "string"
          },
          "Scope": "string"
         },
         "EfsVolumeConfiguration": {
          "AuthorizationConfig": {
           "AccessPointId": "string",
           "Iam": "string"
          },
          "FilesystemId": "string",
          "RootDirectory": "string",
          "TransitEncryption": "string",
          "TransitEncryptionPort": number
         },
         "Host": {
          "SourcePath": "string"
         },
         "Name": "string"
        }]
       },
       "AwsEfsAccessPoint": {
        "AccessPointId": "string",
        "Arn": "string",
        "ClientToken": "string",
        "FileSystemId": "string",
        "PosixUser": {
         "Gid": "string",
         "SecondaryGids": ["string"],
         "Uid": "string"
        },
        "RootDirectory": {
         "CreationInfo": {
```

```
          "OwnerGid": "string",
          "OwnerUid": "string",
          "Permissions": "string"
         },
         "Path": "string"
        }
       },
       "AwsEksCluster": {
        "Arn": "string",
        "CertificateAuthorityData": "string",
        "ClusterStatus": "string",
        "Endpoint": "string",
        "Logging": {
         "ClusterLogging": [{
          "Enabled": boolean,
          "Types": ["string"]
         }]
        },
        "Name": "string",
        "ResourcesVpcConfig": {
         "EndpointPublicAccess": boolean,
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "RoleArn": "string",
        "Version": "string"
       },
       "AwsElasticBeanstalkEnvironment": {
        "ApplicationName": "string",
        "Cname": "string",
        "DateCreated": "string",
        "DateUpdated": "string",
        "Description": "string",
        "EndpointUrl": "string",
        "EnvironmentArn": "string",
        "EnvironmentId": "string",
        "EnvironmentLinks": [{
         "EnvironmentName": "string",
         "LinkName": "string"
        }],
        "EnvironmentName": "string",
        "OptionSettings": [{
         "Namespace": "string",
         "OptionName": "string",
```

```
        "ResourceName": "string",
        "Value": "string"
       }],
       "PlatformArn": "string",
       "SolutionStackName": "string",
       "Status": "string",
       "Tier": {
        "Name": "string",
        "Type": "string",
        "Version": "string"
       },
       "VersionLabel": "string"
      },
      "AwsElasticSearchDomain": {
       "AccessPolicies": "string",
       "DomainStatus": {
        "DomainId": "string",
        "DomainName": "string",
        "Endpoint": "string",
        "Endpoints": {
         "string": "string"
        }
       },
       "DomainEndpointOptions": {
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
       },
       "ElasticsearchClusterConfig": {
        "DedicatedMasterCount": number,
        "DedicatedMasterEnabled": boolean,
        "DedicatedMasterType": "string",
        "InstanceCount": number,
        "InstanceType": "string",
        "ZoneAwarenessConfig": {
         "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
       },
       "ElasticsearchVersion": "string",
       "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
       },
       "LogPublishingOptions": {
```

```
        "AuditLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "IndexSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "SearchSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        }
       },
       "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
       },
       "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
        "NewVersion": "string",
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
       },
       "VPCOptions": {
        "AvailabilityZones": [
         "string"
        ],
        "SecurityGroupIds": [
         "string"
        ],
        "SubnetIds": [
         "string"
        ],
        "VPCId": "string"
       }
      },
      "AwsElbLoadBalancer": {
       "AvailabilityZones": ["string"],
       "BackendServerDescriptions": [{
        "InstancePort": number,
        "PolicyNames": ["string"]
       }],
```

```
        "CanonicalHostedZoneName": "string",
        "CanonicalHostedZoneNameID": "string",
        "CreatedTime": "string",
        "DnsName": "string",
        "HealthCheck": {
         "HealthyThreshold": number,
         "Interval": number,
         "Target": "string",
         "Timeout": number,
         "UnhealthyThreshold": number
        },
        "Instances": [{
         "InstanceId": "string"
        }],
        "ListenerDescriptions": [{
         "Listener": {
          "InstancePort": number,
          "InstanceProtocol": "string",
          "LoadBalancerPort": number,
          "Protocol": "string",
          "SslCertificateId": "string"
         },
         "PolicyNames": ["string"]
        }],
        "LoadBalancerAttributes": {
         "AccessLog": {
          "EmitInterval": number,
          "Enabled": boolean,
          "S3BucketName": "string",
          "S3BucketPrefix": "string"
         },
         "ConnectionDraining": {
          "Enabled": boolean,
          "Timeout": number
         },
         "ConnectionSettings": {
          "IdleTimeout": number
         },
         "CrossZoneLoadBalancing": {
          "Enabled": boolean
         },
         "AdditionalAttributes": [{
                        "Key": "string",
                        "Value": "string"
```

```
                }]
       },
       "LoadBalancerName": "string",
       "Policies": {
        "AppCookieStickinessPolicies": [{
         "CookieName": "string",
         "PolicyName": "string"
        }],
        "LbCookieStickinessPolicies": [{
         "CookieExpirationPeriod": number,
         "PolicyName": "string"
        }],
        "OtherPolicies": ["string"]
       },
       "Scheme": "string",
       "SecurityGroups": ["string"],
       "SourceSecurityGroup": {
        "GroupName": "string",
        "OwnerAlias": "string"
       },
       "Subnets": ["string"],
       "VpcId": "string"
      },
      "AwsElbv2LoadBalancer": {
       "AvailabilityZones": {
        "SubnetId": "string",
        "ZoneName": "string"
       },
       "CanonicalHostedZoneId": "string",
       "CreatedTime": "string",
       "DNSName": "string",
       "IpAddressType": "string",
       "LoadBalancerAttributes": [{
        "Key": "string",
        "Value": "string"
       }],
       "Scheme": "string",
       "SecurityGroups": ["string"],
       "State": {
        "Code": "string",
        "Reason": "string"
       },
       "Type": "string",
       "VpcId": "string"
```

```
      },
      "AwsEventSchemasRegistry": {
       "Description": "string",
       "RegistryArn": "string",
       "RegistryName": "string"
      },
      "AwsEventsEndpoint": {
       "Arn": "string",
       "Description": "string",
       "EndpointId": "string",
       "EndpointUrl": "string",
       "EventBuses": [
           {
               "EventBusArn": "string"
           },
           {
               "EventBusArn": "string"
           }
       ],
       "Name": "string",
       "ReplicationConfig": {
           "State": "string"
       },
       "RoleArn": "string",
       "RoutingConfig": {
           "FailoverConfig": {
               "Primary": {
                   "HealthCheck": "string"
               },
               "Secondary": {
                   "Route": "string"
               }
           }
       },
       "State": "string"
      },
      "AwsEventsEventBus": {
       "Arn": "string",
       "Name": "string",
       "Policy": "string"
      },
      "AwsGuardDutyDetector": {
       "FindingPublishingFrequency": "string",
       "ServiceRole": "string",
```

```
        "Status": "string",
        "DataSources": {
         "CloudTrail": {
          "Status": "string"
         },
         "DnsLogs": {
          "Status": "string"
         },
         "FlowLogs": {
          "Status": "string"
         },
         "S3Logs": {
          "Status": "string"
         },
         "Kubernetes": {
          "AuditLogs": {
           "Status": "string"
          }
         },
         "MalwareProtection": {
          "ScanEc2InstanceWithFindings": {
           "EbsVolumes": {
            "Status": "string"
           }
          },
          "ServiceRole": "string"
         }
        }
       },
       "AwsIamAccessKey": {
        "AccessKeyId": "string",
        "AccountId": "string",
        "CreatedAt": "string",
        "PrincipalId": "string",
        "PrincipalName": "string",
        "PrincipalType": "string",
        "SessionContext": {
         "Attributes": {
          "CreationDate": "string",
          "MfaAuthenticated": boolean
         },
         "SessionIssuer": {
          "AccountId": "string",
          "Arn": "string",
```

```
          "PrincipalId": "string",
          "Type": "string",
          "UserName": "string"
         }
        },
        "Status": "string"
       },
       "AwsIamGroup": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupId": "string",
        "GroupName": "string",
        "GroupPolicyList": [{
         "PolicyName": "string"
        }],
        "Path": "string"
       },
       "AwsIamPolicy": {
        "AttachmentCount": number,
        "CreateDate": "string",
        "DefaultVersionId": "string",
        "Description": "string",
        "IsAttachable": boolean,
        "Path": "string",
        "PermissionsBoundaryUsageCount": number,
        "PolicyId": "string",
        "PolicyName": "string",
        "PolicyVersionList": [{
         "CreateDate": "string",
         "IsDefaultVersion": boolean,
         "VersionId": "string"
        }],
        "UpdateDate": "string"
       },
       "AwsIamRole": {
        "AssumeRolePolicyDocument": "string",
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
```

```
        "InstanceProfileList": [{
         "Arn": "string",
         "CreateDate": "string",
         "InstanceProfileId": "string",
         "InstanceProfileName": "string",
         "Path": "string",
         "Roles": [{
          "Arn": "string",
          "AssumeRolePolicyDocument": "string",
          "CreateDate": "string",
          "Path": "string",
          "RoleId": "string",
          "RoleName": "string"
         }]
        }],
        "MaxSessionDuration": number,
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsIamUser": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
        }]
```

```
      },
      "AwsKinesisStream": {
       "Arn": "string",
       "Name": "string",
       "RetentionPeriodHours": number,
       "ShardCount": number,
       "StreamEncryption": {
        "EncryptionType": "string",
        "KeyId": "string"
       }
      },
      "AwsKmsKey": {
       "AWSAccountId": "string",
       "CreationDate": "string",
       "Description": "string",
       "KeyId": "string",
       "KeyManager": "string",
       "KeyRotationStatus": boolean,
       "KeyState": "string",
       "Origin": "string"
      },
      "AwsLambdaFunction": {
       "Architectures": [
        "string"
       ],
       "Code": {
        "S3Bucket": "string",
        "S3Key": "string",
        "S3ObjectVersion": "string",
        "ZipFile": "string"
       },
       "CodeSha256": "string",
       "DeadLetterConfig": {
        "TargetArn": "string"
       },
       "Environment": {
        "Variables": {
         "Stage": "string"
        },
        "Error": {
         "ErrorCode": "string",
         "Message": "string"
        }
       },
```

```
        "FunctionName": "string",
        "Handler": "string",
        "KmsKeyArn": "string",
        "LastModified": "string",
        "Layers": {
         "Arn": "string",
         "CodeSize": number
        },
        "PackageType": "string",
        "RevisionId": "string",
        "Role": "string",
        "Runtime": "string",
        "Timeout": integer,
        "TracingConfig": {
         "Mode": "string"
        },
        "Version": "string",
        "VpcConfig": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "MasterArn": "string",
        "MemorySize": number
       },
       "AwsLambdaLayerVersion": {
        "CompatibleRuntimes": [
         "string"
        ],
        "CreatedDate": "string",
        "Version": number
       },
       "AwsMskCluster": {
        "ClusterInfo": {
         "ClientAuthentication": {
          "Sasl": {
           "Scram": {
            "Enabled": boolean
           },
           "Iam": {
            "Enabled": boolean
           }
          },
          "Tls": {
           "CertificateAuthorityArnList": [],
```

```
          "Enabled": boolean
         },
         "Unauthenticated": {
          "Enabled": boolean
         }
        },
        "ClusterName": "string",
        "CurrentVersion": "string",
        "EncryptionInfo": {
         "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "string"
         },
         "EncryptionInTransit": {
          "ClientBroker": "string",
          "InCluster": boolean
         }
        },
        "EnhancedMonitoring": "string",
        "NumberOfBrokerNodes": integer
       }
      },
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
       "FirewallName": "string",
       "FirewallPolicyArn": "string",
       "FirewallPolicyChangeProtection": boolean,
       "SubnetChangeProtection": boolean,
       "SubnetMappings": [{
        "SubnetId": "string"
       }],
       "VpcId": "string"
      },
      "AwsNetworkFirewallFirewallPolicy": {
       "Description": "string",
       "FirewallPolicy": {
        "StatefulRuleGroupReferences": [{
         "ResourceArn": "string"
        }],
        "StatelessCustomActions": [{
         "ActionDefinition": {
          "PublishMetricAction": {
```

```
          "Dimensions": [{
           "Value": "string"
          }]
         }
        },
        "ActionName": "string"
       }],
       "StatelessDefaultActions": ["string"],
       "StatelessFragmentDefaultActions": ["string"],
       "StatelessRuleGroupReferences": [{
        "Priority": number,
        "ResourceArn": "string"
       }]
      },
      "FirewallPolicyArn": "string",
      "FirewallPolicyId": "string",
      "FirewallPolicyName": "string"
     },
     "AwsNetworkFirewallRuleGroup": {
      "Capacity": number,
      "Description": "string",
      "RuleGroup": {
       "RulesSource": {
        "RulesSourceList": {
         "GeneratedRulesType": "string",
         "Targets": ["string"],
         "TargetTypes": ["string"]
        },
        "RulesString": "string",
        "StatefulRules": [{
         "Action": "string",
         "Header": {
          "Destination": "string",
          "DestinationPort": "string",
          "Direction": "string",
          "Protocol": "string",
          "Source": "string",
          "SourcePort": "string"
         },
         "RuleOptions": [{
          "Keyword": "string",
          "Settings": ["string"]
         }]
        }],
```

```
          "StatelessRulesAndCustomActions": {
           "CustomActions": [{
            "ActionDefinition": {
             "PublishMetricAction": {
              "Dimensions": [{
               "Value": "string"
              }]
             }
            },
            "ActionName": "string"
           }],
           "StatelessRules": [{
            "Priority": number,
            "RuleDefinition": {
             "Actions": ["string"],
             "MatchAttributes": {
              "DestinationPorts": [{
               "FromPort": number,
               "ToPort": number
              }],
              "Destinations": [{
               "AddressDefinition": "string"
              }],
              "Protocols": [number],
              "SourcePorts": [{
               "FromPort": number,
               "ToPort": number
              }],
              "Sources": [{
               "AddressDefinition": "string"
              }],
              "TcpFlags": [{
               "Flags": ["string"],
               "Masks": ["string"]
              }]
             }
            }
           }]
          }
         },
         "RuleVariables": {
          "IpSets": {
           "Definition": ["string"]
          },
```

```
          "PortSets": {
           "Definition": ["string"]
          }
         }
        },
        "RuleGroupArn": "string",
        "RuleGroupId": "string",
        "RuleGroupName": "string",
        "Type": "string"
       },
       "AwsOpenSearchServiceDomain": {
        "AccessPolicies": "string",
        "AdvancedSecurityOptions": {
         "Enabled": boolean,
         "InternalUserDatabaseEnabled": boolean,
         "MasterUserOptions": {
          "MasterUserArn": "string",
          "MasterUserName": "string",
          "MasterUserPassword": "string"
         }
        },
        "Arn": "string",
        "ClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "WarmCount": number,
         "WarmEnabled": boolean,
         "WarmType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "DomainEndpoint": "string",
        "DomainEndpointOptions": {
         "CustomEndpoint": "string",
         "CustomEndpointCertificateArn": "string",
         "CustomEndpointEnabled": boolean,
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
```

```
        "DomainEndpoints": {
         "string": "string"
        },
        "DomainName": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "EngineVersion": "string",
        "Id": "string",
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "OptionalDeployment": boolean,
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VpcOptions": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        }
       },
       "AwsRdsDbCluster": {
        "ActivityStreamStatus": "string",
```

```
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZones": ["string"],
        "BackupRetentionPeriod": integer,
        "ClusterCreateTime": "string",
        "CopyTagsToSnapshot": boolean,
        "CrossAccountClone": boolean,
        "CustomEndpoints": ["string"],
        "DatabaseName": "string",
        "DbClusterIdentifier": "string",
        "DbClusterMembers": [{
         "DbClusterParameterGroupStatus": "string",
         "DbInstanceIdentifier": "string",
         "IsClusterWriter": boolean,
         "PromotionTier": integer
        }],
        "DbClusterOptionGroupMemberships": [{
         "DbClusterOptionGroupName": "string",
         "Status": "string"
        }],
        "DbClusterParameterGroup": "string",
        "DbClusterResourceId": "string",
        "DbSubnetGroup": "string",
        "DeletionProtection": boolean,
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Endpoint": "string",
        "Engine": "string",
        "EngineMode": "string",
        "EngineVersion": "string",
        "HostedZoneId": "string",
        "HttpEndpointEnabled": boolean,
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "MasterUsername": "string",
```

```
        "MultiAz": boolean,
        "Port": integer,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ReaderEndpoint": "string",
        "ReadReplicaIdentifiers": ["string"],
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRdsDbClusterSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZones": ["string"],
        "ClusterCreateTime": "string",
        "DbClusterIdentifier": "string",
        "DbClusterSnapshotAttributes": [{
         "AttributeName": "string",
         "AttributeValues": ["string"]
        }],
        "DbClusterSnapshotIdentifier": "string",
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "PercentProgress": integer,
        "Port": integer,
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
       },
       "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "FeatureName": "string",
         "Status": "string"
        }],
```

```
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
         "DbParameterGroupName": "string",
         "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
         "DbSubnetGroupArn": "string",
         "DbSubnetGroupDescription": "string",
         "DbSubnetGroupName": "string",
         "SubnetGroupStatus": "string",
         "Subnets": [{
          "SubnetAvailabilityZone": {
           "Name": "string"
          },
          "SubnetIdentifier": "string",
          "SubnetStatus": "string"
         }],
         "VpcId": "string"
        },
        "DeletionProtection": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number,
         "HostedZoneId": "string"
        },
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
```

```
        "EnabledCloudwatchLogsExports": ["string"],
        "Engine": "string",
        "EngineVersion": "string",
        "EnhancedMonitoringResourceArn": "string",
        "IAMDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LatestRestorableTime": "string",
        "LicenseModel": "string",
        "ListenerEndpoint": {
         "Address": "string",
         "HostedZoneId": "string",
         "Port": number
        },
        "MasterUsername": "admin",
        "MaxAllocatedStorage": number,
        "MonitoringInterval": number,
        "MonitoringRoleArn": "string",
        "MultiAz": boolean,
        "OptionGroupMemberships": [{
         "OptionGroupName": "string",
         "Status": "string"
        }],
        "PendingModifiedValues": {
         "AllocatedStorage": number,
         "BackupRetentionPeriod": number,
         "CaCertificateIdentifier": "string",
         "DbInstanceClass": "string",
         "DbInstanceIdentifier": "string",
         "DbSubnetGroupName": "string",
         "EngineVersion": "string",
         "Iops": number,
         "LicenseModel": "string",
         "MasterUserPassword": "string",
         "MultiAZ": boolean,
         "PendingCloudWatchLogsExports": {
          "LogTypesToDisable": ["string"],
          "LogTypesToEnable": ["string"]
         },
         "Port": number,
         "ProcessorFeatures": [{
          "Name": "string",
          "Value": "string"
```

```
        }],
        "StorageType": "string"
       },
       "PerformanceInsightsEnabled": boolean,
       "PerformanceInsightsKmsKeyId": "string",
       "PerformanceInsightsRetentionPeriod": number,
       "PreferredBackupWindow": "string",
       "PreferredMaintenanceWindow": "string",
       "ProcessorFeatures": [{
        "Name": "string",
        "Value": "string"
       }],
       "PromotionTier": number,
       "PubliclyAccessible": boolean,
       "ReadReplicaDBClusterIdentifiers": ["string"],
       "ReadReplicaDBInstanceIdentifiers": ["string"],
       "ReadReplicaSourceDBInstanceIdentifier": "string",
       "SecondaryAvailabilityZone": "string",
       "StatusInfos": [{
        "Message": "string",
        "Normal": boolean,
        "Status": "string",
        "StatusType": "string"
       }],
       "StorageEncrypted": boolean,
       "TdeCredentialArn": "string",
       "Timezone": "string",
       "VpcSecurityGroups": [{
        "VpcSecurityGroupId": "string",
        "Status": "string"
       }]
      },
      "AwsRdsDbSecurityGroup": {
       "DbSecurityGroupArn": "string",
       "DbSecurityGroupDescription": "string",
       "DbSecurityGroupName": "string",
       "Ec2SecurityGroups": [{
        "Ec2SecurityGroupuId": "string",
        "Ec2SecurityGroupName": "string",
        "Ec2SecurityGroupOwnerId": "string",
        "Status": "string"
       }],
       "IpRanges": [{
        "CidrIp": "string",
```

```
        "Status": "string"
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsRdsDbSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZone": "string",
       "DbInstanceIdentifier": "string",
       "DbiResourceId": "string",
       "DbSnapshotIdentifier": "string",
       "Encrypted": boolean,
       "Engine": "string",
       "EngineVersion": "string",
       "IamDatabaseAuthenticationEnabled": boolean,
       "InstanceCreateTime": "string",
       "Iops": number,
       "KmsKeyId": "string",
       "LicenseModel": "string",
       "MasterUsername": "string",
       "OptionGroupName": "string",
       "PercentProgress": integer,
       "Port": integer,
       "ProcessorFeatures": [],
       "SnapshotCreateTime": "string",
       "SnapshotType": "string",
       "SourceDbSnapshotIdentifier": "string",
       "SourceRegion": "string",
       "Status": "string",
       "StorageType": "string",
       "TdeCredentialArn": "string",
       "Timezone": "string",
       "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
       "CustomerAwsId": "string",
       "CustSubscriptionId": "string",
       "Enabled": boolean,
       "EventCategoriesList": ["string"],
       "EventSubscriptionArn": "string",
       "SnsTopicArn": "string",
       "SourceIdsList": ["string"],
       "SourceType": "string",
       "Status": "string",
```

```
        "SubscriptionCreationTime": "string"
       },
       "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
         "NodeRole": "string",
         "PrivateIPAddress": "string",
         "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
         "ClusterParameterStatusList": [{
          "ParameterApplyErrorDescription": "string",
          "ParameterApplyStatus": "string",
          "ParameterName": "string"
         }],
         "ParameterApplyStatus": "string",
         "ParameterGroupName": "string"
        }],
        "ClusterPublicKey": "string",
        "ClusterRevisionNumber": "string",
        "ClusterSecurityGroups": [{
         "ClusterSecurityGroupName": "string",
         "Status": "string"
        }],
        "ClusterSnapshotCopyStatus": {
         "DestinationRegion": "string",
         "ManualSnapshotRetentionPeriod": number,
         "RetentionPeriod": number,
         "SnapshotCopyGrantName": "string"
        },
        "ClusterStatus": "string",
        "ClusterSubnetGroupName": "string",
        "ClusterVersion": "string",
        "DBName": "string",
        "DeferredMaintenanceWindows": [{
         "DeferMaintenanceEndTime": "string",
         "DeferMaintenanceIdentifier": "string",
         "DeferMaintenanceStartTime": "string"
        }],
```

```
        "ElasticIpStatus": {
         "ElasticIp": "string",
         "Status": "string"
        },
        "ElasticResizeNumberOfNodeOptions": "string",
        "Encrypted": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number
        },
        "EnhancedVpcRouting": boolean,
        "ExpectedNextSnapshotScheduleTime": "string",
        "ExpectedNextSnapshotScheduleTimeStatus": "string",
        "HsmStatus": {
         "HsmClientCertificateIdentifier": "string",
         "HsmConfigurationIdentifier": "string",
         "Status": "string"
        },
        "IamRoles": [{
         "ApplyStatus": "string",
         "IamRoleArn": "string"
        }],
        "KmsKeyId": "string",
        "LoggingStatus":{
                    "BucketName": "string",
                    "LastFailureMessage": "string",
                    "LastFailureTime": "string",
                    "LastSuccessfulDeliveryTime": "string",
                    "LoggingEnabled": boolean,
                    "S3KeyPrefix": "string"
                },
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
```

```
        "EnhancedVpcRouting": boolean,
        "MaintenanceTrackName": "string",
        "MasterUserPassword": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PubliclyAccessible": "string"
       },
       "PreferredMaintenanceWindow": "string",
       "PubliclyAccessible": boolean,
       "ResizeInfo": {
        "AllowCancelResize": boolean,
        "ResizeType": "string"
       },
       "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": number,
        "ElapsedTimeInSeconds": number,
        "EstimatedTimeToCompletionInSeconds": number,
        "ProgressInMegaBytes": number,
        "SnapshotSizeInMegaBytes": number,
        "Status": "string"
       },
       "SnapshotScheduleIdentifier": "string",
       "SnapshotScheduleState": "string",
       "VpcId": "string",
       "VpcSecurityGroups": [{
        "Status": "string",
        "VpcSecurityGroupId": "string"
       }]
      },
      "AwsRoute53HostedZone": {
       "HostedZone": {
        "Id": "string",
        "Name": "string",
        "Config": {
         "Comment": "string"
        }
       },
       "NameServers": ["string"],
       "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
         "CloudWatchLogsLogGroupArn": "string",
         "Id": "string",
         "HostedZoneId": "string"
        }
```

```
        },
        "Vpcs": [
         {
          "Id": "string",
          "Region": "string"
         }
        ]
       },
       "AwsS3AccessPoint": {
        "AccessPointArn": "string",
        "Alias": "string",
        "Bucket": "string",
        "BucketAccountId": "string",
        "Name": "string",
        "NetworkOrigin": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "VpcConfiguration": {
         "VpcId": "string"
        }
       },
       "AwsS3AccountPublicAccessBlock": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "AwsS3Bucket": {
        "AccessControlList": "string",
        "BucketLifecycleConfiguration": {
         "Rules": [{
          "AbortIncompleteMultipartUpload": {
           "DaysAfterInitiation": number
          },
          "ExpirationDate": "string",
          "ExpirationInDays": number,
          "ExpiredObjectDeleteMarker": boolean,
          "Filter": {
           "Predicate": {
            "Operands": [{
```

```
            "Prefix": "string",
            "Type": "string"
           },
           {
            "Tag": {
             "Key": "string",
             "Value": "string"
            },
            "Type": "string"
           }
          ],
          "Type": "string"
         }
        },
        "Id": "string",
        "NoncurrentVersionExpirationInDays": number,
        "NoncurrentVersionTransitions": [{
         "Days": number,
         "StorageClass": "string"
        }],
        "Prefix": "string",
        "Status": "string",
        "Transitions": [{
         "Date": "string",
         "Days": number,
         "StorageClass": "string"
        }]
       }]
      },
      "BucketLoggingConfiguration": {
       "DestinationBucketName": "string",
       "LogFilePrefix": "string"
      },
      "BucketName": "string",
      "BucketNotificationConfiguration": {
       "Configurations": [{
        "Destination": "string",
        "Events": ["string"],
        "Filter": {
         "S3KeyFilter": {
          "FilterRules": [{
           "Name": "string",
           "Value": "string"
          }]
```

```
          }
         },
         "Type": "string"
        }]
       },
       "BucketVersioningConfiguration": {
        "IsMfaDeleteEnabled": boolean,
        "Status": "string"
       },
       "BucketWebsiteConfiguration": {
        "ErrorDocument": "string",
        "IndexDocumentSuffix": "string",
        "RedirectAllRequestsTo": {
         "HostName": "string",
         "Protocol": "string"
        },
        "RoutingRules": [{
         "Condition": {
          "HttpErrorCodeReturnedEquals": "string",
          "KeyPrefixEquals": "string"
         },
         "Redirect": {
          "HostName": "string",
          "HttpRedirectCode": "string",
          "Protocol": "string",
          "ReplaceKeyPrefixWith": "string",
          "ReplaceKeyWith": "string"
         }
        }]
       },
       "CreatedAt": "string",
       "ObjectLockConfiguration": {
        "ObjectLockEnabled": "string",
        "Rule": {
         "DefaultRetention": {
          "Days": integer,
          "Mode": "string",
          "Years": integer
         }
        }
       },
       "OwnerAccountId": "string",
       "OwnerId": "string",
       "OwnerName": "string",
```

```
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "ServerSideEncryptionConfiguration": {
         "Rules": [{
          "ApplyServerSideEncryptionByDefault": {
           "KMSMasterKeyID": "string",
           "SSEAlgorithm": "string"
          }
         }]
        }
       },
       "AwsS3Object": {
        "ContentType": "string",
        "ETag": "string",
        "LastModified": "string",
        "ServerSideEncryption": "string",
        "SSEKMSKeyId": "string",
        "VersionId": "string"
       },
       "AwsSagemakerNotebookInstance": {
        "DirectInternetAccess": "string",
        "InstanceMetadataServiceConfiguration": {
         "MinimumInstanceMetadataServiceVersion": "string"
        },
        "InstanceType": "string",
        "LastModifiedTime": "string",
        "NetworkInterfaceId": "string",
        "NotebookInstanceArn": "string",
        "NotebookInstanceName": "string",
        "NotebookInstanceStatus": "string",
        "PlatformIdentifier": "string",
        "RoleArn": "string",
        "RootAccess": "string",
        "SecurityGroups": ["string"],
        "SubnetId": "string",
        "Url": "string",
        "VolumeSizeInGB": number
       },
       "AwsSecretsManagerSecret": {
        "Deleted": boolean,
```

```
        "Description": "string",
        "KmsKeyId": "string",
        "Name": "string",
        "RotationEnabled": boolean,
        "RotationLambdaArn": "string",
        "RotationOccurredWithinFrequency": boolean,
        "RotationRules": {
         "AutomaticallyAfterDays": integer
        }
       },
       "AwsSnsTopic": {
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
         "Endpoint": "string",
         "Protocol": "string"
        },
        "TopicName": "string"
       },
       "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
       },
       "AwsSsmPatchCompliance": {
        "Patch": {
         "ComplianceSummary": {
          "ComplianceType": "string",
          "CompliantCriticalCount": integer,
          "CompliantHighCount": integer,
          "CompliantInformationalCount": integer,
          "CompliantLowCount": integer,
          "CompliantMediumCount": integer,
          "CompliantUnspecifiedCount": integer,
          "ExecutionType": "string",
          "NonCompliantCriticalCount": integer,
```

```
        "NonCompliantHighCount": integer,
        "NonCompliantInformationalCount": integer,
        "NonCompliantLowCount": integer,
        "NonCompliantMediumCount": integer,
        "NonCompliantUnspecifiedCount": integer,
        "OverallSeverity": "string",
        "PatchBaselineId": "string",
        "PatchGroup": "string",
        "Status": "string"
       }
      }
     },
     "AwsStepFunctionStateMachine": {
      "StateMachineArn": "string",
      "Name": "string",
      "Status": "string",
      "RoleArn": "string",
      "Type": "string",
      "LoggingConfiguration": {
       "Level": "string",
       "IncludeExecutionData": boolean
      },
      "TracingConfiguration": {
       "Enabled": boolean
      }
     },
     "AwsWafRateBasedRule": {
      "MatchPredicates": [{
       "DataId": "string",
       "Negated": boolean,
       "Type": "string"
      }],
      "MetricName": "string",
      "Name": "string",
      "RateKey": "string",
      "RateLimit": number,
      "RuleId": "string"
     },
     "AwsWafRegionalRateBasedRule": {
      "MatchPredicates": [{
       "DataId": "string",
       "Negated": boolean,
       "Type": "string"
      }],
```

```
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
      },
      "AwsWafRegionalRule": {
        "MetricName": "string",
        "Name": "string",
        "RuleId": "string",
        "PredicateList": [{
            "DataId": "string",
            "Negated": boolean,
            "Type": "string"
        }]
      },
      "AwsWafRegionalRuleGroup": {
        "MetricName": "string",
        "Name": "string",
        "RuleGroupId": "string",
        "Rules": [{
          "Action": {
            "Type": "string"
          },
          "Priority": number,
          "RuleId": "string",
          "Type": "string"
        }]
      },
      "AwsWafRegionalWebAcl": {
        "DefaultAction": "string",
        "MetricName" : "string",
        "Name": "string",
        "RulesList" : [{
          "Action": {
            "Type": "string"
          },
          "Priority": number,
          "RuleId": "string",
          "Type": "string",
          "ExcludedRules": [{
            "ExclusionType": "string",
            "RuleId": "string"
          }],
```

```
        "OverrideAction": {
         "Type": "string"
        }
       }],
       "WebAclId": "string"
      },
      "AwsWafRule": {
       "MetricName": "string",
       "Name": "string",
       "PredicateList": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "RuleId": "string"
      },
      "AwsWafRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafv2RuleGroup": {
       "Arn": "string",
       "Capacity": number,
       "Description": "string",
       "Id": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
        "Allow": {
         "CustomRequestHandling": {
          "InsertHeaders": [
           {
           "Name": "string",
           "Value": "string"
           },
```

```
          {
          "Name": "string",
          "Value": "string"
          }
         ]
        }
       }
       },
       "Name": "string",
       "Priority": number,
       "VisibilityConfig": {
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string",
        "SampledRequestsEnabled": boolean
       }
      }],
      "VisibilityConfig": {
       "CloudWatchMetricsEnabled": boolean,
       "MetricName": "string",
       "SampledRequestsEnabled": boolean
      }
     },
     "AwsWafWebAcl": {
      "DefaultAction": "string",
      "Name": "string",
      "Rules": [{
       "Action": {
        "Type": "string"
       },
       "ExcludedRules": [{
        "RuleId": "string"
       }],
       "OverrideAction": {
        "Type": "string"
       },
       "Priority": number,
       "RuleId": "string",
       "Type": "string"
      }],
      "WebAclId": "string"
     },
     "AwsWafv2WebAcl": {
      "Arn": "string",
      "Capacity": number,
```

```
        "CaptchaConfig": {
         "ImmunityTimeProperty": {
          "ImmunityTime": number
         }
        },
        "DefaultAction": {
         "Block": {}
        },
        "Description": "string",
        "ManagedbyFirewallManager": boolean,
        "Name": "string",
        "Rules": [{
         "Action": {
          "RuleAction": {
           "Block": {}
          }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
          "SampledRequestsEnabled": boolean,
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string"
         }
        }],
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       },
       "AwsXrayEncryptionConfig": {
        "KeyId": "string",
        "Status": "string",
        "Type": "string"
       },
       "Container": {
        "ContainerRuntime": "string",
        "ImageId": "string",
        "ImageName": "string",
        "LaunchedAt": "string",
        "Name": "string",
        "Privileged": boolean,
        "VolumeMounts": [{
```

```
        "Name": "string",
        "MountPath": "string"
       }]
      },
      "Other": {
       "string": "string"
      },
      "Id": "string",
      "Partition": "string",
      "Region": "string",
      "ResourceRole": "string",
      "Tags": {
       "string": "string"
      },
      "Type": "string"
     }],
     "SchemaVersion": "string",
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Sample": boolean,
     "SourceUrl": "string",
     "Threats": [{
      "FilePaths": [{
       "FileName": "string",
       "FilePath": "string",
       "Hash": "string",
       "ResourceId": "string"
      }],
      "ItemCount": number,
      "Name": "string",
      "Severity": "string"
     }],
     "ThreatIntelIndicators": [{
      "Category": "string",
      "LastObservedAt": "string",
      "Source": "string",
      "SourceUrl": "string",
      "Type": "string",
      "Value": "string"
     }],
     "Title": "string",
```

```
      "Types": ["string"],
      "UpdatedAt": "string",
      "UserDefinedFields": {
       "string": "string"
      },
      "VerificationState": "string",
      "Vulnerabilities": [{
       "CodeVulnerabilities": [{
        "Cwes": [
         "string",
         "string"
        ],
        "FilePath": {
         "EndLine": integer,
         "FileName": "string",
         "FilePath": "string",
         "StartLine": integer
        },
        "SourceArn":"string"
       }],
       "Cvss": [{
        "Adjustments": [{
         "Metric": "string",
         "Reason": "string"
        }],
        "BaseScore": number,
        "BaseVector": "string",
        "Source": "string",
        "Version": "string"
       }],
       "EpssScore": number,
       "ExploitAvailable": "string",
       "FixAvailable": "string",
       "Id": "string",
       "LastKnownExploitAt": "string",
       "ReferenceUrls": ["string"],
       "RelatedVulnerabilities": ["string"],
       "Vendor": {
        "Name": "string",
        "Url": "string",
        "VendorCreatedAt": "string",
        "VendorSeverity": "string",
        "VendorUpdatedAt": "string"
       },
```

```
      "VulnerablePackages": [{
       "Architecture": "string",
       "Epoch": "string",
       "FilePath": "string",
       "FixedInVersion": "string",
       "Name": "string",
       "PackageManager": "string",
       "Release": "string",
       "Remediation": "string",
       "SourceLayerArn": "string",
       "SourceLayerHash": "string",
       "Version": "string"
      }]
     }],
     "Workflow": {
      "Status": "string"
     },
     "WorkflowState": "string"
    }
]
```

ASFF 필드 및 값에 대한 통합의 영향

Security Hub는 두 가지 유형의 통합을 제공합니다.

- 통합 제어 보기(항상 켜져 있음, 끌 수 없음) - 각 제어에는 표준 전반에 걸쳐 단일 식별자가 있습니다. Security Hub 콘솔의 제어 페이지에는 표준 전반의 모든 제어가 표시됩니다.
- 통합 제어 조사 결과(켜거나 끌 수 있음) - 통합 제어 조사 결과를 켜면 Security Hub는 검사가 여러 표준에서 공유되는 경우에도 보안 검사를 위한 단일 조사 결과를 생성합니다. 이는 결과 노이즈를 줄이기 위한 것입니다. 2023년 2월 23일 또는 그 이후에 Security Hub를 활성화한 경우 통합 제어 탐지 결과가 기본적으로 켜집니다. 그렇지 않으면 기본적으로 꺼져 있습니다. 하지만 통합 제어 조사 결과는 관리자 계정에서 설정된 경우에만 Security Hub 멤버 계정에서 활성화됩니다. 관리자 계정에서 이 기능을 끄면 멤버 계정에서도 해당 기능이 꺼집니다. 이 기능을 켜는 방법에 대한 지침은 통합 제어 조사 결과 활성화을 참조하십시오.

두 기능 모두 AWS 보안 검색 형식 (ASFF)에서 결과 필드 및 값을 제어하는 데 변경 사항을 가져옵니다. 이 섹션에서는 이러한 변경을 요약합니다.

통합 제어 보기 - ASFF 변경

통합 제어 보기 기능에는 ASFF의 검색 결과 필드 및 값을 제어하기 위해 다음과 같은 변경 사항이 도입되었습니다.

워크플로가 이러한 제어 결과 필드의 값을 사용하지 않는 경우 조치가 필요하지 않습니다.

이러한 제어 찾기 필드의 특정 값을 사용하는 워크플로가 있는 경우 현재 값을 사용하도록 워크플로를 업데이트하십시오.

ASFF 필드	통합 제어 보기 이전의 샘플 값	통합 제어 보기 이후의 샘플 값과 변경 설명
규정 준수. SecurityControlId	해당 없음 (새 필드)	EC2.2 표준 전체에 단일 제어 ID를 도입합니다. `ProductFields.RuleId` 는 여전히 CIS v1.2.0 제어에 대한 표준 기반 제어 ID를 제공합니다. `ProductFields.ControlId` 는 다른 표준의 제어에 대해 여전히 표준 기반 제어 ID를 제공합니다.
규정 준수. AssociatedStandards	해당 없음 (새 필드)	[{" StandardsId ": "표준/ aws-foundational-security-best -관행/ v/1.0.0"}] 제어가 활성화된 표준을 보여 줍니다.
ProductFields. ArchivalReasons. ----9월----:0/설명	해당 없음 (새 필드)	"통합 제어 조사 결과가 켜져 있거나 꺼졌

ASFF 필드	통합 제어 보기 이전의 샘플 값	통합 제어 보기 이후의 샘플 값과 변경 설명
		기 때문에 조사 결과는 ARCHIVED 상태입니다. 이로 인해 새 조사 결과가 생성될 때 이전 상태의 조사 결과가 보관됩니다." Security Hub가 기존 조사 결과를 보관하는 이유를 설명합니다.
ProductFields. ArchivalReasons. ----9월----:0/ ReasonCode	해당 없음 (새 필드)	"CONSOLID ATED_CONT ROL_FINDI NGS_UPDATE" Security Hub가 기존 조사 결과를 보관하는 이유를 제공합니다.
ProductFields.RecommendationUrl	https://docs.aws.a mazon.com/console/ securityhub/PCI.EC 2.2/remediation	https://docs.aws.a mazon.com/console/ securityhub/EC2.2/ remediation 이 필드는 더 이상 표준을 참조하지 않습니다.

ASFF 필드	통합 제어 보기 이전의 샘플 값	통합 제어 보기 이후의 샘플 값과 변경 설명
Remediation.Recommendation.Text	“이 문제를 해결하는 방법에 대한 지침은 AWS Security Hub PCI DSS 설명서를 참조하십시오.”	“이 문제를 해결하는 방법에 대한 지침은 AWS Security Hub 제어 설명서를 참조하십시오.” 이 필드는 더 이상 표준을 참조하지 않습니다.
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation 이 필드는 더 이상 표준을 참조하지 않습니다.

통합 제어 조사 결과 - ASFF 변경

통합 제어 조사 결과를 켜면 ASFF의 제어 조사 결과 필드 및 값에 대한 다음 변경 사항의 영향을 받을 수 있습니다. 이러한 변경은 통합 제어 보기에 대해 앞서 설명한 변경 사항에 추가된 것입니다.

워크플로가 이러한 제어 결과 필드의 값을 사용하지 않는 경우 조치가 필요하지 않습니다.

이러한 제어 찾기 필드의 특정 값을 사용하는 워크플로가 있는 경우 현재 값을 사용하도록 워크플로를 업데이트하십시오.

> **Note**
>
> AWS v2.0.0의 자동 보안 대응은 통합 제어 결과를 지원합니다. 이 버전의 솔루션을 사용하면 통합 제어 조사 결과를 활성화할 때 워크플로를 유지할 수 있습니다.

ASFF 필드	통합 제어 조사 결과를 활성화하기 전의 예제 값	통합 제어 조사 결과를 활성화한 후의 예제 값 및 변경 설명
GeneratorId	aws-foundational-security-best-프랙티스/V/1.0.0/구성.1	security-control/Config.1 이 필드는 더 이상 표준을 참조하지 않습니다.
Title	PCI.config.1을 활성화해야 합니다. AWS Config	AWS Config 활성화해야 합니다. 이 필드는 더 이상 표준별 정보를 참조하지 않습니다.
Id	arn:aws:securityhub:eu-central-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956	arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 이 필드는 더 이상 표준을 참조하지 않습니다.
ProductFields.ControlId	PCI.EC2.2	제거되었습니다. 대신 `Compliance.SecurityControlId` 을 참조하십시오. 이 필드는 표준에 구애받지 않는 단일 제어 ID를 위해 제거되었습니다.
ProductFields.RuleId	1.3	제거되었습니다. 대신 `Compliance.SecurityControlId` 을 참조하십시오. 이 필드는 표준에 구애받지 않는 단일 제어 ID를 위해 제거되었습니다.

ASFF 필드	통합 제어 조사 결과를 활성화하기 전의 예제 값	통합 제어 조사 결과를 활성화한 후의 예제 값 및 변경 설명
설명	이 PCI DSS AWS Config 컨트롤은 현재 계정 및 지역에서 활성화되었는지 여부를 확인합니다.	이 AWS AWS Config 컨트롤은 현재 계정 및 지역에서 활성화되었는지 여부를 확인합니다. 이 필드는 더 이상 표준을 참조하지 않습니다.

심각도	"Severity": {
	
	"Product": 90,
	
	"Label": "CRITICAL",
	
	"Normalized": 90,
	
	"Original": "CRITICAL"
	
	}
		"Severity": {
		
		"Label": "CRITICAL",
		
		"Normalized": 90,
		
		"Original": "CRITICAL"
		
		}
		
		Security Hub는 더 이상 제품 필드를 사용하여 검색 결과의 심각도를 설명하지 않습니다.

타입	["Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"]	["Software and Configuration Checks/Industry and Regulatory Standards"] 이 필드는 더 이상 표준을 참조하지 않습니다.

ASFF 필드	통합 제어 조사 결과를 활성화하기 전의 예제 값	통합 제어 조사 결과를 활성화한 후의 예제 값 및 변경 설명
규정 준수. RelatedRequirements	["PCI DSS 10.5.2", “PCI DSS 11.5", “CIS 파운데이션 2.5"] AWS	["PCI DSS v3.2.1/10.5.2", “PCI DSS v3.2.1/11.5", “CIS AWS 재단 벤치마크 v1.2.0/2.5"] 이 필드에는 사용 가능한 모든 표준의 관련 요구 사항이 표시됩니다.
CreatedAt	2022-05-05T08:18:13.138Z	2022-09-25T08:18:13.138Z 형식은 동일하게 유지되지만 통합 제어 결과를 켜면 값이 재설정됩니다.
FirstObservedAt	2022-05-07T08:18:13.138Z	2022-09-28T08:18:13.138Z 형식은 동일하게 유지되지만 통합 제어 결과를 켜면 값이 재설정됩니다.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	제거되었습니다. 대신 `Remediation.Recommendation.Url` 을 참조하십시오.
ProductFields.StandardsArn	arn:AWS:보안허브: ::표준/ -관행/ v/1.0.0 aws-foundational-security-best	제거되었습니다. 대신 `Compliance.AssociatedStandards` 을 참조하십시오.

ASFF 필드	통합 제어 조사 결과를 활성화하기 전의 예제 값	통합 제어 조사 결과를 활성화한 후의 예제 값 및 변경 설명
ProductFields.StandardsControlArn	arn:aws: 보안 허브: us-east-1:123456789012: 제어/ -Practices/V/1.0.0/config.1 aws-foundational-security-best	제거되었습니다. Security Hub는 표준 전반의 보안 검사에 대한 결과 하나를 생성합니다.
ProductFields.StandardsGuideArn	arn:aws:securityhub: ::ruleset/ /v/1.2.0 cis-aws-foundations-benchmark	제거되었습니다. 대신 `Compliance.AssociatedStandards` 을 참조하십시오.
ProductFields.StandardsGuideSubscriptionArn	arn:aws: 보안 허브: 미국 동부-2:123456789012:구독/ /v/1.2.0 cis-aws-foundations-benchmark	제거되었습니다. Security Hub는 표준 전반의 보안 검사에 대한 결과 하나를 생성합니다.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012:구독/ -practices/v/1.0.0 aws-foundational-security-best	제거되었습니다. Security Hub는 표준 전반의 보안 검사에 대한 결과 하나를 생성합니다.
ProductFields.aws/securityhub/ FindingId	arn:aws: 보안 허브: us-east-1:: 제품/AWS/보안 허브/arn: aws: 보안 허브: 미국 동부- 1:123456789012: 구독/ -Practices/v/1.0.0/config.1/finding/751C2173-7372-4E12-8656-A5210DFB1D67 aws-foundational-security-best	arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 이 필드는 더 이상 표준을 참조하지 않습니다.

통합 제어 결과를 활성화한 후의 고객 제공 ASFF 필드 값

통합 제어 조사 결과를 켜면 Security Hub는 표준 전반에 걸쳐 하나의 조사 결과를 생성하고 원래 조사 결과(각 표준에 대한 별도의 조사 결과)를 보관합니다. 보관된 조사 결과를 보려면 레코드 상태 필터를 ARCHIVED로 설정한 상태에서 Security Hub 콘솔의 조사 결과 페이지를 방문하거나 `GetFindings`

API 작업을 사용할 수 있습니다. Security Hub 콘솔에서 또는 BatchUpdateFindingsAPI를 사용하여 수행한 원본 검색 결과에 대한 업데이트는 새 검색 결과에 보존되지 않습니다. 필요한 경우 보관된 검색 결과를 참조하여 이 데이터를 복구할 수 있습니다.

고객이 입력한 ASFF 필드	통합 제어 조사 결과를 활성화한 후의 변경 내용 설명
신뢰도	빈 상태로 재설정합니다.
중요도	빈 상태로 재설정합니다.
참고	빈 상태로 재설정합니다.
RelatedFindings	빈 상태로 재설정합니다.
심각도	검색 결과의 기본 심각도(제어의 심각도와 일치)
타입	표준에 구애받지 않는 값으로 재설정합니다.
UserDefinedFields	빈 상태로 재설정합니다.
VerificationState	빈 상태로 재설정합니다.
워크플로	새로 실패한 조사 결과의 기본값은 NEW입니다. 새로 전달된 조사 결과의 기본값은 RESOLVED입니다.

통합 제어 조사 결과를 켜기 전과 후의 생성기 ID

통합 제어 조사 결과를 켜면 제어에 적용되는 생성기 ID 변경 목록은 다음과 같습니다. 이는 2023년 2월 15일 현재 Security Hub가 지원하는 제어에 적용됩니다.

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
arn:AWS:보안허브: ::규칙셋/ /v/1.2.0/rule/1.1 cis-aws-foundations-benchmark	보안 제어/ 1CloudWatch.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.10 cis-aws-foundations-benchmark	security-control/IAM.16

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.11 cis-aws-foundations-benchmark	security-control/IAM.17
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.12 cis-aws-foundations-benchmark	security-control/IAM.4
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.13 cis-aws-foundations-benchmark	security-control/IAM.9
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.14 cis-aws-foundations-benchmark	security-control/IAM.6
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.16 cis-aws-foundations-benchmark	security-control/IAM.2
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.2 cis-aws-foundations-benchmark	security-control/IAM.5
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.20 cis-aws-foundations-benchmark	security-control/IAM.18
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.22 cis-aws-foundations-benchmark	security-control/IAM.1
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.3 cis-aws-foundations-benchmark	security-control/IAM.8
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.4 cis-aws-foundations-benchmark	security-control/IAM.3
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.5 cis-aws-foundations-benchmark	security-control/IAM.11
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.6 cis-aws-foundations-benchmark	security-control/IAM.12
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.7 cis-aws-foundations-benchmark	security-control/IAM.13

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.8 cis-aws-foundations-benchmark	security-control/IAM.14
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/1.9 cis-aws-foundations-benchmark	security-control/IAM.15
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/2.1 cis-aws-foundations-benchmark	보안 제어/ 1CloudTrail.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/2.2 cis-aws-foundations-benchmark	보안 제어/ 4CloudTrail.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/2.3 cis-aws-foundations-benchmark	보안 제어/ 6CloudTrail.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/2.4 cis-aws-foundations-benchmark	보안 제어/ 5CloudTrail.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/2.5 cis-aws-foundations-benchmark	security-control/Config.1
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/2.6 cis-aws-foundations-benchmark	보안 제어/ 7CloudTrail.
arn:aws:보안 허브: ::규칙 세트/ /v/1.2.0/rule/2.7 cis-aws-foundations-benchmark	보안 제어/ 2CloudTrail.
arn:aws:보안 허브: ::규칙 세트/ /v/1.2.0/rule/2.8 cis-aws-foundations-benchmark	security-control/KMS.4
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/2.9 cis-aws-foundations-benchmark	security-control/EC2.6
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.1 cis-aws-foundations-benchmark	보안 제어/ 2CloudWatch.
arn:aws:보안 허브: ::규칙 세트/ /v/1.2.0/rule/3.2 cis-aws-foundations-benchmark	보안 제어/ 3CloudWatch.

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.3 cis-aws-foundations-benchmark	보안 제어/ 1CloudWatch.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.4 cis-aws-foundations-benchmark	보안 제어/ 4CloudWatch.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.5 cis-aws-foundations-benchmark	보안 제어/ 5CloudWatch.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.6 cis-aws-foundations-benchmark	보안 제어/ 6CloudWatch.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.7 cis-aws-foundations-benchmark	보안 제어/ 7CloudWatch.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.8 cis-aws-foundations-benchmark	보안 제어/ 8CloudWatch.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.9 cis-aws-foundations-benchmark	보안 제어/ 9CloudWatch.
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.10 cis-aws-foundations-benchmark	보안 제어/ CloudWatch 1.0
arn:aws:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.11 cis-aws-foundations-benchmark	보안 제어/ CloudWatch 1.1
arn:aws:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.12 cis-aws-foundations-benchmark	보안 제어/ CloudWatch 1.2
arn:aws:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/3.13 cis-aws-foundations-benchmark	보안 제어/ CloudWatch 1.3
arn:aws:보안 허브: ::규칙 세트/ /v/1.2.0/rule/3.14 cis-aws-foundations-benchmark	보안 제어/ CloudWatch 1.4
arn:aws:보안 허브: ::규칙 세트/ /v/1.2.0/rule/4.1 cis-aws-foundations-benchmark	security-control/EC2.13

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/4.2 cis-aws-foundations-benchmark	security-control/EC2.14
arn:AWS:보안 허브: ::규칙 세트/ /v/1.2.0/규칙/4.3 cis-aws-foundations-benchmark	security-control/EC2.2
cis-aws-foundations-benchmark/v/1.4.0/1.10	security-control/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	security-control/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	security-control/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	security-control/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	security-control/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	security-control/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	security-control/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	보안 제어/ 1CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/1.8	security-control/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1.9	security-control/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	security-control/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	security-control/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	security-control/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	security-control/EC2.7
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	security-control/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	보안 제어/ 1CloudTrail.
cis-aws-foundations-benchmark/v/1.4.0/3.2	보안 제어/ 4. CloudTrail

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
cis-aws-foundations-benchmark/v/1.4.0/3.4	보안 제어/ 5. CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.5	security-control/Config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	security-control/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	보안 제어/ 2. CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.8	security-control/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	security-control/EC2.6
cis-aws-foundations-benchmark/v/1.4.0/4.3	보안 제어/ 1CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4.4	보안 제어/ 4. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.5	보안 제어/ 5. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.6	보안 제어/ 6. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.7	보안 제어/ 7. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.8	보안 제어/ 8. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.9	보안 제어/ 9. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.10	보안 제어/ 1.0 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.11	보안 제어/ 1.1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.12	보안 제어/ 1.2 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.13	보안 제어/ 1.3 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.14	보안 제어/ 1.4 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/5.1	security-control/EC2.21
cis-aws-foundations-benchmark/v/1.4.0/5.3	security-control/EC2.2

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/v/1.0.0/계정.1	security-control/Account.1
aws-foundational-security-best-프랙티스/v/1.0.0/ACM.1	security-control/ACM.1
aws-foundational-security-best-프랙티스/v/1.0.0/API 게이트웨이.1	security-control/APIGateway.1
aws-foundational-security-best- 프랙티스/v/1.0.0/API 게이트웨이.2	security-control/APIGateway.2
aws-foundational-security-best- 프랙티스/v/1.0.0/API 게이트웨이.3	security-control/APIGateway.3
aws-foundational-security-best- 프랙티스/v/1.0.0/API 게이트웨이.4	security-control/APIGateway.4
aws-foundational-security-best- 프랙티스/v/1.0.0/API 게이트웨이.5	security-control/APIGateway.5
aws-foundational-security-best- 프랙티스/v/1.0.0/API 게이트웨이.8	security-control/APIGateway.8
aws-foundational-security-best- 프랙티스/v/1.0.0/API 게이트웨이.9	security-control/APIGateway.9
aws-foundational-security-best-프랙티스/v/1.0.0/ .1AutoScaling.	보안 제어/ 1AutoScaling.
aws-foundational-security-best-프랙티스/v/1.0.0/ 2AutoScaling.	보안 제어/ 2AutoScaling.
aws-foundational-security-best-프랙티스/v/1.0.0/ 3AutoScaling.	보안 제어/ 3AutoScaling.
aws-foundational-security-best-프랙티스/v/1.0.0/오토스케일링.5	security-control/Autoscaling.5

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/ v/1.0.0/ .6 AutoScaling	보안 제어/ 6AutoScaling.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 9AutoScaling.	보안 제어/ 9AutoScaling.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 1CloudFront.	보안 제어/ 1CloudFront.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 3CloudFront.	보안 제어/ 3CloudFront.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 4CloudFront.	보안 제어/ 4CloudFront.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 5CloudFront.	보안 제어/ 5CloudFront.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 6CloudFront.	보안 제어/ 6CloudFront.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 7CloudFront.	보안 제어/ 7CloudFront.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 8CloudFront.	보안 제어/ 8CloudFront.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 9CloudFront.	보안 제어/ 9CloudFront.
aws-foundational-security-best-프랙티스/ v/1.0.0/ 1.0 CloudFront	보안 제어/ 1.0 CloudFront
aws-foundational-security-best-프랙티스/ v/1.0.0/ 1.2 CloudFront	보안 제어/ 1.2 CloudFront
aws-foundational-security-best-프랙티스/ v/1.0.0/ 1CloudTrail.	보안 제어/ 1CloudTrail.

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/v/1.0.0/ 2CloudTrail.	보안 제어/ 2CloudTrail.
aws-foundational-security-best-프랙티스/v/1.0.0/ 4CloudTrail.	보안 제어/ 4CloudTrail.
aws-foundational-security-best-프랙티스/v/1.0.0/ 5CloudTrail.	보안 제어/ 5CloudTrail.
aws-foundational-security-best-프랙티스/v/1.0.0/ 1CodeBuild.	보안 제어/ 1CodeBuild.
aws-foundational-security-best-프랙티스/v/1.0.0/ 2CodeBuild.	보안 제어/ 2CodeBuild.
aws-foundational-security-best-프랙티스/v/1.0.0/ 3CodeBuild.	보안 제어/ 3CodeBuild.
aws-foundational-security-best-프랙티스/v/1.0.0/ 4CodeBuild.	보안 제어/ 4CodeBuild.
aws-foundational-security-best-프랙티스/V/1.0.0/구성.1	security-control/Config.1
aws-foundational-security-best-프랙티스/v/1.0.0/DMS.1	security-control/DMS.1
aws-foundational-security-best-프랙티스/V/1.0.0/다이나모드B.1	security-control/DynamoDB.1
aws-foundational-security-best-프랙티스/V/1.0.0/다이나모드B.2	security-control/DynamoDB.2
aws-foundational-security-best-프랙티스/V/1.0.0/다이나모드B.3	security-control/DynamoDB.3
aws-foundational-security-best- 프랙티스/v/1.0.0/EC2.1	security-control/EC2.1

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.3	security-control/EC2.3
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.4	security-control/EC2.4
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.6	security-control/EC2.6
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.7	security-control/EC2.7
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.8	security-control/EC2.8
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.9	security-control/EC2.9
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.10	security-control/EC2.10
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.15	security-control/EC2.15
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.16	security-control/EC2.16
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.17	security-control/EC2.17
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.18	security-control/EC2.18
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.19	security-control/EC2.19
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.2	security-control/EC2.2

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.20	security-control/EC2.20
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.21	security-control/EC2.21
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.23	security-control/EC2.23
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.24	security-control/EC2.24
aws-foundational-security-best-프랙티스/V/1.0.0/EC2.25	security-control/EC2.25
aws-foundational-security-best-프랙티스/V/1.0.0/ECR.1	security-control/ECR.1
aws-foundational-security-best-프랙티스/v/1.0.0/ECR.2	security-control/ECR.2
aws-foundational-security-best-프랙티스/v/1.0.0/ECR.3	security-control/ECR.3
aws-foundational-security-best-프랙티스/v/1.0.0/EC.1	security-control/ECS.1
aws-foundational-security-best-프랙티스/v/1.0.0/EC.10	security-control/ECS.10
aws-foundational-security-best-프랙티스/v/1.0.0/EC.12	security-control/ECS.12
aws-foundational-security-best-프랙티스/v/1.0.0/EC.2	security-control/ECS.2
aws-foundational-security-best-프랙티스/v/1.0.0/EC.3	security-control/ECS.3

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/v/1.0.0/EC.4	security-control/ECS.4
aws-foundational-security-best-프랙티스/v/1.0.0/EC.5	security-control/ECS.5
aws-foundational-security-best-프랙티스/v/1.0.0/EC.8	security-control/ECS.8
aws-foundational-security-best-프랙티스/V/1.0.0/EFS.1	security-control/EFS.1
aws-foundational-security-best-프랙티스/V/1.0.0/EFS.2	security-control/EFS.2
aws-foundational-security-best-프랙티스/V/1.0.0/EFS.3	security-control/EFS.3
aws-foundational-security-best-프랙티스/V/1.0.0/EFS.4	security-control/EFS.4
aws-foundational-security-best-프랙티스/V/1.0.0/EK.2	security-control/EKS.2
aws-foundational-security-best-프랙티스/v/1.0.0/ .1ElasticBeanstalk.	보안 제어/ 1ElasticBeanstalk.
aws-foundational-security-best-프랙티스/v/1.0.0/ 2ElasticBeanstalk.	보안 제어/ 2ElasticBeanstalk.
aws-foundational-security-best-프랙티스/V/1.0.0/ELBv2.1	security-control/ELB.1
aws-foundational-security-best-프랙티스/V/1.0.0/ELB.2	security-control/ELB.2
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.3	security-control/ELB.3

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.4	security-control/ELB.4
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.5	security-control/ELB.5
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.6	security-control/ELB.6
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.7	security-control/ELB.7
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.8	security-control/ELB.8
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.9	security-control/ELB.9
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.10	security-control/ELB.10
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.11	security-control/ELB.11
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.12	security-control/ELB.12
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.13	security-control/ELB.13
aws-foundational-security-best-프랙티스/v/1.0.0/ELB.14	security-control/ELB.14
aws-foundational-security-best-프랙티스/V/1.0.0/EMR.1	security-control/EMR.1
aws-foundational-security-best-프랙티스/V/1.0.0/ES.1	security-control/ES.1

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/V/1.0.0/ES.2	security-control/ES.2
aws-foundational-security-best-프랙티스/v/1.0.0/ES.3	security-control/ES.3
aws-foundational-security-best-프랙티스/v/1.0.0/ES.4	security-control/ES.4
aws-foundational-security-best-프랙티스/v/1.0.0/ES.5	security-control/ES.5
aws-foundational-security-best-프랙티스/v/1.0.0/ES.6	security-control/ES.6
aws-foundational-security-best-프랙티스/v/1.0.0/ES.7	security-control/ES.7
aws-foundational-security-best-프랙티스/v/1.0.0/ES.8	security-control/ES.8
aws-foundational-security-best-프랙티스/v/1.0.0/ .1GuardDuty.	보안 제어/ 1GuardDuty.
aws-foundational-security-best-프랙티스/v/1.0.0/IAM.1	security-control/IAM.1
aws-foundational-security-best-프랙티스/v/1.0.0/IAM.2	security-control/IAM.2
aws-foundational-security-best-프랙티스/v/1.0.0/IAM.21	security-control/IAM.21
aws-foundational-security-best-프랙티스/v/1.0.0/IAM.3	security-control/IAM.3
aws-foundational-security-best-프랙티스/v/1.0.0/IAM.4	security-control/IAM.4

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/v/1.0.0/IAM.5	security-control/IAM.5
aws-foundational-security-best-프랙티스/v/1.0.0/IAM.6	security-control/IAM.6
aws-foundational-security-best-프랙티스/v/1.0.0/IAM.7	security-control/IAM.7
aws-foundational-security-best-프랙티스/v/1.0.0/IAM.8	security-control/IAM.8
aws-foundational-security-best-프랙티스/V/1.0.0/키네시스.1	security-control/Kinesis.1
aws-foundational-security-best-프랙티스/v/1.0.0/kms.1	security-control/KMS.1
aws-foundational-security-best-프랙티스/v/1.0.0/kms.2	security-control/KMS.2
aws-foundational-security-best-프랙티스/v/1.0.0/kms.3	security-control/KMS.3
aws-foundational-security-best-프랙티스/V/1.0.0/람다.1	security-control/Lambda.1
aws-foundational-security-best-프랙티스/V/1.0.0/람다.2	security-control/Lambda.2
aws-foundational-security-best-프랙티스/V/1.0.0/람다.5	security-control/Lambda.5
aws-foundational-security-best-프랙티스/v/1.0.0/ 3NetworkFirewall.	보안 제어/ 3NetworkFirewall.
aws-foundational-security-best-프랙티스/v/1.0.0/ 4NetworkFirewall.	보안 제어/ 4NetworkFirewall.

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/v/1.0.0/ 5NetworkFirewall.	보안 제어/ 5NetworkFirewall.
aws-foundational-security-best-프랙티스/v/1.0.0/ 6NetworkFirewall.	보안 제어/ 6NetworkFirewall.
aws-foundational-security-best-프랙티스/v/1.0.0/오픈서치.1	security-control/Opensearch.1
aws-foundational-security-best- 프랙티스/v/1.0.0/오픈서치.2	security-control/Opensearch.2
aws-foundational-security-best- 프랙티스/v/1.0.0/오픈서치.3	security-control/Opensearch.3
aws-foundational-security-best- 프랙티스/v/1.0.0/오픈서치.4	security-control/Opensearch.4
aws-foundational-security-best- 프랙티스/v/1.0.0/오픈서치.5	security-control/Opensearch.5
aws-foundational-security-best- 프랙티스/v/1.0.0/오픈서치.6	security-control/Opensearch.6
aws-foundational-security-best- 프랙티스/v/1.0.0/오픈서치.7	security-control/Opensearch.7
aws-foundational-security-best- 프랙티스/v/1.0.0/오픈서치.8	security-control/Opensearch.8
aws-foundational-security-best- 프랙티스/v/1.0.0/RDS.1	security-control/RDS.1
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.10	security-control/RDS.10
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.11	security-control/RDS.11

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.12	security-control/RDS.12
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.13	security-control/RDS.13
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.14	security-control/RDS.14
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.15	security-control/RDS.15
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.16	security-control/RDS.16
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.17	security-control/RDS.17
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.18	security-control/RDS.18
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.19	security-control/RDS.19
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.2	security-control/RDS.2
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.20	security-control/RDS.20
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.21	security-control/RDS.21
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.22	security-control/RDS.22
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.23	security-control/RDS.23

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.24	security-control/RDS.24
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.25	security-control/RDS.25
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.3	security-control/RDS.3
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.4	security-control/RDS.4
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.5	security-control/RDS.5
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.6	security-control/RDS.6
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.7	security-control/RDS.7
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.8	security-control/RDS.8
aws-foundational-security-best-프랙티스/v/1.0.0/RDS.9	security-control/RDS.9
aws-foundational-security-best-프랙티스/V/1.0.0/레드시프트.1	security-control/Redshift.1
aws-foundational-security-best-프랙티스/V/1.0.0/레드시프트.2	security-control/Redshift.2
aws-foundational-security-best-프랙티스/V/1.0.0/레드시프트.3	security-control/Redshift.3
aws-foundational-security-best-프랙티스/V/1.0.0/레드시프트.4	security-control/Redshift.4

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/V/1.0.0/레드시프트.6	security-control/Redshift.6
aws-foundational-security-best-프랙티스/V/1.0.0/레드시프트.7	security-control/Redshift.7
aws-foundational-security-best-프랙티스/V/1.0.0/레드시프트.8	security-control/Redshift.8
aws-foundational-security-best-프랙티스/V/1.0.0/레드시프트.9	security-control/Redshift.9
aws-foundational-security-best- 프랙티스/v/1.0.0/S3.1	security-control/S3.1
aws-foundational-security-best-프랙티스/V/1.0.0/S3.12	security-control/S3.12
aws-foundational-security-best-프랙티스/V/1.0.0/S3.13	security-control/S3.13
aws-foundational-security-best-프랙티스/V/1.0.0/S3.2	security-control/S3.2
aws-foundational-security-best-프랙티스/V/1.0.0/S3.3	security-control/S3.3
aws-foundational-security-best-프랙티스/V/1.0.0/S3.5	security-control/S3.5
aws-foundational-security-best-프랙티스/V/1.0.0/S3.6	security-control/S3.6
aws-foundational-security-best-프랙티스/V/1.0.0/S3.8	security-control/S3.8
aws-foundational-security-best-프랙티스/V/1.0.0/S3.9	security-control/S3.9

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/v/1.0.0/ .1SageMaker.	보안 제어/ 1SageMaker.
aws-foundational-security-best-프랙티스/v/1.0.0/ 2SageMaker.	보안 제어/ 2SageMaker.
aws-foundational-security-best-프랙티스/v/1.0.0/ 3SageMaker.	보안 제어/ 3SageMaker.
aws-foundational-security-best-프랙티스/v/1.0.0/ 1SecretsManager.	보안 제어/ 1SecretsManager.
aws-foundational-security-best-프랙티스/v/1.0.0/ 2SecretsManager.	보안 제어/ 2SecretsManager.
aws-foundational-security-best-프랙티스/v/1.0.0/ 3SecretsManager.	보안 제어/ 3SecretsManager.
aws-foundational-security-best-프랙티스/v/1.0.0/ 4SecretsManager.	보안 제어/ 4SecretsManager.
aws-foundational-security-best-프랙티스/V/1.0.0/SQS.1	security-control/SQS.1
aws-foundational-security-best-프랙티스/V/1.0.0/SSM.1	security-control/SSM.1
aws-foundational-security-best-프랙티스/v/1.0.0/SSM.2	security-control/SSM.2
aws-foundational-security-best-프랙티스/v/1.0.0/SSM.3	security-control/SSM.3
aws-foundational-security-best-프랙티스/v/1.0.0/SSM.4	security-control/SSM.4
aws-foundational-security-best-프랙티스/v/1.0.0/WAF.1	security-control/WAF.1

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
aws-foundational-security-best-프랙티스/V/1.0.0/WAF.2	security-control/WAF.2
aws-foundational-security-best-프랙티스/v/1.0.0/WAF.3	security-control/WAF.3
aws-foundational-security-best-프랙티스/v/1.0.0/WAF.4	security-control/WAF.4
aws-foundational-security-best-프랙티스/V/1.0.0/WAF.6	security-control/WAF.6
aws-foundational-security-best-프랙티스/V/1.0.0/WAF.7	security-control/WAF.7
aws-foundational-security-best-프랙티스/V/1.0.0/WAF.8	security-control/WAF.8
aws-foundational-security-best-프랙티스/v/1.0.0/WAF.10	security-control/WAF.10
PCI-DSS/V/3.2.1/PCI. AutoScaling1.	보안 제어/ 1. AutoScaling
PCI-DSS/V/3.2.1/PCI. CloudTrail1.	보안 제어/ 2. CloudTrail
PCI-DSS/V/3.2.1/PCI. CloudTrail2.	보안 제어/ 3CloudTrail.
PCI-DSS/V/3.2.1/PCI. CloudTrail3.	보안 제어/ 4CloudTrail.
PCI-DSS/V/3.2.1/PCI. CloudTrail4.	보안 제어/ 5CloudTrail.
PCI-DSS/V/3.2.1/PCI. CodeBuild1.	보안 제어/ 1. CodeBuild
PCI-DSS/V/3.2.1/PCI. CodeBuild2.	보안 제어/ 2CodeBuild.
pci-dss/v/3.2.1/PCI.Config.1	security-control/Config.1
pci-dss/v/3.2.1/PCI.CW.1	보안 제어/ 1CloudWatch.

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
pci-dss/v/3.2.1/PCI.DMS.1	security-control/DMS.1
pci-dss/v/3.2.1/PCI.EC2.1	security-control/EC2.1
pci-dss/v/3.2.1/PCI.EC2.2	security-control/EC2.2
pci-dss/v/3.2.1/PCI.EC2.4	security-control/EC2.12
pci-dss/v/3.2.1/PCI.EC2.5	security-control/EC2.13
pci-dss/v/3.2.1/PCI.EC2.6	security-control/EC2.6
pci-dss/v/3.2.1/PCI.ELBv2.1	security-control/ELB.1
pci-dss/v/3.2.1/PCI.ES.1	security-control/ES.2
pci-dss/v/3.2.1/PCI.ES.2	security-control/ES.1
PCI-DSS/V/3.2.1/PCI. GuardDuty1.	보안 제어/ 1. GuardDuty
pci-dss/v/3.2.1/PCI.IAM.1	security-control/IAM.4
pci-dss/v/3.2.1/PCI.IAM.2	security-control/IAM.2
pci-dss/v/3.2.1/PCI.IAM.3	security-control/IAM.1
pci-dss/v/3.2.1/PCI.IAM.4	security-control/IAM.6
pci-dss/v/3.2.1/PCI.IAM.5	security-control/IAM.9
pci-dss/v/3.2.1/PCI.IAM.6	security-control/IAM.19
pci-dss/v/3.2.1/PCI.IAM.7	security-control/IAM.8
pci-dss/v/3.2.1/PCI.IAM.8	security-control/IAM.10
pci-dss/v/3.2.1/PCI.KMS.1	security-control/KMS.4
pci-dss/v/3.2.1/PCI.Lambda.1	security-control/Lambda.1

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
pci-dss/v/3.2.1/PCI.Lambda.2	security-control/Lambda.3
pci-dss/v/3.2.1/PCI.Opensearch.1	security-control/Opensearch.2
pci-dss/v/3.2.1/PCI.Opensearch.2	security-control/Opensearch.1
pci-dss/v/3.2.1/PCI.RDS.1	security-control/RDS.1
pci-dss/v/3.2.1/PCI.RDS.2	security-control/RDS.2
pci-dss/v/3.2.1/PCI.Redshift.1	security-control/Redshift.1
pci-dss/v/3.2.1/PCI.S3.1	security-control/S3.3
pci-dss/v/3.2.1/PCI.S3.2	security-control/S3.2
pci-dss/v/3.2.1/PCI.S3.3	security-control/S3.7
pci-dss/v/3.2.1/PCI.S3.5	security-control/S3.5
pci-dss/v/3.2.1/PCI.S3.6	security-control/S3.1
PCI-DSS/V/3.2.1/PCI. SageMaker1.	보안 제어/ 1. SageMaker
pci-dss/v/3.2.1/PCI.SSM.1	security-control/SSM.2
pci-dss/v/3.2.1/PCI.SSM.2	security-control/SSM.3
pci-dss/v/3.2.1/PCI.SSM.3	security-control/SSM.1
service-managed-aws-control-타워/V/1.0.0/ACM.1	security-control/ACM.1
service-managed-aws-control-타워/V/1.0.0/API 게이트웨이.1	security-control/APIGateway.1
service-managed-aws-control-타워/V/1.0.0/API 게이트웨이.2	security-control/APIGateway.2

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/V/1.0.0/API 게이트웨이.3	security-control/APIGateway.3
service-managed-aws-control-타워/V/1.0.0/API 게이트웨이.4	security-control/APIGateway.4
service-managed-aws-control-타워/V/1.0.0/아피 게이트웨이.5	security-control/APIGateway.5
service-managed-aws-controlAutoScaling-타워/v/1.0.0/ 1.	보안 제어/ 1AutoScaling.
service-managed-aws-control-타워/v/1.0.0/ 2AutoScaling.	보안 제어/ 2AutoScaling.
service-managed-aws-control-타워/v/1.0.0/ 3AutoScaling.	보안 제어/ 3AutoScaling.
service-managed-aws-control-타워/v/1.0.0/ 4AutoScaling.	보안 제어/ 4AutoScaling.
service-managed-aws-control-타워/V/1.0.0/오토 스케일링.5	security-control/Autoscaling.5
service-managed-aws-controlAutoScaling-타워/v/1.0.0/ 6.	보안 제어/ 6AutoScaling.
service-managed-aws-control-타워/v/1.0 .0/9AutoScaling.	보안 제어/ 9AutoScaling.
service-managed-aws-control-타워/v/1.0.0/ 1CloudTrail.	보안 제어/ 1CloudTrail.
service-managed-aws-control-타워/v/1.0.0/ 2CloudTrail.	보안 제어/ 2CloudTrail.
service-managed-aws-control-타워/v/1.0.0/ 4CloudTrail.	보안 제어/ 4CloudTrail.

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/v/1.0.0/5CloudTrail.	보안 제어/ 5CloudTrail.
service-managed-aws-control-타워/v/1.0.0/1CodeBuild.	보안 제어/ 1CodeBuild.
service-managed-aws-control-타워/v/1.0.0/2CodeBuild.	보안 제어/ 2CodeBuild.
service-managed-aws-control-타워/v/1.0.0/4CodeBuild.	보안 제어/ 4CodeBuild.
service-managed-aws-control-타워/v/1.0.0/5CodeBuild.	보안 제어/ 5CodeBuild.
service-managed-aws-control-타워/V/1.0.0/DMS.1	security-control/DMS.1
service-managed-aws-control-타워/V/1.0.0/다이나모드B.1	security-control/DynamoDB.1
service-managed-aws-control-타워/V/1.0.0/다이나모드B.2	security-control/DynamoDB.2
service-managed-aws-control-타워/V/1.0.0/EC2.1	security-control/EC2.1
service-managed-aws-control-타워/V/1.0.0/EC2.2	security-control/EC2.2
service-managed-aws-control-타워/V/1.0.0/EC2.3	security-control/EC2.3
service-managed-aws-control-타워/V/1.0.0/EC2.4	security-control/EC2.4
service-managed-aws-control-타워/V/1.0.0/EC2.6	security-control/EC2.6

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/V/1.0.0/EC2.7	security-control/EC2.7
service-managed-aws-control-타워/V/1.0.0/EC2.8	security-control/EC2.8
service-managed-aws-control-타워/V/1.0.0/EC2.9	security-control/EC2.9
service-managed-aws-control-타워/V/1.0.0/EC2.10	security-control/EC2.10
service-managed-aws-control-타워/V/1.0.0/EC2.15	security-control/EC2.15
service-managed-aws-control-타워/V/1.0.0/EC2.16	security-control/EC2.16
service-managed-aws-control-타워/V/1.0.0/EC2.17	security-control/EC2.17
service-managed-aws-control-타워/V/1.0.0/EC2.18	security-control/EC2.18
service-managed-aws-control-타워/V/1.0.0/EC2.19	security-control/EC2.19
service-managed-aws-control-타워/V/1.0.0/EC2.20	security-control/EC2.20
service-managed-aws-control-타워/V/1.0.0/EC2.21	security-control/EC2.21
service-managed-aws-control-타워/V/1.0.0/EC2.22	security-control/EC2.22
service-managed-aws-control-타워/V/1.0.0/ECR.1	security-control/ECR.1

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/V/1.0.0/ECR.2	security-control/ECR.2
service-managed-aws-control-타워/V/1.0.0/ECR.3	security-control/ECR.3
service-managed-aws-control-타워/V/1.0.0/EC.1	security-control/ECS.1
service-managed-aws-control-타워/V/1.0.0/EC.2	security-control/ECS.2
service-managed-aws-control-타워/V/1.0.0/EC.3	security-control/ECS.3
service-managed-aws-control-타워/V/1.0.0/EC.4	security-control/ECS.4
service-managed-aws-control-타워/V/1.0.0/EC.5	security-control/ECS.5
service-managed-aws-control-타워/V/1.0.0/EC.8	security-control/ECS.8
service-managed-aws-control-타워/V/1.0.0/EC.10	security-control/ECS.10
service-managed-aws-control-타워/V/1.0.0/EC.12	security-control/ECS.12
service-managed-aws-control-타워/V/1.0.0/EFS.1	security-control/EFS.1
service-managed-aws-control-타워/V/1.0.0/EFS.2	security-control/EFS.2
service-managed-aws-control-타워/V/1.0.0/EFS.3	security-control/EFS.3

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/V/1.0.0/EFS.4	security-control/EFS.4
service-managed-aws-control-타워/V/1.0.0/EK.2	security-control/EKS.2
service-managed-aws-control-타워/V/1.0.0/엘브.2	security-control/ELB.2
service-managed-aws-control-타워/V/1.0.0/엘브.3	security-control/ELB.3
service-managed-aws-control-타워/V/1.0.0/엘브.4	security-control/ELB.4
service-managed-aws-control-타워/V/1.0.0/엘브.5	security-control/ELB.5
service-managed-aws-control-타워/V/1.0.0/엘브.6	security-control/ELB.6
service-managed-aws-control-타워/V/1.0.0/엘브.7	security-control/ELB.7
service-managed-aws-control-타워/V/1.0.0/엘브.8	security-control/ELB.8
service-managed-aws-control-타워/V/1.0.0/엘브.9	security-control/ELB.9
service-managed-aws-control-타워/V/1.0.0/엘브.10	security-control/ELB.10
service-managed-aws-control-타워/V/1.0.0/엘브.12	security-control/ELB.12
service-managed-aws-control-타워/V/1.0.0/엘브.13	security-control/ELB.13

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/V/1.0.0/엘브.14	security-control/ELB.14
service-managed-aws-control-타워/V/1.0.0/ELBV2.1	security-control/ELBv2.1
service-managed-aws-control-타워/V/1.0.0/EMR.1	security-control/EMR.1
service-managed-aws-control-타워/V/1.0.0/ES.1	security-control/ES.1
service-managed-aws-control-타워/V/1.0.0/ES.2	security-control/ES.2
service-managed-aws-control-타워/V/1.0.0/ES.3	security-control/ES.3
service-managed-aws-control-타워/V/1.0.0/ES.4	security-control/ES.4
service-managed-aws-control-타워/V/1.0.0/ES.5	security-control/ES.5
service-managed-aws-control-타워/V/1.0.0/ES.6	security-control/ES.6
service-managed-aws-control-타워/V/1.0.0/ES.7	security-control/ES.7
service-managed-aws-control-타워/V/1.0.0/ES.8	security-control/ES.8
service-managed-aws-controlElasticBeanstalk-타워/v/1.0.0/ .1.	보안 제어/ 1ElasticBeanstalk.
service-managed-aws-control-타워/v/1.0.0/2ElasticBeanstalk.	보안 제어/ 2ElasticBeanstalk.

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/v/1.0.0/1GuardDuty.	보안 제어/ 1GuardDuty.
service-managed-aws-control-타워/V/1.0.0/IAM.1	security-control/IAM.1
service-managed-aws-control-타워/V/1.0.0/IAM.2	security-control/IAM.2
service-managed-aws-control-타워/V/1.0.0/IAM.3	security-control/IAM.3
service-managed-aws-control-타워/V/1.0.0/IAM.4	security-control/IAM.4
service-managed-aws-control-타워/V/1.0.0/IAM.5	security-control/IAM.5
service-managed-aws-control-타워/V/1.0.0/IAM.6	security-control/IAM.6
service-managed-aws-control-타워/V/1.0.0/IAM.7	security-control/IAM.7
service-managed-aws-control-타워/V/1.0.0/IAM.8	security-control/IAM.8
service-managed-aws-control-타워/V/1.0.0/IAM.21	security-control/IAM.21
service-managed-aws-control-타워/V/1.0.0/키네시스.1	security-control/Kinesis.1
service-managed-aws-control-타워/V/1.0.0/kms.1	security-control/KMS.1
service-managed-aws-control-타워/V/1.0.0/kms.2	security-control/KMS.2

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/V/1.0.0/kms.3	security-control/KMS.3
service-managed-aws-control-타워/V/1.0.0/람다.1	security-control/Lambda.1
service-managed-aws-control-타워/V/1.0.0/람다.2	security-control/Lambda.2
service-managed-aws-control-타워/V/1.0.0/람다.5	security-control/Lambda.5
service-managed-aws-controlNetworkFirewall-타워/v/1.0.0/ 3.	보안 제어/ 3NetworkFirewall.
service-managed-aws-control-타워/v/1.0.0/4NetworkFirewall.	보안 제어/ 4NetworkFirewall.
service-managed-aws-control-타워/v/1.0.0/5NetworkFirewall.	보안 제어/ 5NetworkFirewall.
service-managed-aws-control-타워/v/1.0.0/6NetworkFirewall.	보안 제어/ 6NetworkFirewall.
service-managed-aws-control-타워/V/1.0.0/오픈서치.1	security-control/Opensearch.1
service-managed-aws-control-타워/V/1.0.0/오픈서치.2	security-control/Opensearch.2
service-managed-aws-control-타워/V/1.0.0/오픈서치.3	security-control/Opensearch.3
service-managed-aws-control-타워/V/1.0.0/오픈서치.4	security-control/Opensearch.4
service-managed-aws-control-타워/V/1.0.0/오픈서치.5	security-control/Opensearch.5

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/V/1.0.0/오픈서치.6	security-control/Opensearch.6
service-managed-aws-control-타워/V/1.0.0/오픈서치.7	security-control/Opensearch.7
service-managed-aws-control-타워/V/1.0.0/오픈서치.8	security-control/Opensearch.8
service-managed-aws-control-타워/V/1.0.0/RDS.1	security-control/RDS.1
service-managed-aws-control-타워/V/1.0.0/RDS.2	security-control/RDS.2
service-managed-aws-control-타워/V/1.0.0/RDS.3	security-control/RDS.3
service-managed-aws-control-타워/V/1.0.0/RDS.4	security-control/RDS.4
service-managed-aws-control-타워/V/1.0.0/RDS.5	security-control/RDS.5
service-managed-aws-control-타워/V/1.0.0/RDS.6	security-control/RDS.6
service-managed-aws-control-타워/V/1.0.0/RDS.8	security-control/RDS.8
service-managed-aws-control-타워/V/1.0.0/RDS.9	security-control/RDS.9
service-managed-aws-control-타워/V/1.0.0/RDS.10	security-control/RDS.10
service-managed-aws-control-타워/V/1.0.0/RDS.11	security-control/RDS.11

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/V/1.0.0/RDS.13	security-control/RDS.13
service-managed-aws-control-타워/V/1.0.0/RDS.17	security-control/RDS.17
service-managed-aws-control-타워/V/1.0.0/RDS.18	security-control/RDS.18
service-managed-aws-control-타워/V/1.0.0/RDS.19	security-control/RDS.19
service-managed-aws-control-타워/V/1.0.0/RDS.20	security-control/RDS.20
service-managed-aws-control-타워/V/1.0.0/RDS.21	security-control/RDS.21
service-managed-aws-control-타워/V/1.0.0/RDS.22	security-control/RDS.22
service-managed-aws-control-타워/V/1.0.0/RDS.23	security-control/RDS.23
service-managed-aws-control-타워/V/1.0.0/RDS.25	security-control/RDS.25
service-managed-aws-control-타워/V/1.0.0/레드시프트.1	security-control/Redshift.1
service-managed-aws-control-타워/V/1.0.0/레드시프트.2	security-control/Redshift.2
service-managed-aws-control-타워/V/1.0.0/레드시프트.4	security-control/Redshift.4
service-managed-aws-control-타워/V/1.0.0/레드시프트.6	security-control/Redshift.6

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/V/1.0.0/레드시프트.7	security-control/Redshift.7
service-managed-aws-control-타워/V/1.0.0/레드시프트.8	security-control/Redshift.8
service-managed-aws-control-타워/V/1.0.0/레드시프트.9	security-control/Redshift.9
service-managed-aws-control-타워/V/1.0.0/S3.1	security-control/S3.1
service-managed-aws-control-타워/V/1.0.0/S3.2	security-control/S3.2
service-managed-aws-control-타워/V/1.0.0/S3.3	security-control/S3.3
service-managed-aws-control-타워/V/1.0.0/S3.5	security-control/S3.5
service-managed-aws-control-타워/V/1.0.0/S3.6	security-control/S3.6
service-managed-aws-control-타워/V/1.0.0/S3.8	security-control/S3.8
service-managed-aws-control-타워/V/1.0.0/S3.9	security-control/S3.9
service-managed-aws-control-타워/V/1.0.0/S3.12	security-control/S3.12
service-managed-aws-control-타워/V/1.0.0/S3.13	security-control/S3.13
service-managed-aws-controlSageMaker-타워/v/1.0.0/ .1.	보안 제어/ 1SageMaker.

통합 제어 조사 결과를 켜기 전의 생성기 ID	통합 제어 조사 결과를 켠 후의 생성기 ID
service-managed-aws-control-타워/v/1.0.0/1SecretsManager.	보안 제어/ 1SecretsManager.
service-managed-aws-control-타워/v/1.0.0/2SecretsManager.	보안 제어/ 2SecretsManager.
service-managed-aws-control-타워/v/1.0.0/3SecretsManager.	보안 제어/ 3SecretsManager.
service-managed-aws-control-타워/v/1.0.0/4SecretsManager.	보안 제어/ 4SecretsManager.
service-managed-aws-control-타워/V/1.0.0/스퀘어.1	security-control/SQS.1
service-managed-aws-control-타워/V/1.0.0/SSM.1	security-control/SSM.1
service-managed-aws-control-타워/V/1.0.0/SSM.2	security-control/SSM.2
service-managed-aws-control-타워/V/1.0.0/SSM.3	security-control/SSM.3
service-managed-aws-control-타워/V/1.0.0/SSM.4	security-control/SSM.4
service-managed-aws-control-타워/V/1.0.0/WAF.2	security-control/WAF.2
service-managed-aws-control-타워/V/1.0.0/WAF.3	security-control/WAF.3
service-managed-aws-control-타워/V/1.0.0/WAF.4	security-control/WAF.4

통합이 제어 ID 및 제목에 미치는 영향

통합 제어 보기 및 통합 제어 조사 결과는 표준 전반에 걸쳐 제어 ID 및 제목을 표준화합니다. 보안 제어 ID 및 보안 제어 제목이라는 용어는 이러한 표준에 구애받지 않는 값을 나타냅니다. 다음 테이블은 보안 제어 ID 및 제목과 표준별 제어 ID 및 제목의 매핑을 보여줍니다. 기본 보안 모범 사례 (FSBP) 표준에 속하는 컨트롤의 ID 및 제목은 변경되지 않았습니다. AWS

Security Hub 콘솔에는 계정에서 통합 제어 결과가 켜져 있는지 또는 사용 중지되었는지에 관계없이 표준에 구애받지 않는 보안 제어 ID와 보안 제어 제목이 표시됩니다. 하지만 계정에서 통합 제어 결과가 해제된 경우 Security Hub 조사 결과에는 표준별 제어 제목 (PCI 및 CIS v1.2.0용) 이 포함됩니다. 계정에서 통합 제어 탐지 결과가 해제된 경우 Security Hub 검색 결과에는 표준별 제어 ID와 보안 제어 ID가 포함됩니다. 통합이 제어 조사 결과에 미치는 영향에 대한 자세한 내용은 샘플 제어 조사 결과을 참조하십시오.

서비스 관리형 표준에 속하는 컨트롤의 경우 통합 제어 결과를 켜면 검색 결과의 제어 ID 및 제목에서 접두사가 `CT.` 제거됩니다. AWS Control Tower

이 테이블에서 스크립트를 직접 실행하려면 .csv 파일로 다운로드하십시오.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
CIS v1.2.0	1.1 루트 사용자의 사용을 피합니다.	[CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.
CIS v1.2.0	1.10 IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.	[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
CIS v1.2.0	1.11 IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.	[IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
CIS v1.2.0	1.12 루트 사용자 액세스 키가 없는지 여부를 확인합니다.	[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
CIS v1.2.0	1.13 루트 사용자에 대해 MFA가 활성화되어 있는지 여부를 확인합니다.	[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
CIS v1.2.0	1.14 루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 여부를 확인합니다.	[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
CIS v1.2.0	1.16 IAM 정책이 그룹 또는 역할에만 연결되어 있는지 여부를 확인합니다.	[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
CIS v1.2.0	1.2 콘솔 암호가 있는 모든 IAM 사용자에 대해 다중 인증(MFA)이 활성화되었는지 여부를 확인합니다.	[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
CIS v1.2.0	1.20 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support	[IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
CIS v1.2.0	1.22 전체 "*:*" 관리 권한을 허용하는 IAM 정책이 생성되지 않았는지 확인합니다.	[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
CIS v1.2.0	1.3 90일 이상 사용하지 않은 자격 증명이 비활성화되어 있는지 여부를 확인합니다.	[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
CIS v1.2.0	1.4 90일이 되기 전에 액세스 키가 교체되는지 여부를 확인합니다.	[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
CIS v1.2.0	1.5 IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.	[IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
CIS v1.2.0	1.6 IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.	[IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
CIS v1.2.0	1.7 IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.	[IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
CIS v1.2.0	1.8 IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.	[IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
CIS v1.2.0	1.9 IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.	[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
CIS v1.2.0	2.1 모든 지역에서 CloudTrail 활성화되었는지 확인	[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.
CIS v1.2.0	2.2 CloudTrail 로그 파일 검증이 활성화되었는지 확인	[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.
CIS v1.2.0	2.3 CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인	[CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.
CIS v1.2.0	2.4 CloudTrail 트레일이 로그와 CloudWatch 통합되었는지 확인	[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch
CIS v1.2.0	2.5 AWS Config 활성화되었는지 확인	[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.
CIS v1.2.0	2.6 S3 CloudTrail 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인	[CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail
CIS v1.2.0	2.7 KMS CMK를 사용하여 유휴 상태의 CloudTrail 로그를 암호화해야 합니다.	[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.
CIS v1.2.0	2.8 고객이 생성한 CMK에 대한 교체가 활성화되었는지 확인합니다.	[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
CIS v1.2.0	2.9 모든 VPC에서 VPC 흐름 로깅이 활성화되어 있는지 확인합니다.	[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.
CIS v1.2.0	3.1 무단 API 호출에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.2] 승인되지 않은 API 호출에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	3.10 보안 그룹 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.10] 보안 그룹 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	3.11 네트워크 액세스 제어 목록 (NACL) 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.11] 네트워크 액세스 제어 목록 (NACL) 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	3.12 네트워크 게이트웨이 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.12] 네트워크 게이트웨이 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	3.13 라우팅 테이블 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.13] 라우팅 테이블 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	3.14 VPC 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.14] VPC 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인
CIS v1.2.0	3.2 MFA 없는 로그인에 대해 관리 콘솔에 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.3] MFA를 사용하지 않는 관리 콘솔 로그인에 대한 로그 메트릭 필터 및 경보가 있는지 확인
CIS v1.2.0	3.3 루트 사용자 사용을 위한 로그 지표 필터 및 경보가 있는지 확인합니다.	[CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
CIS v1.2.0	3.4 IAM 정책 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.4] IAM 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	3.5 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인 CloudTrail	[CloudWatch.5] 기간 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오 CloudTrail AWS Config.
CIS v1.2.0	3.6 AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 존재하는지 확인	[CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	3.7 고객 생성 CMK 활성화 또는 예약된 삭제에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제를 위한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	3.8 S3 버킷 정책 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.8] S3 버킷 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	3.9 구성 변경에 대한 AWS Config 로그 메트릭 필터 및 경보가 존재하는지 확인	[CloudWatch.9] AWS Config 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.2.0	4.1 어떤 보안 그룹에서도 0.0.0.0/0에서 포트 22로의 수신을 허용하지 않는지 여부를 확인합니다.	[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
CIS v1.2.0	4.2 어떤 보안 그룹에서도 0.0.0.0/0에서 포트 3389로의 수신을 허용하지 않는지 여부를 확인합니다.	[EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
CIS v1.2.0	4.3 모든 VPC의 기본 보안 그룹이 모든 트래픽을 제한하는지 여부를 확인합니다.	[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
CIS v1.4.0	1.10 콘솔 암호가 있는 모든 IAM 사용자에 대해 다중 인증(MFA)이 활성화되었는지 여부를 확인합니다.	[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
CIS v1.4.0	1.4 90일이 되기 전에 액세스 키가 교체되는지 여부를 확인합니다.	[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
CIS v1.4.0	1.16 전체 "*:*" 관리 권한을 허용하는 IAM 정책이 연결되지 않았는지 확인합니다.	[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
CIS v1.4.0	1.17 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support	[IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
CIS v1.4.0	1.4 루트 사용자 계정 액세스 키가 없는지 여부를 확인합니다.	[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
CIS v1.4.0	1.5 루트 사용자 계정에 대해 MFA가 활성화되어 있는지 확인합니다.	[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
CIS v1.4.0	1.6 루트 사용자 계정에 대해 하드웨어 MFA가 활성화되어 있는지 확인합니다.	[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
CIS v1.4.0	1.7 관리 및 일상 작업에 루트 사용자 사용을 제거합니다.	[CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.
CIS v1.4.0	1.8 IAM 비밀번호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.	[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
CIS v1.4.0	1.9 IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.	[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
CIS v1.4.0	2.1.2 S3 버킷 정책이 HTTP 요청을 거부하도록 설정되어 있는지 확인합니다.	[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.
CIS v1.4.0	2.1.5.1 S3 퍼블릭 액세스 차단 설정을 활성화해야 합니다.	[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.
CIS v1.4.0	2.1.5.2 S3 퍼블릭 액세스 차단 설정은 버킷 수준에서 활성화되어야 합니다.	[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
CIS v1.4.0	2.2.1 EBS 볼륨 암호화가 활성화되었는지 확인합니다.	[EC2.7] EBS 기본 암호화를 활성화해야 합니다.
CIS v1.4.0	2.3.1 RDS 인스턴스에 암호화가 활성화되어 있는지 확인합니다.	[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.
CIS v1.4.0	3.1 모든 지역에서 CloudTrail 활성화되었는지 확인	[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.
CIS v1.4.0	3.2 CloudTrail 로그 파일 검증이 활성화되었는지 확인	[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.
CIS v1.4.0	3.4 CloudTrail 트레일이 로그와 통합되었는지 확인 CloudWatch	[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch
CIS v1.4.0	3.5 모든 지역에서 AWS Config 활성화되었는지 확인	[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.
CIS v1.4.0	3.6 S3 CloudTrail 버킷에서 S3 버킷 액세스 로깅이 활성화되었는지 확인합니다.	[CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
CIS v1.4.0	3.7 KMS CMK를 사용하여 유휴 상태의 CloudTrail 로그를 암호화해야 합니다.	[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.
CIS v1.4.0	3.8 고객이 생성한 CMK에 대한 교체가 활성화되었는지 확인합니다.	[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS
CIS v1.4.0	3.9 모든 VPC에서 VPC 흐름 로깅이 활성화되어 있는지 확인합니다.	[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.
CIS v1.4.0	4.4 IAM 정책 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.4] IAM 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.4.0	4.5 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인 CloudTrail	[CloudWatch.5] 기간 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오 CloudTrail AWS Config.
CIS v1.4.0	4.6 AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 존재하는지 확인	[CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.4.0	4.7 고객 생성 CMK 활성화 또는 예약된 삭제에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제를 위한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.4.0	4.8 S3 버킷 정책 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.8] S3 버킷 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.4.0	4.9 구성 변경에 대한 AWS Config 로그 메트릭 필터 및 경보가 존재하는지 확인	[CloudWatch.9] AWS Config 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
CIS v1.4.0	4.10 보안 그룹 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.10] 보안 그룹 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.4.0	4.11 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.11] 네트워크 액세스 제어 목록 (NACL) 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.4.0	4.12 네트워크 게이트웨이 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.12] 네트워크 게이트웨이 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.4.0	4.13 라우팅 테이블 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.13] 라우팅 테이블 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
CIS v1.4.0	4.14 VPC 변경 사항에 대해 로그 지표 필터 및 경보가 존재하는지 여부를 확인합니다.	[CloudWatch.14] VPC 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인
CIS v1.4.0	5.1 네트워크 ACL이 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않는지 확인합니다.	[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
CIS v1.4.0	5.3 모든 VPC의 기본 보안 그룹이 모든 트래픽을 제한하는지 여부를 확인합니다.	[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.
PCI DSS v3.2.1	PCI. AutoScaling.1 로드 밸런서와 연결된 Auto Scaling 그룹은 로드 밸런서 상태 점검을 사용해야 합니다.	[AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.
PCI DSS v3.2.1	PCI. CloudTrail.1 미사용 CloudTrail 로그는 CMK를 사용하여 AWS KMS 암호화해야 합니다.	[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
PCI DSS v3.2.1	PCI. CloudTrail.2를 CloudTrail 활성화해야 합니다.	[CloudTrail.3] 하나 이상의 트레일을 활성화해야 합니다. CloudTrail
PCI DSS v3.2.1	PCI. CloudTrail.3 CloudTrail 로그 파일 검증이 활성화되어야 합니다.	[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.
PCI DSS v3.2.1	PCI. CloudTrail.4 CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch	[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch
PCI DSS v3.2.1	PCI. CodeBuild1. CodeBuild GitHub 또는 비트버킷 소스 리포지토리 URL은 OAuth를 사용해야 합니다.	[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
PCI DSS v3.2.1	PCI. CodeBuild.2 CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.	[CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
PCI DSS v3.2.1	PCI.config.1을 AWS Config 활성화해야 합니다.	[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.
PCI DSS v3.2.1	[PCI.CW.1 루트 사용자 사용을 위한 로그 지표 필터 및 경보가 있는지 확합니다.	[CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.
PCI DSS v3.2.1	PCI.DMS.1 Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.	[DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
PCI DSS v3.2.1	PCI.EC2.1 EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.	[EC2.1] Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.
PCI DSS v3.2.1	PCI.EC2.2 VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 금지해야 합니다.	[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
PCI DSS v3.2.1	PCI.EC2.4 사용하지 않는 EC2 EIP를 제거해야 합니다.	[EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.
PCI DSS v3.2.1	PCI.EC2.5 보안 그룹은 0.0.0.0/0에서 포트 22로의 수신을 허용해서는 안 됩니다.	[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
PCI DSS v3.2.1	PCI.EC2.6 VPC 흐름 로깅은 모든 VPC에서 활성화되어야 합니다.	[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.
PCI DSS v3.2.1	PCI.ELBv2.1 Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.	[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.
PCI DSS v3.2.1	PCI.ES.1 Elasticsearch 도메인은 VPC에 있어야 합니다.	[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
PCI DSS v3.2.1	PCI.ES2 Elasticsearch 도메인에서 저장 시 암호화를 활성화해야 합니다.	[ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
PCI DSS v3.2.1	PCI. GuardDuty.1을 GuardDuty 활성화해야 합니다.	[GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
PCI DSS v3.2.1	PCI.IAM.1 IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.	[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
PCI DSS v3.2.1	PCI.IAM.2 IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.	[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
PCI DSS v3.2.1	PCI.IAM.3 IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.	[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
PCI DSS v3.2.1	PCI.IAM.4 루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.	[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
PCI DSS v3.2.1	PCI.IAM.5 루트 사용자에 대해 가상 MFA를 활성화해야 합니다.	[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
PCI DSS v3.2.1	PCI.IAM.6 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.	[IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
PCI DSS v3.2.1	PCI.IAM.7 IAM 사용자 보안 인증은 미리 정의된 일수 내에 사용하지 않을 경우 비활성화해야 합니다.	[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
PCI DSS v3.2.1	PCI.IAM.8 IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.	[IAM.10] IAM 사용자를 위한 암호 정책은 엄격한 기준을 적용해야 합니다. AWS Config
PCI DSS v3.2.1	PCI.KMS.1 고객 마스터 키(CMK) 교체가 활성화되어야 합니다.	[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS
PCI DSS v3.2.1	PCI.Lambda.1 Lambda 함수는 퍼블릭 액세스를 금지해야 합니다.	[Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.
PCI DSS v3.2.1	PCI.Lambda.2 Lambda 함수는 VPC에 있어야 합니다.	[Lambda.3] Lambda 함수는 VPC에 있어야 합니다.
PCI DSS v3.2.1	PCI.OpenSearch.1 OpenSearch 도메인은 VPC에 있어야 합니다.	[Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
PCI DSS v3.2.1	PCI.Opensearch.2 EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.	[Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
PCI DSS v3.2.1	PCI.RDS.1 RDS 스냅샷은 비공개 상태여야 합니다.	[RDS.1] RDS 스냅샷은 비공개여야 합니다.
PCI DSS v3.2.1	PCI.RDS.2 RDS DB 인스턴스는 퍼블릭 액세스를 금지해야 합니다.	[RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
PCI DSS v3.2.1	PCI.Redshift.1 Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.	[PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
PCI DSS v3.2.1	PCI.S3.1 S3 버킷은 퍼블릭 쓰기 액세스를 금지해야 합니다.	[S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다.
PCI DSS v3.2.1	PCI.S3.2 S3 버킷은 퍼블릭 읽기 액세스를 금지해야 합니다.	[S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.
PCI DSS v3.2.1	PCI.S3.3 S3 버킷에 크로스 리전 복제가 활성화되어 있어야 합니다.	[S3.7] S3 범용 버킷은 지역 간 복제를 사용해야 합니다.
PCI DSS v3.2.1	PCI.S3.5 S3 버킷에는 SSL(Secure Socket Layer) 사용 요청이 필요합니다.	[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.
PCI DSS v3.2.1	PCI.S3.6 S3 퍼블릭 액세스 차단 설정을 활성화해야 합니다.	[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.
PCI DSS v3.2.1	PCI. SageMaker.1 Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.	[SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
PCI DSS v3.2.1	PCI.SSM.1 Systems Manager가 관리하는 EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.	[SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
PCI DSS v3.2.1	PCI.SSM.2 Systems Manager에서 관리하는 EC2 인스턴스의 연결 규정 준수 상태는 COMPLIANT여야 합니다.	[SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

표준	표준 제어 ID 및 제목	보안 제어 ID 및 제목
PCI DSS v3.2.1	PCI.SSM.3 EC2 인스턴스는 다음으로 관리해야 합니다. AWS Systems Manager	[SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager

통합을 위한 워크플로 업데이트

워크플로가 제어 결과 필드의 특정 형식을 사용하지 않는 경우 별도의 조치가 필요하지 않습니다.

워크플로가 표에 나와 있는 제어 찾기 필드의 특정 형식을 사용하는 경우 워크플로를 업데이트해야 합니다. 예를 들어 특정 제어 ID에 대한 작업을 트리거하는 Amazon CloudWatch Events 규칙을 생성한 경우 (예: 제어 ID가 CIS 2.7과 같은 경우 AWS Lambda 함수 호출) 해당 제어 CloudTrail `Compliance.SecurityControlId` 필드인.2를 사용하도록 규칙을 업데이트하십시오.

변경된 제어 찾기 필드 또는 값을 사용하여 사용자 지정 통찰력을 만든 경우 현재 필드 또는 값을 사용하도록 해당 통찰력을 업데이트하십시오.

ASFF 예제

다음 섹션에는 AWS 보안 검색 결과 형식 (ASFF) 의 필수 및 선택적 속성의 예와 ASFF가 지원하는 각 리소스의 예가 나와 있습니다.

주제

- 필수 최상위 속성
- 선택적 최상위 속성
- Resources

필수 최상위 속성

AWS 보안 검색 결과 형식 (ASFF) 의 다음 최상위 속성은 Security Hub의 모든 검색 결과에 필요합니다. 이러한 필수 속성에 대한 자세한 내용은 AWS Security Hub API 참조의 AwsSecurityFinding 섹션을 참조하세요.

AwsAccountId

검색 결과가 적용되는 AWS 계정 ID.

예

```
"AwsAccountId": "111111111111"
```

CreatedAt

결과로 캡처된 잠재적 보안 문제가 생성된 시기를 나타냅니다.

예

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub는 가장 최근 업데이트로부터 90일 후 또는 업데이트가 발생하지 않는 경우 생성 날짜로부터 90일 후에 조사 결과를 삭제합니다. 결과를 90일 이상 저장하려면 결과를 S3 버킷으로 EventBridge 라우팅하는 Amazon의 규칙을 구성하면 됩니다.

설명

결과에 대한 설명입니다. 이 필드는 일반적인 표준 문안 텍스트이거나 결과의 인스턴스에만 해당하는 세부 정보일 수 있습니다.

Security Hub가 생성하는 제어 조사 결과의 경우 이 필드는 제어에 대한 설명을 제공합니다.

통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

예

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

결과를 생성한 솔루션별 구성 요소(로직의 개별 단위)에 대한 식별자입니다.

Security Hub가 생성하는 제어 조사 결과의 경우 통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

예

```
"GeneratorId": "security-control/Config.1"
```

Id

결과의 제품별 식별자입니다. Security Hub가 생성하는 제어 조사 결과에 대해 이 필드는 조사 결과 Amazon 리소스 이름(ARN)을 제공합니다.

통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

예

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956

"
```

ProductArn

제품이 Security Hub에 등록된 후 타사 조사 결과 제품을 고유하게 식별하는 Security Hub에서 생성된 Amazon 리소스 이름(ARN)입니다.

이 필드의 형식은 `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*입니다.

- Security Hub와 통합된 AWS 서비스의 경우 는 "aws“`product-id`이어야 하고 는 AWS 공용 서비스 이름이어야 합니다. `company-id` AWS 제품 및 서비스는 계정과 연결되어 있지 않으므로 ARN `account-id` 섹션은 비어 있습니다. AWS Security Hub와 아직 통합되지 않은 서비스는 타사 제품으로 간주됩니다.
- 퍼블릭 제품의 경우 `company-id` 및 `product-id`는 등록 시 지정된 ID 값이어야 합니다.
- 프라이빗 제품의 경우 `company-id`가 계정 ID여야 합니다. `product-id`는 예약어 "default" 또는 등록 시 지정된 ID여야 합니다.

예

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN

    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
```

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

리소스

Resources객체는 검색 결과에서 참조하는 AWS 리소스를 설명하는 일련의 리소스 데이터 유형을 제공합니다.

예

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
```

```
                    }
                },
                {
                    "Count": 59,
                    "Type": "EMAIL_ADDRESS",
                    "Occurrences": {
                        "Pages": [
                            {
                                "PageNumber": 1,
                                "OffsetRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                },
                                "LineRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                            {
                                "Start": 1,
                                "End": 13
                            }
                       ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                        "Records": [
                            {
                                "RecordIndex": 1,
                                "JsonPath": "$.ssn.value"
                            }
```

```
                            ]
                        }
                    },
                    {
                        "Count": 32,
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
},
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
```

```
    "InstanceMetadataTags": "disabled"
   }
  },
   "NetworkInterfaces": [
   {
    "NetworkInterfaceId": "eni-e5aa89a3"
   }
   ],
   "SubnetId": "PublicSubnet",
   "Type": "i3.xlarge",
   "VirtualizationType": "hvm",
   "VpcId": "TestVPCIpv6"
  }

]
```

SchemaVersion

결과의 형식을 지정할 스키마 버전입니다. 이 필드의 값은 AWS로 식별되는 공식적으로 게시된 버전 중 하나여야 합니다. 현재 릴리스의 AWS 보안 검색 결과 형식 스키마 버전은 입니다`2018-10-08`.

예

```
"SchemaVersion": "2018-10-08"
```

심각도

결과의 중요성을 정의합니다. 이 객체에 대한 자세한 내용은 AWS Security Hub API 참조의 `Severity`을 참조하십시오.

`Severity`는 결과의 최상위 객체이자 `FindingProviderFields` 객체 아래에 중첩되어 있습니다.

결과의 최상위 `Severity` 객체 값은 `BatchUpdateFindings` API에 의해서만 업데이트해야 합니다.

심각도 정보를 제공하려면 결과 공급자가 `BatchImportFindings` API 요청 시 `FindingProviderFields` 아래의 `Severity` 객체를 업데이트해야 합니다.
새 검색 결과에 대한 `BatchImportFindings` 요청이 제공만 `Label` 하거나 제공만 하는 경우 `Normalized` Security Hub는 다른 필드의 값을 자동으로 채웁니다. `Product`및 `Original` 필드를 채울 수도 있습니다.

최상위 `Finding.Severity` 객체가 있지만 존재하지 않는 경우 Security `Finding.FindingProviderFields` Hub는 `FindingProviderFields.Severity` 객체를 생성

하고 전체를 객체에 Finding.Severity object 복사합니다. 이렇게 하면 최상위 객체를 덮어쓰더라도 공급자가 제공한 원본 세부 정보가 FindingProviderFields.Severity 구조 내에 보존됩니다. Severity

결과의 심각도는 관련 자산 또는 기본 리소스의 중요성을 고려하지 않습니다. 중요성은 결과와 관련된 리소스의 중요도 수준으로 정의됩니다. 예를 들어 미션 크리티컬 애플리케이션과 관련된 리소스는 비프로덕션 테스트와 관련된 리소스보다 중요도가 더 높습니다. 리소스 중요성에 대한 정보를 캡처하려면 Criticality 필드를 사용합니다.

조사 결과의 기본 심각도 점수를 ASFF의 Severity.Label 값으로 변환할 때는 다음 지침을 사용하는 것이 좋습니다.

- INFORMATIONAL – 이 범주에는 PASSED, WARNING, 또는 NOT AVAILABLE 검사 결과 또는 민감한 데이터 식별에 대한 결과가 포함될 수 있습니다.
- LOW – 향후 손상으로 이어질 수 있는 조사 결과. 예를 들어 이 범주에는 취약성, 구성 약점, 노출된 비밀번호가 포함될 수 있습니다.
- MEDIUM – 활성 상태의 손상과 관련이 있지만 공격자가 목적을 달성했다는 증거는 없는 조사 결과. 예를 들어, 이 범주에는 맬웨어 활동, 해킹 활동 및 비정상적인 동작 감지가 포함될 수 있습니다.
- HIGH 또는 CRITICAL – 데이터 손실, 위반 행위 또는 서비스 거부 등 공격자의 목적 달성을 나타내는 조사 결과.

예

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

Title

결과의 제목입니다. 이 필드는 일반적인 표준 문안 텍스트이거나 결과의 이 인스턴스에만 해당하는 세부 정보를 포함할 수 있습니다.

제어 조사 결과의 경우 이 필드는 제어의 제목을 제공합니다.

통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

예

```
"Title": "AWS Config should be enabled"
```

타입

결과를 분류하는 *namespace*/*category*/*classifier* 형식으로 구성된 하나 이상의 결과 유형입니다. 통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

Types는 BatchUpdateFindings를 사용해서만 업데이트해야 합니다.

Types에 대한 값을 입력하고자 하는 결과 공급자는 FindingProviderFields 아래의 Types 속성을 사용해야 합니다.

다음 목록에서 1단계 글머리 기호는 네임스페이스이고 2단계 글머리 기호는 범주이며 3단계 글머리 기호는 분류자입니다. 조사 결과 공급자는 정의된 네임스페이스를 사용하여 조사 결과를 정렬하고 그룹화하는 것이 좋습니다. 정의된 범주와 분류자를 사용할 수도 있지만 필수는 아닙니다. 소프트웨어 및 구성 점검 네임스페이스에만 분류자가 정의되어 있습니다.

네임스페이스/범주/분류자에 대한 부분 경로를 정의할 수 있습니다. 예를 들어 다음 결과 유형은 모두 유효합니다.

- TTP
- TTPs/Defense Evasion
- TTPS/디펜스 회피/ CloudTrailStopped

다음 목록의 전술, 기술 및 절차(TTP) 범주는 MITER ATT & CK MatrixTM에 맞춰 정렬됩니다. Unusual Behaviors 네임스페이스는 일반적인 통계 이상과 같은 일반적인 비정상적인 동작을 반영하며 특정 TTP에 맞게 정렬되지 않습니다. 그러나 비정상 동작과 TTP 결과 유형을 모두 사용하여 결과를 분류할 수 있습니다.

네임스페이스, 범주, 분류자 목록:

- 소프트웨어 및 구성 점검
  - 취약성
    - CVE
  - AWS 보안 모범 사례
    - 네트워크 연결성
    - 실행 시간 행동 분석

- 산업 및 규제 표준
  - AWS 기본 보안 모범 사례
  - CIS 호스트 강화 벤치마크
  - CIS 재단 벤치마크 AWS
  - PCI-DSS
  - Cloud Security Alliance(CSA) 규제
  - ISO 90001 규제
  - ISO 27001 규제
  - ISO 27017 규제
  - ISO 27018 규제
  - SOC 1
  - SOC 2
  - HIPAA 규제(미국)
  - NIST 800-53 규제(미국)
  - NIST CSF 규제(미국)
  - IRAP 규제(호주)
  - K-ISMS 규제(한국)
  - MTCS 규제(싱가포르)
  - FISC 규제(일본)
  - My Number Act 규제(일본)
  - ENS 규제(스페인)
  - Cyber Essentials Plus 규제(영국)
  - G-Cloud 규제(영국)
  - C5 규제(독일)
  - IT-Grundschutz 규제(독일)
  - GDPR 규제(유럽)
  - TISAX 규제(유럽)
- 패치 관리
- TTP
  - 초기 액세스

  - Execution
  - Persistence
  - 권한 에스컬레이션
  - 방어 회피
  - 자격 증명 액세스
  - Discovery
  - 수평 이동
  - 수집
  - 명령 및 제어
- 효과
  - 데이터 노출
  - 데이터 유출
  - 데이터 폐기
  - 서비스 거부 공격
  - 리소스 소비
- 비정상 동작
  - 애플리케이션
  - 네트워크 흐름
  - IP 주소
  - User
  - VM
  - 컨테이너
  - Serverless
  - 프로세스
  - 데이터베이스
  - 데이터
- 민감한 데이터 식별
  - PII
  - 암호

  - 법적 고지

- 금융
- 보안
- 업무

예

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
```

UpdatedAt

결과 공급자가 결과 레코드를 마지막으로 업데이트한 시기를 나타냅니다.

이 타임스탬프는 검색 결과 레코드가 마지막으로 업데이트되었거나 가장 최근에 업데이트된 시간을 반영합니다. 따라서 이벤트 또는 취약성이 마지막으로 관찰된 시점 또는 가장 최근에 관찰된 시점을 반영하는 `LastObservedAt` 타임스탬프와 다를 수 있습니다.

결과 레코드를 업데이트할 때 이 타임스탬프를 현재 타임스탬프로 업데이트해야 합니다. 결과 레코드를 생성하면 `CreatedAt` 및 `UpdatedAt` 타임스탬프는 같아야 합니다. 결과 레코드를 업데이트한 후 이 필드의 값은 이전에 포함했던 모든 값보다 최근이어야 합니다.

단, `BatchUpdateFindings` API 작업을 사용하여 `UpdatedAt`을 업데이트할 수는 없습니다. `BatchImportFindings`를 사용해야만 업데이트할 수 있습니다.

예

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub는 가장 최근 업데이트로부터 90일 후 또는 업데이트가 발생하지 않는 경우 생성 날짜로부터 90일 후에 조사 결과를 삭제합니다. 결과를 90일 이상 저장하려면 결과를 S3 버킷으로 EventBridge 라우팅하는 Amazon의 규칙을 구성하면 됩니다.

선택적 최상위 속성

이러한 최상위 속성은 AWS 보안 탐지 형식 (ASFF) 에서 선택 사항입니다. 이러한 속성에 대한 자세한 내용은 AWS Security Hub API 참조를 참조하십시오 AwsSecurityFinding.

Action

`Action` 객체는 리소스에 영향을 주거나 리소스에 대해 취해진 작업에 대한 세부 정보를 제공합니다.

예

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                   "GeoLocation": {
                       "Lon": 0,
                       "Lat": 0
                   },
                   "Organization": {
                       "AsnOrg": "ExampleASO",
                       "Org": "ExampleOrg",
                       "Isp": "ExampleISP",
                       "Asn": 64496
                   }
                }
            }
        ],
```

```
        "Blocked": false
    }
}
```

AwsAccountName

검색 결과가 적용되는 AWS 계정 이름.

예

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

결과를 생성한 제품의 회사 이름입니다. 통제 기반 조사 결과의 경우 회사는 다음과 같습니다. AWS

Security Hub는 각 결과에 대해 이 속성을 자동으로 채웁니다. `BatchImportFindings` 또는 `BatchUpdateFindings`를 사용하여 업데이트할 수 없습니다. 사용자 지정 통합을 사용하는 경우는 예외입니다. the section called “사용자 지정 제품 통합 사용”을 참조하십시오.

Security Hub 콘솔을 사용하여 회사 이름을 기준으로 조사 결과를 필터링할 때는 이 속성을 사용합니다. Security Hub API를 사용하여 조사 결과를 제품 이름별로 필터링할 때는 `ProductFields` 아래의 `aws/securityhub/CompanyName` 속성을 사용합니다. Security Hub는 이러한 두 속성을 동기화하지 않습니다.

예

```
"CompanyName": "AWS"
```

Compliance

`Compliance` 객체는 제어와 관련된 검색 세부 정보를 제공합니다. 이 속성은 Security Hub 컨트롤에서 생성된 검색 결과와 Security Hub로 AWS Config 보내는 검색 결과에 대해 반환됩니다.

예

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
```

```
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

신뢰도

결과가 식별하고자 하는 동작이나 문제를 정확하게 식별할 가능성입니다.

`Confidence`는 [BatchUpdateFindings](#)를 사용해서만 업데이트해야 합니다.

Confidence에 대한 값을 입력하고자 하는 결과 공급자는 FindingProviderFields 아래의 Confidence 속성을 사용해야 합니다. the section called “FindingProviderFields 사용하기”를 참조하십시오.

Confidence는 비율 척도를 사용하여 0~100점으로 채점됩니다. 0은 0% 신뢰도를 의미하고, 100은 100% 신뢰도를 의미합니다. 예를 들어 실제 유출이 확인되지 않았기 때문에 네트워크 트래픽의 통계적 편차를 기반으로 한 데이터 유출 감지는 신뢰도가 낮습니다.

예

```
"Confidence": 42
```

중요도

결과와 관련된 리소스에 할당된 중요도 수준입니다.

Criticality는 BatchUpdateFindings API 작업을 호출해서만 업데이트해야 합니다. BatchImportFindings로 이 객체를 업데이트하지 마십시오.

Criticality에 대한 값을 입력하고자 하는 결과 공급자는 FindingProviderFields 아래의 Criticality 속성을 사용해야 합니다. the section called “FindingProviderFields 사용하기”을 참조하십시오.

Criticality는 정수만 지원하는 비율 척도를 사용하여 0~100점을 기준으로 점수가 부여됩니다. 0점은 기본 리소스에 중요성이 없음을 의미하며 100점은 가장 중요한 리소스에 예약됩니다.

각 리소스에 Criticality을 할당할 때는 다음 사항을 고려하십시오.

- 영향을 받는 리소스에 민감한 데이터(예: PII가 있는 S3 버킷)가 포함되어 있습니까?
- 영향을 받는 리소스에서 악의적 공격자가 더 깊이 액세스하거나 또 다른 악의적 활동(예: 시스템 관리자 계정 공격)을 수행할 가능성이 확대될 수 있습니까?
- 리소스가 비즈니스에 중요한 자산(예: 손상될 경우 수익에 상당한 영향을 미칠 수 있는 핵심 비즈니스 시스템)입니까?

다음 지침을 적용할 수 있습니다.

- 미션 크리티컬 시스템을 지원하거나 매우 민감한 데이터를 포함하는 리소스는 75~100점 범위에서 점수를 매길 수 있습니다.

- 중요한(핵심적이지는 않은) 데이터를 지원하거나 다소 중요한 데이터를 포함하는 리소스는 25~74점 범위에서 점수를 매길 수 있습니다.
- 중요하지 않은 시스템을 지원하거나 중요하지 않은 데이터를 포함하는 리소스는 반드시 0~24점 범위로 점수를 매겨야 합니다.

예

```
"Criticality": 99
```

FindingProviderFields

`FindingProviderFields`에는 다음 속성이 포함될 수 있습니다.

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

위 필드는 `FindingProviderFields` 개체 아래에 중첩되지만 이름은 최상위 ASFF 필드와 유사합니다. 검색 결과 제공자가 Security Hub로 새 검색 결과를 보내면 Security Hub는 해당 최상위 필드를 기반으로 객체가 비어 있는 경우 `FindingProviderFields` 객체를 자동으로 채웁니다.

제공자 검색은 Security Hub API의 `BatchImportFindings`작업을 사용하여 업데이트할 `FindingProviderFields` 수 있습니다. 검색 제공자는 이 객체를 로 업데이트할 수 없습니다 `BatchUpdateFindings`.

Security Hub에서 `BatchImportFindings`에서 `FindingProviderFields`로의 업데이트와 해당 최상위 속성을 처리하는 방법에 대한 자세한 내용은 the section called “FindingProviderFields 사용하기”을 참조하십시오.

고객은 `BatchUpdateFindings` 작업을 사용하여 최상위 필드를 업데이트할 수 있습니다. 고객은 업데이트할 `FindingProviderFields` 수 없습니다.

예

```
"FindingProviderFields": {
```

```
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

결과로 캡처된 잠재적 보안 문제가 처음 발견된 시기를 나타냅니다.

이 타임스탬프는 이벤트 또는 취약성이 처음 관찰된 시간을 반영합니다. 따라서 이 결과 레코드가 생성된 시간을 반영하는 `CreatedAt` 타임스탬프와 다를 수 있습니다.

이 타임스탬프는 결과 레코드의 업데이트 시에도 변하지 않아야 하지만, 보다 정확한 타임스탬프가 결정되면 업데이트할 수 있습니다.

예

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

조사 결과로 캡처된 잠재적 보안 문제가 보안 조사 결과 제품에 의해 가장 최근에 발견된 시기를 나타냅니다.

이 타임스탬프는 이벤트 또는 취약성이 마지막으로 또는 가장 최근에 관찰된 시간을 반영합니다. 따라서 이 검색 결과 레코드가 마지막으로 업데이트된 시점 또는 가장 최근에 업데이트된 시점을 반영하는 `UpdatedAt` 타임스탬프와 다를 수 있습니다.

이 타임스탬프를 입력할 수는 있지만 최초 관찰 시 필수적이지는 않습니다. 처음 관찰 시 이 필드를 입력하는 경우 타임스탬프는 `FirstObservedAt` 타임스탬프와 동일해야 합니다. 결과가 관찰될 때마다 마지막으로 또는 가장 최근에 관찰된 타임스탬프를 반영하여 이 필드를 업데이트해야 합니다.

예

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

`Malware` 객체는 결과와 관련된 악성코드 목록을 제공합니다.

예

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

Network(사용 중지)

`Network` 객체는 결과에 대한 네트워크 관련 정보를 제공합니다.

이 객체는 사용 중지되었습니다. 이 데이터를 입력하려면 데이터를 `Resources`의 리소스에 매핑하거나 `Action` 객체를 사용할 수 있습니다.

예

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
```

```
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

NetworkPath 객체는 결과와 관련된 네트워크 경로에 대한 정보를 제공합니다. NetworkPath의 각 항목은 경로의 구성 요소를 나타냅니다.

예

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
```

```
                "Address": [ "203.0.113.0/24" ]
            }
        }
    }
]
```

참고

Note 객체는 검색 결과에 추가할 수 있는 사용자 정의 메모를 지정합니다.

결과 공급자는 검색 결과에 대한 초기 메모를 입력할 수 있지만 그 후에 메모를 추가할 수는 없습니다. 메모는 BatchUpdateFindings를 사용해서만 업데이트할 수 있습니다.

예

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

이 PatchSummary 객체는 선택한 규정 준수 표준을 기준으로 인스턴스의 패치 규정 준수 상태를 요약하여 제공합니다.

예

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

프로세스

`Process` 객체는 결과에 대한 프로세스 관련 세부 정보를 제공합니다.

예제

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Security Hub가 결과를 수신하고 처리를 시작하는 시기를 나타냅니다.

이는 결과 공급자와 보안 문제 및 결과의 상호 작용과 관련된 필수 타임스탬프인 `CreatedAt` 및 `UpdatedAt`과 다릅니다. `ProcessedAt` 타임스탬프는 Security Hub가 결과를 처리하기 시작하는 시기를 나타냅니다. 처리가 완료된 후 사용자 계정에 결과가 나타납니다.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

보안 탐지 결과 제품에 정의된 AWS 보안 탐지 결과 형식에 포함되지 않은 추가 솔루션별 세부 정보가 포함될 수 있는 데이터 유형입니다.

Security Hub 제어에서 생성된 조사 결과의 경우 제어에 대한 정보가 `ProductFields`에 포함됩니다. the section called “제어 조사 결과 생성 및 업데이트”을 참조하십시오.

이 필드는 중복 데이터를 포함해서는 안 되며 AWS 보안 검색 결과 형식 필드와 충돌하는 데이터를 포함해서는 안 됩니다.

“aws/" 접두사는 AWS 제품 및 서비스용으로만 예약된 네임스페이스를 나타내며 타사 통합에서 얻은 결과와 함께 제출해서는 안 됩니다.

필수는 아니지만 제품은 필드 이름의 형식을 `company-id/product-id/field-name`으로 지정해야 합니다. 여기서 `company-id`와 `product-id`는 결과의 `ProductArn`에 입력된 것과 일치합니다.

`Archival`을 참조하는 필드는 Security Hub가 기존 결과를 보관할 때 사용됩니다. 예를 들어 Security Hub는 제어 또는 표준을 비활성화할 때와 통합 제어 조사 결과를 켜거나 끌 때 기존 조사 결과를 보관합니다.

이 필드에는 결과를 생성한 제어를 포함하는 표준에 대한 정보도 포함될 수 있습니다.

예

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

결과를 생성한 제품의 이름을 입력합니다. 제어 기반 조사 결과의 경우 제품 이름은 Security Hub입니다.

Security Hub는 각 결과에 대해 이 속성을 자동으로 채웁니다. `BatchImportFindings` 또는 `BatchUpdateFindings`를 사용하여 업데이트할 수 없습니다. 사용자 지정 통합을 사용하는 경우는 예외입니다. the section called “사용자 지정 제품 통합 사용”을 참조하십시오.

Security Hub 콘솔을 사용하여 제품 이름을 기준으로 조사 결과를 필터링할 때는 이 속성을 사용합니다.

Security Hub API를 사용하여 조사 결과를 제품 이름별로 필터링할 때는 `ProductFields` 아래의 `aws/securityhub/ProductName` 속성을 사용합니다.

Security Hub는 이러한 두 속성을 동기화하지 않습니다.

RecordState

결과의 레코드 상태를 입력합니다.

기본적으로 서비스에서 처음 생성된 조사 결과는 ACTIVE로 간주됩니다.

ARCHIVED 상태는 결과를 보기에서 숨겨야 함을 나타냅니다. 보관된 조사 결과는 즉시 삭제되지 않습니다. 이를 검색, 검토 및 보고할 수 있습니다. Security Hub는 연결된 리소스가 삭제되거나, 리소스가 존재하지 않거나, 제어가 비활성화된 경우 제어 기반 조사 결과를 자동으로 보관합니다.

RecordState는 결과 공급자를 찾기 위한 것으로, BatchImportFindings를 통해서만 업데이트할 수 있습니다. BatchUpdateFindings를 사용하여 업데이트할 수 없습니다.

결과에 대한 조사 상태를 추적하려면 RecordState 대신 Workflow를 사용하십시오.

레코드 상태가 ARCHIVED에서 ACTIVE로 변경되고 결과의 워크플로 상태가 NOTIFIED 또는 RESOLVED 인 경우 Security Hub는 자동으로 워크플로 상태를 NEW로 설정합니다.

예

```
"RecordState": "ACTIVE"
```

리전

검색 결과가 생성된 AWS 리전 출처를 지정합니다.

Security Hub는 각 결과에 대해 이 속성을 자동으로 채웁니다. BatchImportFindings 또는 BatchUpdateFindings를 사용하여 업데이트할 수 없습니다.

예

```
"Region": "us-west-2"
```

RelatedFindings

현재 조사 결과와 관련된 조사 결과 목록을 입력합니다.

RelatedFindings는 BatchUpdateFindings API 작업으로만 업데이트해야 합니다. BatchImportFindings로 이 객체를 업데이트하면 안 됩니다.

BatchImportFindings 요청의 경우 결과 공급자는 FindingProviderFields 아래의 RelatedFindings 객체를 사용해야 합니다.

RelatedFindings 속성 설명을 보려면 AWS Security Hub API 참조의 RelatedFinding를 참조하십시오.

예

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

이제 Security Hub가 와 통합되었습니다

Remediation 객체는 결과를 처리하기 위해 권장되는 문제 해결 단계에 대한 정보를 제공합니다.

예

```
"Remediation": {
    "Recommendation": {
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

Sample

결과가 샘플 결과인지 여부를 지정합니다.

```
"Sample": true
```

SourceUrl

SourceUrl 객체는 결과 제품의 현재 결과에 대한 페이지로 연결되는 URL을 제공합니다.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

ThreatIntelIndicator 객체는 결과와 관련된 위협 인텔리전스 세부 정보를 제공합니다.

예

```
"ThreatIntelIndicators": [
```

```
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

Threats

Threats 객체는 결과로 탐지된 위협에 대한 세부 정보를 제공합니다.

예

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

결과와 연관된 이름/값 문자열 페어의 목록을 입력합니다. 이는 결과에 추가되는 사용자 정의 필드입니다. 이러한 필드는 특정 구성을 통해 자동으로 생성될 수 있습니다.

결과 공급자는 제품이 생성하는 데이터에 이 필드를 사용해서는 안 됩니다. 대신 검색 제공자는 표준 AWS 보안 검색 결과 형식 `ProductFields` 필드에 매핑되지 않는 데이터에 대해 이 필드를 사용할 수 있습니다.

이 필드는 BatchUpdateFindings를 사용해서만 업데이트할 수 있습니다.

예

```
"UserDefinedFields": {
    "reviewedByCio": "true",
```

```
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

결과의 진실성을 입력합니다. 조사 결과 제품은 이 필드에 UNKNOWN 값을 입력할 수 있습니다. 조사 결과 제품의 시스템에 의미 있는 유사점이 있는 경우 조사 결과 제품은 이 필드의 값을 입력해야 합니다. 이 필드는 일반적으로 사용자가 결과를 조사한 이후의 사용자 결정 또는 작업으로 채워집니다.

검색 공급자는 이 속성의 초기 값을 입력할 수 있지만 그 이후에는 업데이트할 수 없습니다. 이 속성은 BatchUpdateFindings를 사용해서만 업데이트할 수 있습니다.

```
"VerificationState": "Confirmed"
```

취약성

Vulnerabilities 객체는 결과와 관련된 취약성 목록을 제공합니다.

예

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
```

```
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

워크플로

[Workflow](#) 객체는 결과 조사 상태에 대한 정보를 제공합니다.

이 필드는 고객이 수정, 오케스트레이션 및 티켓 작성 도구와 함께 사용하기 위한 것입니다. 결과 공급자를 위한 용도는 아닙니다.

`BatchUpdateFindings`를 사용하여 `Workflow` 필드를 업데이트할 수만 있습니다. 고객은 콘솔에서 업데이트할 수도 있습니다. the section called “조사 결과에 대한 워크플로 상태 설정”을 참조하십시오.

예

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (사용 중지)

이 객체는 사용 중지되었으며 `Workflow` 객체의 `Status` 필드로 대체되었습니다.

이 필드는 결과의 워크플로 상태를 제공합니다. 조사 결과 제품은 이 필드에 `NEW` 값을 입력할 수 있습니다. 조사 결과 제품의 시스템에 의미 있는 유사점이 있는 경우 조사 결과 제품은 이 필드의 값을 입력할 수 있습니다.

예

```
"WorkflowState": "NEW"
```

Resources

`Resources` 객체는 결과에 관련된 리소스에 대한 정보를 제공합니다.

여기에는 최대 32개의 리소스 객체로 구성된 배열이 포함됩니다.

리소스 이름의 형식을 결정하려면 AWS 보안 탐지 형식 (ASFF) 구문 섹션을 참조하세요.

각 리소스 객체의 예를 보려면 다음 목록에서 선택하세요.

주제

- Resource attributes
- AwsAmazonMQ
- AwsApiGateway
- AwsAppSync
- AwsAthena

- AwsAutoScaling
- AwsBackup
- AwsCertificateManager
- AwsCloudFormation
- AwsCloudFront
- AwsCloudTrail
- AwsCloudWatch
- AwsCodeBuild
- AwsDms
- AwsDynamoDB
- AwsEc2
- AwsEcr
- AwsEcs
- AwsEfs
- AwsEks
- AwsElasticBeanstalk
- AwsElasticSearch
- AwsElb
- AwsEventBridge
- AwsGuardDuty
- AwsIam
- AwsKinesis
- AwsKms
- AwsLambda
- AwsMsk
- AwsNetworkFirewall
- AwsOpenSearchService
- AwsRds
- AwsRedshift
- AwsRoute53

- AwsS3
- AwsSageMaker
- AwsSecretsManager
- AwsSns
- AwsSqs
- AwsSsm
- AwsStepFunctions
- AwsWaf
- AwsXray
- Container
- Other

Resource attributes

다음은 AWS 보안 검색 결과 형식 (ASFF) 의 `Resources` 객체에 대한 설명과 예제입니다. 필드에 대한 자세한 내용은 리소스 섹션을 참조하세요.

ApplicationArn

결과와 관련된 애플리케이션의 Amazon 리소스 이름(ARN)을 식별합니다.

예

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

결과와 관련된 애플리케이션의 이름을 식별합니다.

예

```
"ApplicationName": "SampleApp"
```

DataClassification

이 DataClassification 필드는 리소스에서 감지된 민감한 데이터에 대한 정보를 제공합니다.

예

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
```

```
                                "LineRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                           {
                               "Start": 1,
                               "End": 13
                           }
                       ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                        "Records": [
                            {
                                "RecordIndex": 1,
                                "JsonPath": "$.ssn.value"
                            }
                        ]
                    }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
            {
```

```
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
}
```

Details

이 Details 필드는 적절한 객체를 사용하는 단일 리소스에 대한 추가 정보를 제공합니다. Resources 객체의 개별 리소스 객체에 각 리소스를 입력해야 합니다.

단, 결과 크기가 최대 240KB를 초과하는 경우 해당 Details 객체는 결과에서 제거됩니다. AWS Config 규칙을 사용하는 제어 결과의 경우 AWS Config 콘솔에서 리소스 세부 정보를 볼 수 있습니다.

Security Hub는 지원되는 리소스 유형에 사용 가능한 리소스 세부 정보 집합을 제공합니다. 이러한 세부 정보는 Type 객체 값에 해당합니다. 가능한 경우 항상 제공된 유형을 사용하십시오.

예를 들어 리소스가 S3 버킷인 경우 리소스 Type을 AwsS3Bucket으로 설정하고 AwsS3Bucket 객체에 리소스 세부 정보를 제공합니다.

Other 객체를 사용하여 사용자 지정 필드 및 값을 입력할 수 있습니다. Other 객체는 다음과 같은 경우에 사용합니다.

- 리소스 유형(리소스 값 Type)에는 해당하는 세부 정보 객체가 없습니다. 리소스에 대한 세부 정보를 입력하려면 Other 객체를 사용합니다.
- 리소스 유형의 객체에 채우려는 모든 필드가 포함되어 있지 않습니다. 이 경우 리소스 유형의 세부 정보 객체를 사용하여 사용 가능한 필드를 채웁니다. Other 객체를 사용하여 유형별 하위 필드에 없는 필드를 채웁니다.
- 리소스 유형이 제공된 유형 중 하나가 아닙니다. 이 경우 Resource.Type을 Other로 설정하고 Other 객체를 사용하여 세부 정보를 채웁니다.

예

```
"Details": {
  "AwsEc2Instance": {
```

```
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

Id

주어진 리소스 유형에 대한 식별자입니다.

Amazon AWS 리소스 이름 (ARN) 으로 식별되는 리소스의 경우 이는 ARN입니다.

ARN이 없는 AWS 리소스의 경우 이는 리소스를 생성한 AWS 서비스에서 정의한 식별자입니다.

AWS 리소스가 아닌 경우 이는 리소스와 연결된 고유 식별자입니다.

예

```
"Id": "arn:aws:s3:::example-bucket"
```

Partition

리소스가 있는 파티션입니다. 파티션은 그룹입니다 AWS 리전. 각 파티션의 AWS 계정 범위는 한 파티션으로 지정됩니다.

지원되는 파티션은 다음과 같습니다.

- `aws` – AWS 리전
- `aws-cn` - 중국 리전
- `aws-us-gov` – AWS GovCloud (US) Region

예

```
"Partition": "aws"
```

리전

이 리소스가 위치한 AWS 리전 위치의 코드입니다. 리전 코드 목록은 리전 엔드포인트를 참조하세요.

예

```
"Region": "us-west-2"
```

ResourceRole

검색 결과에서 리소스의 역할을 식별합니다. 리소스는 결과 활동의 대상이거나 활동을 수행한 행위자입니다.

예

```
"ResourceRole": "target"
```

Tags

통합 AWS 서비스 및 타사 제품의 검색 결과를 포함하여 Security Hub에 수집된 결과에 리소스 태그를 추가할 수 있습니다. AWS Resource Groups 태깅 API의 `GetResources` 작동이 지원하는 리소스에 태그를 지정할 수 있습니다. 지원되는 리소스 목록은 Resource Groups 태깅 API를 지원하는 서비스를 참조하십시오.

태그를 추가하면 검색 결과가 처리될 때 리소스와 관련된 태그를 알 수 있습니다. 관련 태그가 있는 리소스에만 Tags 속성을 포함할 수 있습니다. 리소스에 연결된 태그가 없는 경우 결과에 Tags 속성을 포함하지 마세요.

조사 결과에 리소스 태그를 포함하면 데이터 강화 파이프라인을 구축하거나 보안 탐지 결과의 메타데이터를 수동으로 보강할 필요가 없습니다. 또한 태그를 사용하여 결과 및 통찰력을 검색 또는 필터링하고 자동화 규칙을 만들 수 있습니다.

태그에 적용되는 제한에 대한 자세한 내용은 태그 이름 지정 제한 및 요구 사항을 참조하십시오.

이 필드에는 AWS 리소스에 있는 태그만 제공할 수 있습니다. AWS 보안 검색 형식에 정의되지 않은 데이터를 제공하려면 Other 세부 정보 하위 필드를 사용하십시오.

예

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Type

세부 정보가 입력되는 리소스 유형입니다.

가능한 경우 항상 AwsEc2Instance 또는 AwsS3Bucket과 같은 제공된 리소스 유형 중 하나를 사용하세요.

리소스 유형이 제공된 리소스 유형과 일치하지 않는 경우 리소스 Type을 Other로 설정하고 Other 세부 정보 하위 필드를 사용하여 세부 정보를 채웁니다.

지원되는 값은 리소스에 나열되어 있습니다.

예

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ

다음은 AwsAmazonMQ 리소스에 대한 AWS 보안 검색 형식 (ASFF) 의 예입니다.

AwsAmazonMQBroker

AwsAmazonMQBroker는 Amazon MQ에서 실행하는 메시지 브로커 환경인 Amazon MQ 브로커에 대한 정보를 제공합니다.

다음 예제는 AwsAmazonMQBroker 객체에 대한 ASFF를 보여 줍니다. AwsAmazonMQBroker속성 설명을 보려면 AWS Security Hub API 참조의 AwsAmazonMQBroker를 참조하십시오.

예

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
```

```
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway

다음은 AwsApiGateway 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsApiGatewayRestApi

이 AwsApiGatewayRestApi 객체에는 Amazon API Gateway 버전 1에 있는 REST API에 대한 정보가 들어 있습니다.

다음은 AWS Security Finding 형식(ASFF)의 AwsApiGatewayRestApi 결과의 예입니다. AwsApiGatewayRestApi속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsApiGatewayRestApiDetails.

예

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
```

```
}
```

AwsApiGatewayStage

`AwsApiGatewayStage` 객체는 버전 1 Amazon API Gateway 단계에 대한 정보를 제공합니다.

다음은 AWS Security Finding 형식(ASFF)의 `AwsApiGatewayStage` 결과의 예입니다. `AwsApiGatewayStage`속성 설명을 보려면 AWS Security Hub API AwsApiGatewayStageDetails참조를 참조하십시오.

예

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
```

```
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayV2Api

`AwsApiGatewayV2Api` 객체에는 Amazon API Gateway의 버전 2 API에 대한 정보가 들어 있습니다.

다음은 AWS Security Finding 형식(ASFF)의 `AwsApiGatewayV2Api` 결과의 예입니다. `AwsApiGatewayV2Api`속성에 대한 설명을 보려면 AWS Security Hub API ApiDetails 참조의 AwsApiGatewayV2를 참조하십시오.

예

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
```

```
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2스테이지

`AwsApiGatewayV2Stage`에는 Amazon API Gateway의 버전 2 단계에 대한 정보가 들어 있습니다.

다음은 AWS Security Finding 형식(ASFF)의 `AwsApiGatewayV2Stage` 결과의 예입니다. `AwsApiGatewayV2Stage`속성에 대한 설명을 보려면 AWS Security Hub API StageDetails 참조의 AwsApiGatewayV2를 참조하십시오.

예

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
```

```
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```


AwsAppSync

다음은 AwsAppSync 리소스에 대한 AWS 보안 검색 형식 (ASFF) 의 예입니다.

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi응용 프로그램의 최상위 AWS AppSync 구조인 GraphQL API에 대한 정보를 제공합니다.

다음 예제는 AwsAppSyncGraphQLApi 객체에 대한 ASFF를 보여 줍니다. AwsAppSyncGraphQLApi속성에 대한 설명을 보려면 API 참조의 AwsAppSyncGraphQLapi를 참조하십시오.AWS Security Hub

예

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena

다음은 AwsAthena 리소스에 대한 AWS 보안 검색 형식 (ASFF) 의 예입니다.

AwsAthenaWorkGroup

AwsAthenaWorkGroup는 Amazon Athena 워크그룹에 대한 정보를 제공합니다. 워크그룹을 사용하면 사용자, 팀, 애플리케이션 또는 워크로드를 분리할 수 있습니다. 또한 데이터 처리 제한을 설정하고 비용을 추적하는 데도 도움이 됩니다.

다음 예제는 AwsAthenaWorkGroup 객체에 대한 ASFF를 보여 줍니다. AwsAthenaWorkGroup속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsAthenaWorkGroup.

예

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling

다음은 AwsAutoScaling 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsAutoScalingAutoScalingGroup

AwsAutoScalingAutoScalingGroup 객체는 자동 스케일링 그룹에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding 형식(ASFF)의 AwsAutoScalingAutoScalingGroup 결과의 예입니다. AwsAutoScalingAutoScalingGroup속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsAutoScalingAutoScalingGroupDetails.

예

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
```

```
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
                 },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

`AwsAutoScalingLaunchConfiguration` 객체는 시작 구성에 대한 세부 정보를 제공합니다.

다음은 AWS 보안 `AwsAutoScalingLaunchConfiguration` 탐지 형식 (ASFF) 의 검색 결과 예제입니다.

`AwsAutoScalingLaunchConfiguration`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsAutoScalingLaunchConfigurationDetails.

예

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
```

```
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
```

```
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup

다음은 AwsBackup 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsBackupBackupPlan

AwsBackupBackupPlan 객체는 AWS Backup 백업 계획에 대한 정보를 제공합니다. AWS Backup 백업 계획은 AWS 리소스를 백업할 시기와 방법을 정의하는 정책 표현식입니다.

다음 예는 AwsBackupBackupPlan 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. AwsBackupBackupPlan속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsBackupBackupPlan.

예

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
```

```
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```


AwsBackupBackupVault

`AwsBackupBackupVault` 객체는 AWS Backup 백업 볼트에 대한 정보를 제공합니다. AWS Backup 백업 저장소는 백업을 저장하고 구성하는 컨테이너입니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsBackupBackupVault 보여줍니다. AwsBackupBackupVault속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsBackupBackupVault.

예

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
       "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

AwsBackupRecoveryPoint 객체는 복구 지점이라고도 하는 AWS Backup 백업에 대한 정보를 제공합니다. AWS Backup 복구 지점은 지정된 시점의 리소스 콘텐츠를 나타냅니다.

다음 예에서는 AwsBackupRecoveryPoint 객체의 ASFF (AWS 보안 검색 결과 형식) 를 보여줍니다. AwsBackupBackupVault속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsBackupRecoveryPoint.

예

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
```

```
    "StorageClass": "WARM"
}
```

AwsCertificateManager

다음은 AwsCertificateManager 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsCertificateManagerCertificate

AwsCertificateManagerCertificate 객체는 AWS Certificate Manager (ACM) 인증서에 대한 세부 정보를 제공합니다.

다음은 AWS 보안 AwsCertificateManagerCertificate 탐지 형식 (ASFF) 의 검색 결과 예제입니다. AwsCertificateManagerCertificate속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsCertificateManagerCertificateDetails.

예

```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
```

```
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
            "Name": "DIGITAL_SIGNATURE",
        },
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
"_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
```

```
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation

다음은 AwsCloudFormation 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsCloudFormationStack

AwsCloudFormationStack 객체는 최상위 템플릿에 리소스로 중첩된 AWS CloudFormation 스택에 대한 세부 정보를 제공합니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsCloudFormationStack 보여줍니다. AwsCloudFormationStack속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsCloudFormationStackDetails.

예

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
```

```
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```

AwsCloudFront

다음은 AwsCloudFront 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsCloudFrontDistribution

AwsCloudFrontDistribution객체는 Amazon CloudFront 배포 구성에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding 형식(ASFF)의 AwsCloudFrontDistribution 결과의 예입니다. AwsCloudFrontDistribution속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsCloudFrontDistributionDetails.

예

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
         "Bucket": "myawslogbucket.s3.amazonaws.com",
         "Enabled": false,
         "IncludeCookies": false,
         "Prefix": "myawslog/"
     },
```

```
    "OriginGroups": {
         "Items": [
             {
                "FailoverCriteria": {
                    "StatusCodes": {
                         "Items": [
                             200,
                             301,
                             404
                         ]
                         "Quantity": 3
                     }
                }
             }
          ]
    },
    "Origins": {
          "Items": [
              {
                 "CustomOriginConfig": {
                     "HttpPort": 80,
                     "HttpsPort": 443,
                     "OriginKeepaliveTimeout": 60,
                     "OriginProtocolPolicy": "match-viewer",
                     "OriginReadTimeout": 30,
                     "OriginSslProtocols": {
                       "Items": ["SSLv3", "TLSv1"],
                       "Quantity": 2
                     }
                 }
              },
          ]
    },
                 "DomainName": "my-bucket.s3.amazonaws.com",
                 "Id": "my-origin",
                 "OriginPath": "/production",
                 "S3OriginConfig": {
                     "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                 }
          ]
    },
    "Status": "Deployed",
    "ViewerCertificate": {
```

```
            "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
            "Certificate": "ASCAJRRE5XYF52TKRY5M4",
            "CertificateSource": "iam",
            "CloudFrontDefaultCertificate": true,
            "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
            "MinimumProtocolVersion": "TLSv1.2_2021",
            "SslSupportMethod": "sni-only"
      },
      "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail

다음은 `AwsCloudTrail` 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsCloudTrailTrail

`AwsCloudTrailTrail` 객체는 AWS CloudTrail 추적에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding 형식(ASFF)의 `AwsCloudTrailTrail` 결과의 예입니다. `AwsCloudTrailTrail`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsCloudTrailTrailDetails.

예

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
```

```
}
```

AwsCloudWatch

다음은 AwsCloudWatch 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsCloudWatchAlarm

AwsCloudWatchAlarm객체는 경보 상태가 변경될 때 지표를 감시하거나 조치를 수행하는 Amazon CloudWatch 경보에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 탐지 형식 (ASFF) 을 AwsCloudWatchAlarm 보여줍니다. AwsCloudWatchAlarm속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsCloudWatchAlarmDetails.

예

```
"AwsCloudWatchAlarm": {
 "ActonsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
```

```
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild

다음은 AwsCodeBuild 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsCodeBuildProject

AwsCodeBuildProject 객체는 AWS CodeBuild 프로젝트에 대한 정보를 제공합니다.

다음은 AWS Security Finding 형식(ASFF)의 AwsCodeBuildProject 결과의 예입니다. AwsCodeBuildProject속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsCodeBuildProjectDetails.

예

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
```

```
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "EncryptionKey": "string",
   "Certificate": "string",
   "Environment": {
      "Certificate": "string",
      "EnvironmentVariables": [
           {
                "Name": "string",
                "Type": "string",
                "Value": "string"
           }
      ],
   "ImagePullCredentialsType": "string",
   "PrivilegedMode": boolean,
   "RegistryCredential": {
       "Credential": "string",
       "CredentialProvider": "string"
   },
   "Type": "string"
   },
   "LogsConfig": {
        "CloudWatchLogs": {
             "GroupName": "string",
             "Status": "string",
             "StreamName": "string"
        },
        "S3Logs": {
             "EncryptionDisabled": boolean,
             "Location": "string",
             "Status": "string"
        }
   },
   "Name": "string",
   "ServiceRole": "string",
   "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
   },
   "VpcConfig": {
```

```
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
    }
}
```

AwsDms

다음은 AwsDms 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsDmsEndpoint

AwsDmsEndpoint객체는 AWS Database Migration Service (AWS DMS) 엔드포인트에 대한 정보를 제공합니다. 엔드포인트는 데이터 저장소에 대한 연결, 데이터 저장소 유형, 위치 정보를 제공합니다.

다음 예제는 AwsDmsEndpoint 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. AwsDmsEndpoint속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsDmsEndpointDetails.

예

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

AwsDmsReplicationInstance객체는 AWS Database Migration Service (AWS DMS) 복제 인스턴스에 대한 정보를 제공합니다. DMS는 복제 인스턴스를 사용하여 소스 데이터 저장소에 연결하고, 소스 데이터를 읽고, 대상 데이터 저장소에서 사용할 수 있도록 데이터 형식을 지정합니다.

다음 예제는 AwsDmsReplicationInstance 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. AwsDmsReplicationInstance속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsDmsReplicationInstanceDetails.

예

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

AwsDmsReplicationTask객체는 AWS Database Migration Service (AWS DMS) 복제 작업에 대한 정보를 제공합니다. 복제 작업은 소스 엔드포인트에서 대상 엔드포인트로 데이터 세트를 이동합니다.

다음 예제는 AwsDmsReplicationInstance 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. AwsDmsReplicationInstance속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsDmsReplicationInstance.

예

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
```

```
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
```

```
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```

AwsDynamoDB

다음은 AwsDynamoDB 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsDynamoDbTable

AwsDynamoDbTable 객체는 Amazon DynamoDB 테이블에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding 형식(ASFF)의 AwsDynamoDbTable 결과의 예입니다. AwsDynamoDbTable속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsDynamoDbTableDetails.

예

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
        {
            "AttributeName": "attribute2",
```

```
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
```

```
    ],
    "GlobalTableVersion": "V1",
    "ItemCount": 2705,
    "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
     ],
     "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
     "LatestStreamLabel": "2019-12-03T23:23:10.248",
     "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
```

```
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2

다음은 `AwsEc2` 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsEc2ClientVpnEndpoint

`AwsEc2ClientVpnEndpoint`객체는 AWS Client VPN 엔드포인트에 대한 정보를 제공합니다. Client VPN 엔드포인트는 클라이언트 VPN 세션을 활성화하고 관리하기 위해 생성 및 구성하는 리소스입니다. 이는 모든 Client VPN 세션의 종료 지점입니다.

다음 예제는 AwsEc2ClientVpnEndpoint 객체의 AWS 보안 검색 형식 (ASFF) 을 보여 줍니다. AwsEc2ClientVpnEndpoint속성에 대한 설명을 보려면 AWS Security Hub API ClientVpnEndpointDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

`AwsEc2Eip` 객체는 탄력적 IP 주소에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2Eip` 보여줍니다. `AwsEc2Eip`속성에 대한 설명을 보려면 AWS Security Hub API EipDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

`AwsEc2Instance` 객체는 Amazon EC2 인스턴스에 대한 세부 정보를 제공합니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2Instance` 보여줍니다. `AwsEc2Instance`속성에 대한 설명을 보려면 AWS Security Hub API InstanceDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
```

```
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

`AwsEc2LaunchTemplate` 객체에는 인스턴스 구성 정보를 지정하는 Amazon Elastic Compute Cloud 시작 템플릿에 대한 세부 정보가 들어 있습니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2LaunchTemplate` 보여 줍니다. `AwsEc2LaunchTemplate`속성에 대한 설명을 보려면 AWS Security Hub API LaunchTemplateDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
```

```
        "VolumeType:" "gp2"
       }
      }],
      "MetadataOptions": {
       "HttpTokens": "enabled",
       "HttpPutResponseHopLimit" : 1
      },
      "Monitoring": {
       "Enabled": true,
      "NetworkInterfaces": [{
       "AssociatePublicIpAddress" : true,
      }],
     "LaunchTemplateName": "string",
     "LicenseSpecifications": ["string"],
     "SecurityGroupIds": ["sg-01fce87ad6e019725"],
     "SecurityGroups": ["string"],
     "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

`AwsEc2NetworkAcl` 객체에는 Amazon EC2 네트워크 액세스 제어 목록(ACL)에 대한 세부 정보가 포함됩니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2NetworkAcl` 보여줍니다. `AwsEc2NetworkAcl`속성에 대한 설명을 보려면 AWS Security Hub API NetworkAclDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
   }],
   "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
```

```
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
        "RuleAction": "allow",
        "RuleNumber": 100
    }]
}
```

AwsEc2NetworkInterface

`AwsEc2NetworkInterface` 객체는 Amazon EC2 네트워크 인터페이스에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2NetworkInterface` 보여 줍니다. `AwsEc2NetworkInterface`속성에 대한 설명을 보려면 AWS Security Hub API NetworkInterfaceDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
```

```
}
```

AwsEc2RouteTable

`AwsEc2RouteTable` 객체는 Amazon EC2 라우팅 테이블에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2RouteTable` 보여줍니다. `AwsEc2RouteTable`속성에 대한 설명을 보려면 AWS Security Hub API RouteTableDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

`AwsEc2SecurityGroup`객체는 Amazon EC2 보안 그룹을 설명합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsEc2SecurityGroup 보여줍니다. AwsEc2SecurityGroup속성에 대한 설명을 보려면 AWS Security Hub API SecurityGroupDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
    ]
}
```

AwsEc2Subnet

AwsEc2Subnet 객체는 Amazon EC2의 서브넷에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsEc2Subnet 보여줍니다. AwsEc2Subnet속성에 대한 설명을 보려면 AWS Security Hub API SubnetDetails 참조의 AwsEc 2를 참조하십시오.

예

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

AwsEc2TransitGateway이 객체는 Virtual Private Cloud(VPC)와 온프레미스 네트워크를 상호 연결하는 Amazon EC2 전송 게이트웨이에 대한 세부 정보를 제공합니다.

다음은 AWS 보안 AwsEc2TransitGateway 탐지 형식 (ASFF) 의 검색 결과 예제입니다. AwsEc2TransitGateway속성 설명을 보려면 AWS Security Hub API TransitGatewayDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
```

```
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

`AwsEc2Volume` 객체는 Amazon EC2 볼륨에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2Volume` 보여줍니다. `AwsEc2Volume`속성에 대한 설명을 보려면 AWS Security Hub API VolumeDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

`AwsEc2Vpc` 객체는 Amazon EC2 VPC에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2Vpc` 보여줍니다. `AwsEc2Vpc`속성에 대한 설명을 보려면 AWS Security Hub API VpcDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

`AwsEc2VpcEndpointService` 객체에는 VPC 엔드포인트 서비스의 서비스 구성에 대한 세부 정보가 들어 있습니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2VpcEndpointService` 보여 줍니다. `AwsEc2VpcEndpointService`속성에 대한 설명을 보려면 AWS Security Hub API VpcEndpointServiceDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2VpcEndpointService": {
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
```

```
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

`AwsEc2VpcPeeringConnection` 객체는 두 VPC 간의 네트워킹 연결에 대한 세부 정보를 제공합니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2VpcPeeringConnection` 보여줍니다. `AwsEc2VpcPeeringConnection`속성에 대한 설명을 보려면 AWS Security Hub API VpcPeeringConnectionDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "ExpirationTime": "2022-02-18T15:31:53.161Z",
```

```
 "RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "192.168.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "Status": {
  "Code": "initiating-request",
  "Message": "Active"
 },
 "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```

AwsEc2VpnConnection

`AwsEc2VpnConnection` 객체는 Amazon EC2 VPN 연결에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEc2VpnConnection` 보여줍니다. `AwsEc2VpnConnection`속성에 대한 설명을 보려면 AWS Security Hub API VpnConnectionDetails 참조의 AwsEc 2를 참조하십시오.

예

```
"AwsEc2VpnConnection": {
    "VpnConnectionId": "vpn-205e4f41",
    "State": "available",
    "CustomerGatewayConfiguration": "",
    "CustomerGatewayId": "cgw-5699703f",
    "Type": "ipsec.1",
    "VpnGatewayId": "vgw-2ccb2245",
    "Category": "VPN"
    "TransitGatewayId": "tgw-09b6f3a659e2b5elf",
```

```
    "VgwTelemetry": [
        {
            "OutsideIpAddress": "92.0.2.11",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:09:32.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        },
        {
            "OutsideIpAddress": "92.0.2.12",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:10:51.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        }
    ],
    "Routes": [{
        "DestinationCidrBlock": "10.24.34.0/24",
        "State": "available"
   }],
    "Options": {
        "StaticRoutesOnly": true
        "TunnelOptions": [{
            "DpdTimeoutSeconds": 30,
            "IkeVersions": ["ikev1", "ikev2"],
            "Phase1DhGroupNumbers": [14, 15, 16, 17, 18},
            "Phase1EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase1IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase1LifetimeSeconds": 28800,
            "Phase2DhGroupNumbers": [14, 15, 16, 17, 18],
            "Phase2EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase2IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase2LifetimeSeconds": 28800,
            "PreSharedKey": "RltXC3REhTw1RAdiM2s1uMfkkSDLyGJoe1QEWeGxqkQ=",
            "RekeyFuzzPercentage": 100,
            "RekeyMarginTimeSeconds": 540,
            "ReplayWindowSize": 1024,
            "TunnelInsideCidr": "10.24.34.0/23"
        }]
   }
}
```

AwsEcr

다음은 AwsEcr 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsEcrContainerImage

AwsEcrContainerImage 객체는 Amazon ECR 이미지에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsEcrContainerImage 보여줍니다. AwsEcrContainerImage속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEcrContainerImageDetails.

예

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

AwsEcrRepository 객체는 Amazon Elastic 컨테이너 레지스트리 리포지토리에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsEcrRepository 보여줍니다. AwsEcrRepository속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEcrRepositoryDetails.

예

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
```

```
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs

다음은 AwsEcs 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsEcsCluster

AwsEcsCluster 객체는 Amazon Elastic Container Service 클러스터에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsEcsCluster 보여줍니다. AwsEcsCluster속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEcsClusterDetails.

예

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
```

```
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

`AwsEcsContainer` 객체에는 Amazon ECS 컨테이너에 대한 세부 정보가 들어 있습니다.

다음 예제는 `AwsEcsContainer` 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. `AwsEcsContainer`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEcsContainerDetails.

예

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

`AwsEcsService` 객체는 Amazon ECS 클러스터 내의 서비스에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEcsService` 보여줍니다. `AwsEcsService`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEcsServiceDetails.

예

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
```

```
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
```

```
        {
            "Field": "",
            "Type": ""
        }
    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

`AwsEcsTask` 객체는 Amazon ECS 작업에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEcsTask` 보여줍니다. `AwsEcsTask`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEcsTask.

예

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
```

```
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
}
```

AwsEcsTaskDefinition

`AwsEcsTaskDefinition` 객체에는 작업 정의에 대한 세부 정보가 들어 있습니다. 작업 정의는 Amazon Elastic Container Service 작업의 컨테이너 및 볼륨 정의를 설명합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsEcsTaskDefinition` 보여줍니다. `AwsEcsTaskDefinition`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEcsTaskDefinitionDetails.

예

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
```

```
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
                    "LogDriver": "awslogs",
                    "Options": {
                        "awslogs-group": "/ecs/sinatra-hi",
                        "awslogs-region": "ap-southeast-1",
                        "awslogs-stream-prefix": "ecs"
                    },
                    "SecretOptions": []

                },
                "MemoryReservation": 128,
                "Name": "web",
                "PortMappings": [
                    {
                        "ContainerPort": 4567,
                        "HostPort":4567,
                        "Protocol": "tcp"
                    }
                ],
                "Privileged": true,
                "StartTimeout": 10,
                "StopTimeout": 100,
            }
        ],
        "Family": "sinatra-hi",
        "NetworkMode": "host",
        "RequiresCompatibilities": ["EC2"],
        "Status": "ACTIVE",
        "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    }
```

AwsEfs

다음은 `AwsEfs` 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsEfsAccessPoint

`AwsEfsAccessPoint` 객체는 Amazon Elastic File System에 저장된 파일에 대한 세부 정보를 제공합니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsEfsAccessPoint 보여줍니다. AwsEfsAccessPoint속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEfsAccessPointDetails.

예

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

AwsEks

다음은 AwsEks 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsEksCluster

AwsEksCluster 객체는 Amazon EKS 클러스터에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsEksCluster 보여줍니다. AwsEksCluster속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEksClusterDetails.

예

```
{
  "AwsEksCluster": {
```

```
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk

다음은 `AwsElasticBeanstalk` 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsElasticBeanstalkEnvironment

`AwsElasticBeanstalkEnvironment` 개체에는 AWS Elastic Beanstalk 환경에 대한 세부 정보가 들어 있습니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsElasticBeanstalkEnvironment 보여줍니다. AwsElasticBeanstalkEnvironment속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsElasticBeanstalkEnvironmentDetails.

예

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
```

```
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch

다음은 AwsElasticSearch 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsElasticSearchDomain

AwsElasticSearchDomain객체는 Amazon OpenSearch 서비스 도메인에 대한 세부 정보를 제공합니다.

다음 예제는 AwsElasticSearchDomain 객체의 AWS 보안 탐지 형식 (ASFF) 을 보여줍니다. AwsElasticSearchDomain속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsElasticSearchDomainDetails.

예

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
```

```
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
           "DedicatedMasterCount": number,
           "DedicatedMasterEnabled": boolean,
           "DedicatedMasterType": "string",
           "InstanceCount": number,
           "InstanceType": "string",
           "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
           },
           "ZoneAwarenessEnabled": boolean
    },
    "ElasticsearchVersion": "string",
    "EncryptionAtRestOptions": {
           "Enabled": boolean,
           "KmsKeyId": "string"
    },
    "LogPublishingOptions": {
           "AuditLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "IndexSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "SearchSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           }
    },
    "NodeToNodeEncryptionOptions": {
           "Enabled": boolean
    },
    "ServiceSoftwareOptions": {
           "AutomatedUpdateDate": "string",
           "Cancellable": boolean,
           "CurrentVersion": "string",
           "Description": "string",
           "NewVersion": "string",
```

```
            "UpdateAvailable": boolean,
            "UpdateStatus": "string"
    },
    "VPCOptions": {
           "AvailabilityZones": [
                 "string"
           ],
           "SecurityGroupIds": [
                 "string"
           ],
           "SubnetIds": [
                 "string"
           ],
          "VPCId": "string"
    }
}
```

AwsElb

다음은 AwsElb 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsElbLoadBalancer

AwsElbLoadBalancer 객체에는 Classic Load Balancer에 대한 세부 정보가 포함됩니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsElbLoadBalancer 보여줍니다. AwsElbLoadBalancer속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsElbLoadBalancerDetails.

예

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
```

```
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "doc-example-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
```

```
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

`AwsElbv2LoadBalancer` 객체는 로드 밸런서에 대한 정보를 제공합니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsElbv2LoadBalancer` 보여줍니다. `AwsElbv2LoadBalancer`속성에 대한 설명을 보려면 AWS Security Hub API LoadBalancerDetails 참조의 AwsElbv 2를 참조하십시오.

예

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
                        "CanonicalHostedZoneId": "string",
                        "CreatedTime": "string",
                        "DNSName": "string",
                        "IpAddressType": "string",
                        "LoadBalancerAttributes": [
                            {
                                "Key": "string",
                                "Value": "string"
                            }
                        ],
                        "Scheme": "string",
                        "SecurityGroups": [ "string" ],
                        "State": {
                            "Code": "string",
                            "Reason": "string"
                        },
                        "Type": "string",
                        "VpcId": "string"
                    }
```

AwsEventBridge

다음은 AwsEventBridge 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsEventSchemasRegistry

AwsEventSchemasRegistry객체는 Amazon EventBridge 스키마 레지스트리에 대한 정보를 제공합니다. 스키마는 전송되는 이벤트의 구조를 정의합니다 EventBridge. 스키마 레지스터는 스키마를 수집하고 논리적으로 그룹화하는 컨테이너입니다.

다음 예제는 AwsEventSchemasRegistry 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. AwsEventSchemasRegistry속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEventSchemasRegistry.

예

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

`AwsEventsEndpoint`객체는 Amazon EventBridge 글로벌 엔드포인트에 대한 정보를 제공합니다. 엔드포인트는 리전 내결함성을 높여 애플리케이션의 가용성을 향상시킬 수 있습니다.

다음 예는 `AwsEventsEndpoint` 객체의 AWS 보안 탐지 형식 (ASFF) 을 보여줍니다. `AwsEventsEndpoint`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEventsEndpointDetails.

예

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
```

```
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

`AwsEventsEventbus`객체는 Amazon EventBridge 글로벌 엔드포인트에 대한 정보를 제공합니다. 엔드포인트는 리전 내결함성을 높여 애플리케이션의 가용성을 향상시킬 수 있습니다.

다음 예는 `AwsEventsEventbus` 객체의 AWS 보안 탐지 형식 (ASFF) 을 보여줍니다. `AwsEventsEventbus`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsEventsEventbusDetails.

예

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule
\",\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty

다음은 `AwsGuardDuty` 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsGuardDutyDetector

`AwsGuardDutyDetector`객체는 Amazon GuardDuty 감지기에 대한 정보를 제공합니다. 감지기는 GuardDuty 서비스를 나타내는 객체입니다. GuardDuty 작동하려면 탐지기가 필요합니다.

다음 예는 AwsGuardDutyDetector 객체의 AWS 보안 탐지 형식 (ASFF) 을 보여줍니다. AwsGuardDutyDetector속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsGuardDutyDetector.

예

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                 }
             },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
         }
    }
}
```

AwsIam

다음은 AwsIam 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsIamAccessKey

AwsIamAccessKey 객체에는 결과와 관련된 IAM 액세스 키에 대한 세부 정보가 들어 있습니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsIamAccessKey 보여줍니다. AwsIamAccessKey속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsIamAccessKeyDetails.

예

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
                            },
                            "SessionIssuer": {
                                "AccountId": "string",
                                "Arn": "string",
                                "PrincipalId": "string",
                                "Type": "string",
                                "UserName": "string"
                            }
                        },
                        "Status": "string"
                    }
```

AwsIamGroup

AwsIamGroup 객체에는 IAM 그룹에 대한 세부 정보가 포함됩니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsIamGroup 보여줍니다. AwsIamGroup속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsIamGroupDetails.

예

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

`AwsIamPolicy` 객체는 IAM 권한 정책을 나타냅니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsIamPolicy` 보여줍니다. `AwsIamPolicy`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsIamPolicyDetails.

예

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
```

```
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

`AwsIamRole` 객체는 역할의 정책을 모두 포함한 IAM 역할에 대한 정보가 들어 있습니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsIamRole` 보여줍니다. `AwsIamRole`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsIamRoleDetails.

예

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17','Statement': [{'Effect':
 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
            "PolicyName": "Example policy 1"
        },
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
                        "Path": "/",
                        "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
```

```
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
        "Path": "/",
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

`AwsIamUser` 객체는 사용자에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsIamUser` 보여줍니다. `AwsIamUser`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsIamUserDetails.

예

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
```

```
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

AwsKinesis

다음은 AwsKinesis 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsKinesisStream

AwsKinesisStream 객체는 Amazon Kinesis Data Streams에 대한 세부 정보를 제공합니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsKinesisStream 보여줍니다. AwsKinesisStream속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsKinesisStreamDetails.

예

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms

다음은 AwsKms 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsKmsKey

AwsKmsKey객체는 에 대한 세부 정보를 제공합니다. AWS KMS key

다음 예제는 AwsKmsKey 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. AwsKmsKey속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsKmsKeyDetails.

예

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

다음은 AwsLambda 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsLambdaFunction

AwsLambdaFunction 객체는 Lambda 함수의 구성에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsLambdaFunction 보여줍니다. AwsLambdaFunction속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsLambdaFunctionDetails.

예

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "DOC-EXAMPLE-BUCKET",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
```

```
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

`AwsLambdaLayerVersion` 객체는 Lambda 계층 버전에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsLambdaLayerVersion` 보여줍니다. `AwsLambdaLayerVersion`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsLambdaLayerVersionDetails.

예

```
"AwsLambdaLayerVersion": {
```

```
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk

다음은 AwsMsk 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsMskCluster

이 AwsMskCluster 객체는 Amazon Managed Streaming for Apache Kafka(Amazon MSK) 클러스터에 대한 정보를 제공합니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsMskCluster 보여줍니다. AwsMskCluster속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsMskClusterDetails.

예

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
```

```
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall

다음은 AwsNetworkFirewall 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsNetworkFirewallFirewall

AwsNetworkFirewallFirewall 객체에는 AWS Network Firewall 방화벽에 대한 세부 정보가 포함됩니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsNetworkFirewallFirewall 보여줍니다. AwsNetworkFirewallFirewall속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsNetworkFirewallFirewallDetails.

예

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
```

```
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

`AwsNetworkFirewallFirewallPolicy` 객체는 방화벽 정책에 대한 세부 정보를 제공합니다. 방화벽 정책은 네트워크 방화벽의 동작을 정의합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsNetworkFirewallFirewallPolicy` 보여줍니다. `AwsNetworkFirewallFirewallPolicy`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsNetworkFirewallFirewallPolicyDetails.

예

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
     ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
   "FirewallPolicyName": "InitialFirewall",
   "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

`AwsNetworkFirewallRuleGroup` 객체는 AWS Network Firewall 규칙 그룹에 대한 세부 정보를 제공합니다. 규칙 그룹은 네트워크 트래픽을 검사하고 제어하는 데 사용됩니다. 상태 비저장 규칙 그룹은 개별 패킷에 적용됩니다. 상태 저장 규칙 그룹은 트래픽 흐름의 컨텍스트에서 패킷에 적용됩니다.

규칙 그룹은 방화벽 정책에서 참조됩니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsNetworkFirewallRuleGroup` 보여줍니다. `AwsNetworkFirewallRuleGroup`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsNetworkFirewallRuleGroupDetails.

예 - 상태 비저장 규칙 그룹

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
                                "aws:pass"
                            ],
                            "MatchAttributes": {
                                "DestinationPorts": [
                                    {
                                        "FromPort": 443,
                                        "ToPort": 443
                                    }
                                ],
                                "Destinations": [
                                    {
                                        "AddressDefinition": "192.0.2.0/24"
```

```
                                    }
                                ],
                                "Protocols": [
                                            6
                                ],
                                "SourcePorts": [
                                    {
                                        "FromPort": 0,
                                        "ToPort": 65535
                                    }
                                ],
                                "Sources": [
                                    {
                                         "AddressDefinition": "198.51.100.0/24"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

예 - 상태 저장 규칙 그룹

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
             "StatefulRules": [
                 {
                     "Action": "PASS",
                     "Header": {
                         "Destination": "Any",
                         "DestinationPort": "443",
```

```
                        "Direction": "ANY",
                        "Protocol": "TCP",
                        "Source": "Any",
                        "SourcePort": "Any"
                    },
                    "RuleOptions": [
                        {
                           "Keyword": "sid:1"
                        }
                    ]
                }
            ]
        }
    }
}
```

다음은 AwsNetworkFirewallRuleGroup 속성에 대한 유효한 값 예제 목록입니다.

- Action

  유효한 값: PASS | DROP | ALERT

- Protocol

  유효한 값: IP | TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP

- Flags

  유효한 값: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- Masks

  유효한 값: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

AwsOpenSearchService

다음은 AwsOpenSearchService 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsOpenSearchServiceDomain

AwsOpenSearchServiceDomain객체에는 Amazon OpenSearch 서비스 도메인에 대한 정보가 들어 있습니다.

다음 예제는 AwsOpenSearchServiceDomain 객체의 AWS 보안 탐지 형식 (ASFF) 을 보여줍니다. AwsOpenSearchServiceDomain속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsOpenSearchServiceDomainDetails.

예

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
        },
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
```

```
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
```

```
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds

다음은 AwsRds 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsRdsDbCluster

AwsRdsDbCluster 객체는 Amazon RDS 데이터베이스 클러스터에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsRdsDbCluster 보여줍니다. AwsRdsDbCluster속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsRdsDbClusterDetails.

예

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
```

```
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

`AwsRdsDbClusterSnapshot` 객체에는 Amazon RDS DB 클러스터 스냅샷에 대한 정보가 포함됩니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsRdsDbClusterSnapshot` 보여줍니다. `AwsRdsDbClusterSnapshot`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsRdsDbClusterSnapshotDetails.

예

```
"AwsRdsDbClusterSnaphot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

`AwsRdsDbInstance` 객체는 Amazon RDS DB 인스턴스에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsRdsDbInstance 보여줍니다. AwsRdsDbInstance속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsRdsDbInstanceDetails.

예

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
    "DbParameterGroups": [
        {
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
```

```
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
```

```
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

`AwsRdsDbSecurityGroup` 객체에는 Amazon Relational Database Service에 대한 정보가 포함됩니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsRdsDbSecurityGroup` 보여줍니다. `AwsRdsDbSecurityGroup`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsRdsDbSecurityGroupDetails.

예

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
    ],
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

`AwsRdsDbSnapshot` 객체에는 Amazon RDS DB 클러스터 스냅샷에 대한 세부 정보가 포함됩니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsRdsDbSnapshot` 보여줍니다. `AwsRdsDbSnapshot`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsRdsDbSnapshotDetails.

예

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

`AwsRdsEventSubscription`에는 RDS 이벤트 알림 구독에 대한 세부 정보가 들어 있습니다. 구독을 통해 RDS는 SNS 주제에 이벤트를 게시할 수 있습니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsRdsEventSubscription` 보여줍니다. `AwsRdsEventSubscription`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsRdsEventSubscriptionDetails.

예

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
```

```
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift

다음은 `AwsRedshift` 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsRedshiftCluster

`AwsRedshiftCluster` 객체에는 Amazon Redshift 클러스터에 대한 세부 정보가 포함됩니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsRedshiftCluster` 보여줍니다. `AwsRedshiftCluster`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsRedshiftClusterDetails.

예

```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
```

```
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
             "PrivateIPAddress": "192.0.2.224",
             "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
```

```
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
```

```
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "test-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
```

```
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
```

```
}
```

AwsRoute53

다음은 AwsRoute53 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsRoute53HostedZone

AwsRoute53HostedZone객체는 호스팅 영역에 할당된 4개의 이름 서버를 포함하여 Amazon Route 53 호스팅 영역에 대한 정보를 제공합니다. 호스팅 영역은 단일 상위 도메인 이름에 속하는 함께 관리할 수 있는 레코드 컬렉션을 나타냅니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsRoute53HostedZone 보여줍니다. AwsRoute53HostedZone속성에 대한 설명을 보려면 AWS Security Hub API HostedZoneDetails 참조의 AwsRoute 53을 참조하십시오.

예

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
```

```
            "Region": "us-east-1"
        }
    ]
}
```

AwsS3

다음은 AwsS3 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsS3AccessPoint

AwsS3AccessPoint는 Amazon S3 액세스 포인트에 대한 정보를 제공합니다. S3 액세스 포인트는 S3 객체 작업을 수행하는 데 사용할 수 있는 S3 버킷에 연결된 네트워크 엔드포인트입니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsS3AccessPoint 보여줍니다. AwsS3AccessPoint속성에 대한 설명을 보려면 API 참조의 AccessPointDetailsAWSS3를AWS Security Hub 참조하십시오.

예

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "DOC-EXAMPLE-BUCKET1",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

AwsS3AccountPublicAccessBlock은 계정의 Amazon S3 퍼블릭 액세스 차단 구성에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsS3AccountPublicAccessBlock 보여줍니다. AwsS3AccountPublicAccessBlock속성에 대한 설명을 보려면 API 참조의 AccountPublicAccessBlockDetailsAWSS3를AWS Security Hub 참조하십시오.

예

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

AwsS3Bucket 객체는 Amazon S3 버킷에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsS3Bucket 보여줍니다. AwsS3Bucket속성에 대한 설명을 보려면 API 참조의 BucketDetailsAWSS3를AWS Security Hub 참조하십시오.

예

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
               "Filter": {
                   "Predicate": {
                       "Operands": [
                           {
                               "Prefix": "tmp/",
                               "Type": "LifecyclePrefixPredicate"
                           },
```

```
                        {
                            "Tag": {
                                "Key": "ArchiveAge",
                                "Value": "9m"
                            },
                            "Type": "LifecycleTagPredicate"
                        }
                    ],
                    "Type": "LifecycleAndOperator"
                }
            },
            "ID": "Move rotated logs to Glacier",
            "NoncurrentVersionExpirationInDays": -1,
            "NoncurrentVersionTransitions": [
                {
                    "Days": 2,
                    "StorageClass": "GLACIER"
                }
            ],
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2020-11-10T00:00:00.000Z",
                    "Days": 100,
                    "StorageClass": "GLACIER"
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-858726136312",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "DOC-EXAMPLE-BUCKET1",
"BucketNotificationConfiguration": {
 "Configurations": [{
  "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
  "Events": [
   "s3:ObjectCreated:Put"
  ],
  "Filter": {
   "S3KeyFilter": {
```

```
        "FilterRules": [
        {
         "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
         "Value": "pre"
        },
        {
         "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
         "Value": "suf"
        },
        ]
       }
      },
      "Type": "LambdaConfiguration"
     }]
    },
    "BucketVersioningConfiguration": {
     "IsMfaDeleteEnabled": true,
     "Status": "Off"
    },
    "BucketWebsiteConfiguration": {
     "ErrorDocument": "error.html",
     "IndexDocumentSuffix": "index.html",
     "RedirectAllRequestsTo": {
      "HostName": "example.com",
      "Protocol": "http"
     },
     "RoutingRules": [{
      "Condition": {
       "HttpErrorCodeReturnedEquals": "Redirected",
       "KeyPrefixEquals": "index"
        },
      "Redirect": {
       "HostName": "example.com",
       "HttpRedirectCode": "401",
       "Protocol": "HTTP",
       "ReplaceKeyPrefixWith": "string",
       "ReplaceKeyWith": "string"
      }
     }]
    },
    "CreatedAt": "2007-11-30T01:46:56.000Z",
    "ObjectLockConfiguration": {
     "ObjectLockEnabled": "Enabled",
     "Rule": {
```

```
      "DefaultRetention": {
       "Days": null,
       "Mode": "GOVERNANCE",
       "Years": 12
      },
     },
    },
    "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
    "OwnerName": "s3bucketowner",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true,
    },
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
     }
}
```

AwsS3Object

`AwsS3Object` 객체는 Amazon S3 객체에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsS3Object` 보여줍니다. `AwsS3Object`속성에 대한 설명을 보려면 API 참조의 ObjectDetailsAWSS3를AWS Security Hub 참조하십시오.

예

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
```

```
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker

다음은 AwsSageMaker 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsSageMakerNotebookInstance

AwsSageMakerNotebookInstance객체는 Jupyter Notebook 앱을 실행하는 기계 학습 컴퓨팅 인스턴스인 Amazon SageMaker 노트북 인스턴스에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 탐지 형식 (ASFF) 을 보여줍니다. AwsSageMakerNotebookInstance AwsSageMakerNotebookInstance속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsSageMakerNotebookInstanceDetails.

예

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
```

```
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager

다음은 AwsSecretsManager 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsSecretsManagerSecret

이 AwsSecretsManagerSecret 객체는 Secrets Manager 암호에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsSecretsManagerSecret 보여줍니다. AwsSecretsManagerSecret속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsSecretsManagerSecretDetails.

예

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns

다음은 AwsSns 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsSnsTopic

AwsSnsTopic 객체에는 Amazon Simple Notification Service 주제에 대한 세부 정보가 포함됩니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsSnsTopic 보여줍니다. AwsSnsTopic속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsSnsTopicDetails.

예

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
         "Endpoint": "http://sampleendpoint.com",
         "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

AwsSqs

다음은 AwsSqs 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsSqsQueue

AwsSqsQueue 객체에는 Amazon Simple Queue Service 대기열에 대한 정보가 들어 있습니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsSqsQueue 보여줍니다. AwsSqsQueue속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsSqsQueueDetails.

예

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
    "QueueName": "sample-queue"
}
```

AwsSsm

다음은 AwsSsm 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsSsmPatchCompliance

AwsSsmPatchCompliance 객체는 인스턴스를 패치하는 데 사용된 패치 기준선을 기반으로 인스턴스의 패치 상태에 대한 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsSsmPatchCompliance 보여줍니다. AwsSsmPatchCompliance속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsSsmPatchComplianceDetails.

예

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions

다음은 AwsStepFunctions 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsStepFunctionStateMachine

AwsStepFunctionStateMachine 객체는 일련의 이벤트 기반 단계로 구성된 워크플로인 AWS Step Functions 상태 시스템에 대한 정보를 제공합니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsStepFunctionStateMachine 보여줍니다. AwsStepFunctionStateMachine속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsStepFunctionStateMachine.

예

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf

다음은 AwsWaf 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsWafRateBasedRule

AwsWafRateBasedRule 객체에는 글로벌 리소스의 AWS WAF 속도 기반 규칙에 대한 세부 정보가 들어 있습니다. AWS WAF 속도 기반 규칙은 요청을 허용, 차단 또는 집계할 시기를 지정하는 설정을 제공합니다. 속도 기반 규칙은 지정된 기간 동안 도착한 요청 수를 포함합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. AwsWafRateBasedRule AwsWafRateBasedRule속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsWafRateBasedRuleDetails.

예

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

AwsWafRegionalRateBasedRule 객체에는 리전 리소스의 속도 기반 규칙에 대한 세부 정보가 들어 있습니다. 속도 기반 규칙은 요청을 허용, 차단 또는 계산할 시기를 지정하는 설정을 제공합니다. 속도 기반 규칙은 지정된 기간 동안 도착한 요청 수를 포함합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 AwsWafRegionalRateBasedRule 보여줍니다. AwsWafRegionalRateBasedRule속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsWafRegionalRateBasedRuleDetails.

예

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
```

```
}
```

AwsWafRegionalRule

`AwsWafRegionalRule`객체는 AWS WAF 지역 규칙에 대한 세부 정보를 제공합니다. 이 규칙은 허용, 차단 또는 계산하려는 웹 요청을 식별합니다.

다음 예제는 `AwsWafRegionalRule` 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. `AwsWafRegionalRule`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsWafRegionalRuleDetails.

예

```
"AwsWafRegionalRule": {
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

`AwsWafRegionalRuleGroup` 객체는 AWS WAF 리전 규칙 그룹에 대한 세부 정보를 제공합니다. 규칙 그룹은 웹 액세스 제어 목록(웹 ACL)에 추가하는 사전 정의된 규칙 모음입니다.

다음 예는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsWafRegionalRuleGroup` 보여줍니다. `AwsWafRegionalRuleGroup`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsWafRegionalRuleGroupDetails.

예

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
```

```
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl` AWS WAF 지역별 웹 액세스 제어 목록 (웹 ACL) 에 대한 세부 정보를 제공합니다. 웹 ACL에는 허용, 차단 또는 계산할 요청을 식별하는 규칙이 포함되어 있습니다.

다음은 AWS Security Finding 형식(ASFF)의 `AwsWafRegionalWebAcl` 결과의 예입니다. `AwsApiGatewayV2Stage`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsWafRegionalWebAclDetails.

예

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
```

```
}
```

AwsWafRule

`AwsWafRule` AWS WAF 규칙에 대한 정보를 제공합니다. AWS WAF 규칙은 허용, 차단 또는 집계하려는 웹 요청을 식별합니다.

다음은 AWS 보안 검색 결과 형식 (ASFF) 에서의 `AwsWafRule` 검색 결과의 예시입니다. `AwsApiGatewayV2Stage`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsWafRuleDetails.

예

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup` AWS WAF 규칙 그룹에 대한 정보를 제공합니다. AWS WAF 규칙 그룹은 웹 액세스 제어 목록(웹 ACL)에 추가하는 미리 정의된 규칙의 모음입니다.

다음은 AWS 보안 검색 형식 (ASFF) 에서 `AwsWafRuleGroup` 찾은 예제입니다. `AwsApiGatewayV2Stage`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsWafRuleGroupDetails.

예

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
```

```
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

`AwsWafv2RuleGroup`개체는 AWS WAF V2 규칙 그룹에 대한 세부 정보를 제공합니다.

다음 예제는 `AwsWafv2RuleGroup` 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. `AwsWafv2RuleGroup`속성에 대한 설명을 보려면 AWS Security Hub API RuleGroupDetails 참조의 AwsWafv 2를 참조하십시오.

예

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
```

```
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

`AwsWafWebAcl`객체는 AWS WAF 웹 ACL에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsWafWebAcl` 보여줍니다. `AwsWafWebAcl`속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsWafWebAclDetails.

예

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
```

```
}
```

AwsWafv2WebAcl

`AwsWafv2WebAcl`객체는 AWS WAF V2 웹 ACL에 대한 세부 정보를 제공합니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 `AwsWafv2WebAcl` 보여줍니다. `AwsWafv2WebAcl`속성에 대한 설명을 보려면 AWS Security Hub API WebAclDetails 참조의 AwsWafv 2를 참조하십시오.

예

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
```

```
      "CloudWatchMetricsEnabled": true,
      "MetricName": "TestingJsonBodyMetric"
    }
}
```

AwsXray

다음은 AwsXray 리소스에 대한 AWS 보안 검색 형식의 예입니다.

AwsXrayEncryptionConfig

AwsXrayEncryptionConfig객체에는 의 암호화 구성에 대한 정보가 들어 있습니다. AWS X-Ray

다음 예제는 AwsXrayEncryptionConfig 객체의 AWS 보안 검색 형식 (ASFF) 을 보여줍니다. AwsXrayEncryptionConfig속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 AwsXrayEncryptionConfigDetails.

예

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

Container

결과와 관련된 컨테이너 세부 정보입니다.

다음 예제는 객체의 AWS 보안 검색 형식 (ASFF) 을 Container 보여줍니다. Container속성에 대한 설명을 보려면 AWS Security Hub API 참조를 참조하십시오 ContainerDetails.

예

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
```

```
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Other

`Other` 객체를 사용하여 사용자 지정 필드 및 값을 입력할 수 있습니다. `Other` 객체는 다음과 같은 경우에 사용합니다.

- 리소스 유형에 해당 `Details` 객체가 없습니다. 리소스에 대한 세부 정보를 입력하려면 `Other` 객체를 사용합니다.
- 리소스 유형에 대한 `Details` 객체에는 채우려는 모든 속성이 포함되어 있지 않습니다. 이 경우 리소스 유형의 `Details` 객체를 사용하여 사용 가능한 필드를 채웁니다. `Other` 객체를 사용하여 유형별 객체에 없는 속성을 채울 수 있습니다.
- 리소스 유형이 제공된 유형 중 하나가 아닙니다. 이 경우 `Resource.Type`을 `Other`로 설정하고 `Other` 객체를 사용하여 세부 정보를 채웁니다.

유형: 최대 50개의 키-값 쌍의 맵

각 키-값 쌍은 다음 요구 사항을 충족해야 합니다.

- 키는 128자 미만이어야 합니다.
- 값은 1,024자 미만이어야 합니다.

AWS Security Hub에서의 인사이트

AWS Security Hub 통찰력은 관련 결과의 모음입니다. 이는 주의와 개입이 필요한 보안 영역을 식별합니다. 예를 들어, 통찰력은 보안이 취약한 것으로 감지된 EC2 인스턴스를 지정할 수 있습니다. 통찰력은 전체 결과 공급자의 결과를 함께 나타냅니다.

각 통찰력은 그룹화 기준 문과 선택적 필터에 의해 정의됩니다. 그룹화 기준 문은 일치하는 결과를 그룹화하는 방법을 나타내며 통찰력이 적용되는 항목 유형을 식별합니다. 예를 들어 통찰력이 리소스 식별자별로 그룹화된 경우 통찰력은 리소스 식별자 목록을 생성합니다. 선택적 필터는 통찰력과 일치하는 결과의 범위를 식별합니다. 예를 들어 특정 공급자의 결과나 특정 리소스 유형과 연관된 결과만 볼 수 있습니다.

Security Hub에서는 여러 가지 기본 제공 관리형 통찰력을 제공합니다. 관리형 통찰력은 수정하거나 삭제할 수 없습니다.

AWS 환경 및 사용에 따른 고유한 보안 문제를 추적하기 위해 사용자 지정 통찰력을 생성할 수 있습니다.

통찰력은 일치하는 결과를 생성하는 통합 또는 표준을 활성화한 경우에만 결과를 반환합니다. 예를 들어, 관리형 통찰력 29. Top resources by counts of failed CIS checks(실패한 CIS 점검 횟수별 상위 리소스)는 CIS AWS 기반 표준을 활성화한 경우에만 결과를 반환합니다.

주제

인사이트 목록 보기 및 필터링

인사이트 페이지에는 사용 가능한 인사이트 목록이 표시됩니다.

기본적으로 목록에는 관리형 인사이트와 사용자 지정 인사이트가 모두 표시됩니다. 인사이트 유형을 기반으로 인사이트 목록을 필터링하려면 필터 필드 옆에 있는 드롭다운 메뉴에서 인사이트 유형을 선택합니다.

- 사용 가능한 인사이트를 모두 표시하려면 모든 인사이트를 선택합니다. 이 항목이 기본 옵션입니다.

- 관리형 인사이트만 표시하려면 Security Hub 관리형 인사이트를 선택합니다.
- 사용자 지정 인사이트만 표시하려면 사용자 지정 인사이트를 선택합니다.

또한, 인사이트 이름의 텍스트를 기반으로 인사이트 목록을 필터링할 수 있습니다.

필터 필드에 목록을 필터링하는 데 사용할 텍스트를 입력합니다. 필터는 대소문자를 구분하지 않습니다. 필터는 인사이트 이름의 모든 위치에서 텍스트가 포함된 인사이트를 찾습니다.

인사이트 결과 및 조사 결과 보기 및 조치 수행

AWS Security Hub는 각 인사이트에 대해 먼저 필터 기준과 일치하는 결과를 확인한 다음 그룹화 속성을 사용하여 일치하는 결과를 그룹화합니다.

인사이트 페이지에서 결과 및 조사 결과를 보고 조치를 취할 수 있습니다.

리전 간 집계를 활성화하면, 집계 리전에는 관리형 인사이트 결과에 집계 지역 및 연결된 리전에서 나온 조사 결과가 포함됩니다. 사용자 지정 인사이트 결과의 경우 인사이트가 리전별로 필터링되지 않으면 집계 리전 및 연결된 리전의 조사 결과가 결과에 포함됩니다.

다른 리전에는 인사이트 결과가 해당 리전에 대한 것만 해당됩니다.

리전 간 집계를 구성하는 방법에 대한 자세한 내용은 크로스 리전 집계 활성화을 참고하십시오.

인사이트 결과 보기 및 조치 수행(콘솔)

인사이트 결과는 인사이트에 대한 결과의 그룹화된 목록으로 구성됩니다. 예를 들어 인사이트이 리소스 ID별로 그룹화된 경우 인사이트 결과는 리소스 ID의 목록입니다. 결과 목록의 각 항목은 해당 항목에 일치하는 조사 결과 수를 나타냅니다.

조사 결과를 리소스 식별자 또는 리소스 유형으로 그룹화하는 경우 조사 결과에는 일치하는 조사 결과에 있는 모든 리소스가 포함됩니다. 여기에는 필터 기준의 리소스 유형과 유형이 다른 리소스가 포함됩니다. 예를 들어, 인사이트 는 S3 버킷과 관련된 조사 결과를 식별합니다. 일치하는 조사 결과에 S3 버킷 리소스와 IAM 액세스 키 리소스가 모두 포함된 경우 인사이트 결과에는 두 리소스가 모두 포함됩니다.

결과 목록은 가장 일치하는 조사 결과부터 순서대로 정렬됩니다.

Security Hub는 결과를 100개만 표시할 수 있습니다. 그룹화 값이 100개를 초과하는 경우 처음 100개만 표시됩니다.

결과 목록 외에도 인사이트 결과에는 다음 속성에 대해 일치하는 조사 결과 수를 요약하는 차트 세트가 표시됩니다.

- 심각도 레이블 - 각 심각도 레이블에 대한 조사 결과 수
- AWS 계정 ID — 매칭 결과에 대한 상위 5개 계정 ID
- 리소스 유형 - 일치하는 조사 결과에 대한 상위 5개 리소스 유형
- 리소스 ID - 일치하는 조사 결과에 대한 상위 5개 리소스 ID
- 제품 이름 - 일치하는 조사 결과에 대한 상위 5개 조사 결과 공급자

사용자 지정 작업을 구성한 경우 선택한 결과를 사용자 지정 작업으로 보낼 수 있습니다. 작업은 `Security Hub Insight Results` 이벤트 유형의 CloudWatch 규칙과 연결되어야 합니다. the section called “자동 응답 및 해결” 섹션을 참조하십시오.

사용자 지정 작업을 구성하지 않으면 작업 메뉴가 비활성화됩니다.

인사이트 결과 목록을 표시하고 조치를 취하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 Insights를 선택합니다.
3. 인사이트 결과 목록을 표시하려면 인사이트 이름을 선택합니다.
4. 사용자 지정 작업으로 보낼 각 결과에 대한 확인란을 선택합니다.
5. 작업 메뉴에서 사용자 지정 작업을 선택합니다.

인사이트 결과 보기(Security Hub API, AWS CLI)

인사이트 결과를 보려면 API 호출 또는 AWS Command Line Interface을 사용할 수 있습니다.

인사이트 결과를 보려면 (Security Hub API, AWS CLI)

- Security Hub API - `GetInsightResults` 작업을 사용합니다. 결과를 반환할 인사이트를 식별하려면 인사이트 ARN이 필요합니다. 사용자 지정 인사이트를 위한 인사이트 ARN을 얻으려면 `GetInsights` 작업을 사용하십시오.
- AWS CLI – 명령줄에서 `get-insight-results` 명령을 실행합니다.

```
aws securityhub get-insight-results --insight-arn <insight ARN>
```

예제

```
aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

인사이트 조사 결과에 대한 조사 결과 보기(콘솔)

인사이트 결과 목록에서 각 결과에 대한 조사 결과 목록을 표시할 수 있습니다.

인사이트 조사 결과를 표시하고 조치를 취하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 Insights를 선택합니다.
3. 인사이트 결과 목록을 표시하려면 인사이트 이름을 선택합니다.
4. 인사이트 결과에 대한 조사 결과 목록을 표시하려면 결과 목록에서 항목을 선택합니다.

조사 결과 목록에는 워크플로우 상태가 `NEW` 또는 `NOTIFIED`인 선택한 통합에 대한 활성 조사 결과가 표시됩니다.

조사 결과 목록에서 다음 작업을 수행할 수 있습니다.

- 목록 필터 및 그룹화 변경
- 개별 조사 결과에 대한 세부 정보 보기
- 조사 결과의 워크플로 상태 업데이트
- 사용자 지정 작업에 조사 결과 전송

관리형 인사이트

AWS에서는 여러 관리형 인사이트를 제공합니다.

관리형 인사이트은 편집하거나 삭제할 수 없습니다. 인사이트 결과와 검색 결과를 보고 조치를 취할 수 있습니다. 관리형 인사이트를 새 사용자 지정 인사이트의 기반으로 사용할 수도 있습니다.

다른 모든 인사이트과 마찬가지로, 관리형 인사이트은 일치하는 결과를 생성할 수 있는 제품 통합 또는 보안 표준을 활성화한 경우에만 결과를 반환합니다.

리소스 식별자별로 그룹화된 인사이트의 경우 결과에는 일치하는 조사 결과에 있는 모든 리소스의 식별자가 포함됩니다. 여기에는 필터 기준의 리소스 유형과 유형이 다른 리소스가 포함됩니다. 예를 들어, 인사이트 2는 Amazon S3 버킷과 관련된 조사 결과를 식별합니다. 일치하는 조사 결과에 S3 버킷 리소스와 IAM 액세스 키 리소스가 모두 포함된 경우 인사이트 결과에는 두 리소스가 모두 포함됩니다.

Security Hub는 다음과 같은 관리형 인사이트를 제공합니다.

1. 가장 많은 결과가 포함된 AWS 리소스

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   그룹화 기준: 리소스 식별자

   조사 결과 필터:

   - 레코드 상태가 `ACTIVE`임
   - 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임
2. 퍼블릭 쓰기 또는 읽기 권한이 있는 S3 버킷

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

   그룹화 기준: 리소스 식별자

   조사 결과 필터:

   - 유형이 `Effects/Data Exposure`로 시작
   - 리소스 유형이 `AwsS3Bucket`임
   - 레코드 상태가 `ACTIVE`임
   - 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임
3. 가장 많은 결과를 생성하는 AMI

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   그룹화 기준: EC2 인스턴스 이미지 ID

   조사 결과 필터:

   - 리소스 유형이 `AwsEc2Instance`임
   - 레코드 상태가 `ACTIVE`임
   - 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임

4. 알려진 Tactics, Techniques, and Procedures(TTP)와 관련된 EC2 인스턴스

   ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

   그룹화 기준: 리소스 ID

   조사 결과 필터:

   - 유형이 `TTPs`로 시작
   - 리소스 유형이 `AwsEc2Instance`임
   - 레코드 상태가 `ACTIVE`임
   - 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임

5. 액세스 키 활동이 의심스러운 AWS 보안 주체

   ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

   그룹화 기준: IAM 액세스 키 보안 주체 이름

   조사 결과 필터:

   - 리소스 유형이 `AwsIamAccessKey`임
   - 레코드 상태가 `ACTIVE`임
   - 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임

6. 보안 표준/모범 사례를 준수하지 않는 AWS 리소스 인스턴스

   ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

   그룹화 기준: 리소스 ID

   조사 결과 필터:

   - 유형이 `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`임
   - 레코드 상태가 `ACTIVE`임
   - 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임

7. 잠재적인 데이터 유출과 관련된 AWS 리소스

   ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

   그룹화 기준:: 리소스 ID

조사 결과 필터:

- 유형이 Effects/Data Exfiltration/로 시작
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

8. 무단 리소스 사용과 관련된 AWS 리소스

ARN: arn:aws:securityhub:::insight/securityhub/default/8

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 Effects/Resource Consumption로 시작
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

9. 보안 표준/모범 사례를 준수하지 않는 S3 버킷

ARN: arn:aws:securityhub:::insight/securityhub/default/11

그룹화 기준: 리소스 ID

조사 결과 필터:

- 리소스 유형이 AwsS3Bucket임
- 유형이 Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

10. 민감한 데이터가 포함된 S3 버킷

ARN: arn:aws:securityhub:::insight/securityhub/default/12

그룹화 기준: 리소스 ID

조사 결과 필터:

- 리소스 유형이 AwsS3Bucket임
- 유형이 Sensitive Data Identifications/로 시작
- 레코드 상태가 ACTIVE임

- 워크플로우 상태가 NEW 또는 NOTIFIED임

11. 유출되었을 수 있는 자격 증명

    ARN: arn:aws:securityhub:::insight/securityhub/default/13

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 유형이 Sensitive Data Identifications/Passwords/로 시작
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

12. 중요한 취약성에 대한 보안 패치가 없는 EC2 인스턴스

    ARN: arn:aws:securityhub:::insight/securityhub/default/16

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 유형이 Software and Configuration Checks/Vulnerabilities/CVE로 시작
    - 리소스 유형이 AwsEc2Instance임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

13. 전반적으로 비정상적 동작을 하는 EC2 인스턴스

    ARN: arn:aws:securityhub:::insight/securityhub/default/17

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 유형이 Unusual Behaviors로 시작
    - 리소스 유형이 AwsEc2Instance임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

14. 인터넷에서 액세스할 수 있는 포트가 있는 EC2 인스턴스

    ARN: arn:aws:securityhub:::insight/securityhub/default/18

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 Software and Configuration Checks/AWS Security Best Practices/Network Reachability로 시작
- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

15. 보안 표준/모범 사례를 준수하지 않는 EC2 인스턴스

ARN: arn:aws:securityhub:::insight/securityhub/default/19

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 다음 중 하나로 시작:
  - Software and Configuration Checks/Industry and Regulatory Standards/
  - Software and Configuration Checks/AWS Security Best Practices
- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

16. 인터넷에 개방된 EC2 인스턴스

ARN: arn:aws:securityhub:::insight/securityhub/default/21

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 Software and Configuration Checks/AWS Security Best Practices/Network Reachability로 시작
- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

17. 공격자 정찰과 관련된 EC2 인스턴스

ARN: arn:aws:securityhub:::insight/securityhub/default/22

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 TTPs/Discovery/Recon으로 시작
- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

18. 맬웨어와 관련된 AWS 리소스

ARN: arn:aws:securityhub:::insight/securityhub/default/23

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 다음 중 하나로 시작:
  - Effects/Data Exfiltration/Trojan
  - TTPs/Initial Access/Trojan
  - TTPs/Command and Control/Backdoor
  - TTPs/Command and Control/Trojan
  - Software and Configuration Checks/Backdoor
  - Unusual Behaviors/VM/Backdoor
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

19. 암호 화폐 문제와 관련된 AWS 리소스

ARN: arn:aws:securityhub:::insight/securityhub/default/24

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 다음 중 하나로 시작:
  - Effects/Resource Consumption/Cryptocurrency
  - TTPs/Command and Control/CryptoCurrency
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

20. 무단 액세스 시도가 있는 AWS 리소스

    ARN: arn:aws:securityhub:::insight/securityhub/default/25

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 유형이 다음 중 하나로 시작:
      - TTPs/Command and Control/UnauthorizedAccess
      - TTPs/Initial Access/UnauthorizedAccess
      - Effects/Data Exfiltration/UnauthorizedAccess
      - Unusual Behaviors/User/UnauthorizedAccess
      - Effects/Resource Consumption/UnauthorizedAccess
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

21. 지난 주에 가장 많은 조회수를 기록한 위협 인텔리전스 지표

    ARN: arn:aws:securityhub:::insight/securityhub/default/26

    조사 결과 필터:

    - 지난 7일 이내에 생성됨

22. 결과 개수 기준 상위 계정

    ARN: arn:aws:securityhub:::insight/securityhub/default/27

    그룹화 기준: AWS 계정 ID

    조사 결과 필터:

    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

23. 결과 개수 기준 상위 제품

    ARN: arn:aws:securityhub:::insight/securityhub/default/28

    그룹화 기준: 제품 이름

    조사 결과 필터:

    - 레코드 상태가 ACTIVE임

- 워크플로우 상태가 NEW 또는 NOTIFIED임

24. 결과 개수 기준 심각도

    ARN: arn:aws:securityhub:::insight/securityhub/default/29

    그룹화 기준: 심각도 레이블

    조사 결과 필터:

    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

25. 결과 개수 기준 상위 S3 버킷

    ARN: arn:aws:securityhub:::insight/securityhub/default/30

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 리소스 유형이 AwsS3Bucket임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

26. 결과 개수 기준 상위 EC2 인스턴스

    ARN: arn:aws:securityhub:::insight/securityhub/default/31

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 리소스 유형이 AwsEc2Instance임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

27. 결과 개수 기준별 상위 AMI

    ARN: arn:aws:securityhub:::insight/securityhub/default/32

    그룹화 기준: EC2 인스턴스 이미지 ID

    조사 결과 필터:

    - 리소스 유형이 AwsEc2Instance임
    - 레코드 상태가 ACTIVE임

- 워크플로우 상태가 NEW 또는 NOTIFIED임

28. 결과 개수 기준 상위 IAM 사용자

    ARN: arn:aws:securityhub:::insight/securityhub/default/33

    그룹화 기준: IAM 액세스 키 ID

    조사 결과 필터:

    - 리소스 유형이 AwsIamAccessKey임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

29. CIS 점검 실패 횟수 기준 상위 리소스

    ARN: arn:aws:securityhub:::insight/securityhub/default/34

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 생성기 ID가 arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule로 시작
    - 마지막 날에 업데이트됨
    - 규정 준수 상태가 FAILED임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

30. 결과 개수 기준 상위 통합

    ARN: arn:aws:securityhub:::insight/securityhub/default/35

    그룹화 기준: 제품 ARN

    조사 결과 필터:

    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

31. 가장 실패한 보안 검사가 있는 리소스

    ARN: arn:aws:securityhub:::insight/securityhub/default/36

    그룹화 기준: 리소스 ID

조사 결과 필터:

- 마지막 날에 업데이트됨
- 규정 준수 상태가 FAILED임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

32. 활동이 의심스러운 IAM 사용자

ARN: arn:aws:securityhub:::insight/securityhub/default/37

그룹화 기준: IAM 사용자

조사 결과 필터:

- 리소스 유형이 AwsIamUser임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

33. 가장 많은 결과가 포함된 AWS Health 리소스

ARN: arn:aws:securityhub:::insight/securityhub/default/38

그룹화 기준: 리소스 ID

조사 결과 필터:

- ProductName equals Health

34. 가장 많은 결과가 포함된 AWS Config 리소스

ARN: arn:aws:securityhub:::insight/securityhub/default/39

그룹화 기준: 리소스 ID

조사 결과 필터:

- ProductName equals Config

35. 가장 많은 결과가 포함된 애플리케이션

ARN: arn:aws:securityhub:::insight/securityhub/default/40

그룹화 기준: ResourceApplicationArn

조사 결과 필터:

- `RecordState` equals `ACTIVE`
- `Workflow.Status` 같음 `NEW` 또는 `NOTIFIED`

사용자 지정 통찰력

AWS Security Hub 관리형 통찰력 외에도 사용자 환경에 맞는 문제를 추적하는 사용자 지정 통찰력을 Security Hub에서 생성할 수 있습니다. 사용자 지정 통찰력 문제에 대해 큐레이션된 부분 집합을 추적하는 방법을 제공합니다

설정하는 데 유용할 수 있는 사용자 지정 통찰력의 몇 가지 예는 다음과 같습니다.

- 관리자 계정을 소유하고 있는 경우, 사용자 지정 통찰력을 설정하여 구성원 계정에 영향을 미치는 중요하고 심각도가 높은 조사 결과를 추적할 수 있습니다.
- 통합된 특정 AWS 서비스를 사용하는 경우, 사용자 지정 통찰력을 설정하여 해당 서비스의 중요하고 심각도가 높은 조사 결과를 추적할 수 있습니다.
- 타사 통합을 사용하는 경우, 사용자 지정 통찰력을 설정하여 해당 통합 제품에서 중요하고 심각도가 높은 결과를 추적할 수 있습니다.

완전히 새로운 사용자 지정 통찰력을 생성하거나 기존 사용자 지정 통찰력 또는 관리형 통찰력을 시작할 수 있습니다.

각 통찰력은 다음 옵션으로 구성됩니다.

- 그룹화 속성 – 그룹화 속성은 통찰력 결과 목록에 표시되는 항목을 결정합니다. 예를 들어, 그룹화 속성이 제품 이름이면 통찰력 결과에 각 결과 공급자와 연관된 결과 수가 표시됩니다.
- 선택적 필터 - 필터는 통찰력과 일치하는 결과의 범위를 좁힙니다.

  Security Hub에서는 결과를 쿼리할 때 필터 세트에 Boolean AND 로직을 적용합니다. 즉, 결과는 제공된 모든 필터와 일치해야 합니다. 예를 들어, 필터가 “제품 이름이 GuardDuty임” 및 “리소스 유형이 `AwsS3Bucket`임“인 경우 일치하는 결과는 이 두 기준과 일치해야 합니다.

  그러나 Security Hub에서는 속성은 동일하지만 다른 값을 사용하는 필터에 Boolean OR 로직을 적용합니다. 예를 들어, 필터가 “제품 이름이 GuardDuty임“이고 “제품 이름이 Amazon Inspector임“이면 GuardDuty 또는 Amazon Inspector에 의해 생성된 경우 결과가 일치합니다.

리소스 식별자 또는 리소스 유형을 그룹화 속성으로 사용하는 경우 통찰력 결과에는 일치하는 조사 결과에 있는 모든 리소스가 포함됩니다. 이 목록은 리소스 유형 필터와 일치하는 리소스에만 국한되지 않

습니다. 예를 들어, 통찰력은 S3 버킷과 관련된 조사 결과를 식별하고 해당 결과를 리소스 식별자별로 그룹화합니다. 일치하는 조사 결과에는 S3 버킷 리소스와 IAM 액세스 키 리소스가 모두 포함됩니다. 통찰력 결과에는 두 리소스가 모두 포함됩니다.

사용자 지정 통찰력 생성(콘솔)

콘솔에서 완전히 새로운 통찰력을 생성할 수 있습니다.

사용자 지정 통찰력을 생성하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 Insights를 선택합니다.
3. Create insight(통찰력 생성)를 선택하십시오.
4. 통찰력에 대한 그룹화 속성을 선택하려면
   a. 검색 상자를 선택하여 필터 옵션을 표시합니다.
   b. 그룹화 기준을 선택합니다.
   c. 이 통찰력과 관련되어 있는 결과를 그룹화하는 데 사용할 속성을 선택합니다.
   d. Apply(적용)를 선택합니다.
5. (선택 사항) 이 통찰력에 사용할 추가 필터를 선택합니다. 각 필터에 대해 필터 기준을 정의한 다음 적용를 선택합니다.
6. Create insight(통찰력 생성)를 선택하십시오.
7. Insight name(통찰력 이름)을 입력한 다음 Create insight(통찰력 생성)를 선택합니다.

사용자 지정 통찰력 생성(프로그래밍 방식)

선호하는 방법을 선택하고 단계에 따라 Security Hub에서 프로그래밍 방식으로 사용자 지정 통찰력을 생성합니다. 필터를 지정하여 통찰력의 조사 결과 모음을 특정 하위 집합으로 좁힐 수 있습니다.

다음 탭에는 사용자 지정 통찰력을 생성하기 위한 지침이 몇 가지 언어로 포함되어 있습니다. 추가 언어에 대한 지원이 필요하면 AWS에서의 빌드 도구를 참조하십시오.

Security Hub API

1. `CreateInsight` 작업을 실행합니다.
2. 사용자 지정 통찰력의 이름을 `Name` 매개변수에 입력합니다.

3. 통찰력에 포함할 조사 결과를 지정하기 위해 `Filters` 매개변수를 채웁니다.
4. `GroupByAttribute` 매개 변수를 채워 통찰력에 포함된 조사 결과를 그룹화하는 데 사용할 속성을 지정합니다.
5. 선택적으로 `SortCriteria` 파라미터를 채워 특정 필드를 기준으로 결과를 정렬할 수 있습니다.

크로스 리전 집계를 활성화하고 집계 리전에서 이 API를 호출하면 집계 및 연결된 리전에서 일치하는 조사 결과에 통찰력이 적용됩니다.

AWS CLI

1. 명령줄에서 `create-insight` 명령을 실행합니다.
2. 사용자 지정 통찰력의 이름을 `name` 매개변수에 입력합니다.
3. 통찰력에 포함할 조사 결과를 지정하기 위해 `filters` 매개변수를 채웁니다.
4. `group-by-attribute` 매개 변수를 채워 통찰력에 포함된 조사 결과를 그룹화하는 데 사용할 속성을 지정합니다.

크로스 리전 집계를 활성화하고 집계 리전에서 이 명령을 실행하면 집계 및 연결된 리전에서 나온 일치하는 조사 결과에 통찰력이 적용됩니다.

```
aws securityhub create-insight --name <insight name> --filters <filter values> --
group-by-attribute <attribute name>
```

예

```
aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

1. `New-SHUBInsight` cmdlet을 사용하십시오.
2. 사용자 지정 통찰력의 이름을 `Name` 매개변수에 입력합니다.
3. 통찰력에 포함할 조사 결과를 지정하기 위해 `Filter` 매개변수를 채웁니다.
4. `GroupByAttribute` 매개 변수를 채워 통찰력에 포함된 조사 결과를 그룹화하는 데 사용할 속성을 지정합니다.

크로스 리전 집계를 활성화하고 집계 리전에서 이 cmdlet를 사용하는 경우, 집계 및 연결된 리전에서 나온 일치하는 조사 결과에 통찰력이 적용됩니다.

예

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

사용자 지정 통찰력 수정(콘솔)

기존 사용자 지정 통찰력을 수정하여 그룹화 값과 필터를 변경할 수 있습니다. 변경한 후 업데이트를 원래 통찰력에 저장하거나 업데이트된 버전을 새 통찰력으로 저장할 수 있습니다.

통찰력을 수정하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 Insights를 선택합니다.
3. 수정할 사용자 지정 통찰력을 선택합니다.
4. 필요에 따라 통찰력 구성을 편집합니다.

   - 통찰력의 결과를 그룹화하는 데 사용한 속성을 변경하려면

     a. 기존의 그룹화를 제거하려면 그룹화 기준 설정 옆에 있는 X를 선택합니다.

     b. 검색 창을 선택합니다.

     c. 그룹화에 사용할 속성을 선택합니다.

     d. Apply(적용)를 선택합니다.
   - 통찰력에서 필터를 제거하려면 필터 옆의 원으로 둘러싸인 X를 선택하십시오.
   - 통찰력에 필터를 추가하려면

     a. 검색 창을 선택합니다.

b. 필터로 사용할 속성과 값을 선택합니다.

c. Apply(적용)를 선택합니다.

5. 업데이트를 완료하면 Save insight(통찰력 저장)를 선택합니다.
6. 메시지가 표시되면 다음 중 하나를 수행합니다.

- 기존 통찰력을 업데이트하여 변경 사항을 반영하려면 ***<Insight_Name>*** 업데이트를 선택한 다음 Save insight(통찰력 저장)를 선택합니다.
- 업데이트가 적용된 새 통찰력을 생성하려면 Save new insight(새 통찰력 저장)를 선택합니다. Insight name(통찰력 이름)을 입력한 다음 Save insight(통찰력 저장)를 선택합니다.

사용자 지정 통찰력 수정(프로그래밍 방식)

사용자 지정 통찰력을 수정하려면 원하는 방법을 선택하고 지침을 따르십시오.

Security Hub API

1. `UpdateInsight` 작업을 실행합니다.
2. 사용자 지정 통찰력을 식별할 수 있도록 통찰력의 Amazon Resource Name(ARN)을 제공합니다. 사용자 지정 통찰력의 ARN을 가져오려면 `GetInsights` 작업을 실행합니다.
3. 필요에 따라 `Name`, `Filters`, `GroupByAttribute` 매개변수를 업데이트합니다.

AWS CLI

1. 명령줄에서 `update-insight` 명령을 실행합니다.
2. 사용자 지정 통찰력을 식별할 수 있도록 통찰력의 Amazon Resource Name(ARN)을 제공합니다. 사용자 지정 통찰력의 ARN을 가져오려면 `get-insights` 명령을 실행합니다.
3. 필요에 따라 `name`, `filters`, `group-by-attribute` 매개변수를 업데이트합니다.

```
aws securityhub update-insight --insight-arn <insight ARN> [--name <new name>] [--
filters <new filters>] [--group-by-attribute <new grouping attribute>]
```

예

```
aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
```

```
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

1. `Update-SHUBInsight` cmdlet을 사용하십시오.
2. 사용자 지정 통찰력을 식별할 수 있도록 통찰력의 Amazon Resource Name(ARN)을 제공합니다. 사용자 지정 통찰력의 ARN을 가져오려면 `Get-SHUBInsight` cmdlet을 사용하십시오.
3. 필요에 따라 `Name`, `Filter`, `GroupByAttribute` 매개변수를 업데이트합니다.

예

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

관리형 통찰력을 통해 새 사용자 지정 통찰력 생성(콘솔)

관리형 통찰력에 대한 변경 사항을 저장하거나 관리형 통찰력을 삭제할 수 없습니다. 관리형 통찰력을 새 사용자 지정 통찰력의 기반으로 사용할 수 있습니다.

관리형 통찰력을 통해 새 사용자 지정 통찰력을 생성하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 Insights를 선택합니다.
3. 작업할 관리형 통찰력을 선택합니다.
4. 필요에 따라 통찰력 구성을 편집합니다.

- 통찰력의 결과를 그룹화하는 데 사용한 속성을 변경하려면
  a. 기존의 그룹화를 제거하려면 그룹화 기준 설정 옆에 있는 X를 선택합니다.
  b. 검색 창을 선택합니다.
  c. 그룹화에 사용할 속성을 선택합니다.
  d. Apply(적용)를 선택합니다.
- 통찰력에서 필터를 제거하려면 필터 옆의 원으로 둘러싸인 X를 선택하십시오.
- 통찰력에 필터를 추가하려면
  a. 검색 창을 선택합니다.
  b. 필터로 사용할 속성과 값을 선택합니다.
  c. Apply(적용)를 선택합니다.

5. 업데이트가 완료되면 Create insight(통찰력 생성)를 선택합니다.
6. 메시지가 표시되면 Insight name(통찰력 이름)을 입력한 다음 Create insight(통찰력 생성)를 선택합니다.

사용자 지정 통찰력 삭제(콘솔)

사용자 지정 통찰력을 더 이상 원하지 않으면 삭제할 수 있습니다. 관리형 통찰력은 삭제할 수 없습니다.

사용자 지정 통찰력을 삭제하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 Insights를 선택합니다.
3. 삭제할 사용자 지정 통찰력을 찾습니다.
4. 이러한 통찰력을 보려면 추가 옵션 아이콘(카드 오른쪽 상단에 있는 점 세 개)을 선택합니다.
5. Delete(삭제)를 선택합니다.

사용자 지정 통찰력 삭제(프로그래밍 방식)

사용자 지정 통찰력을 삭제하려면 원하는 방법을 선택하고 지침을 따르십시오.

Security Hub API

1. `DeleteInsight` 작업을 실행합니다.

2. 삭제할 사용자 지정 통찰력을 식별하려면 해당 통찰력의 ARN을 제공하십시오. 사용자 지정 통찰력의 ARN을 가져오려면 `GetInsights` 작업을 실행합니다.

AWS CLI

1. 명령줄에서 `delete-insight` 명령을 실행합니다.
2. 사용자 지정 통찰력을 식별하려면 통찰력의 ARN을 제공하십시오. 사용자 지정 통찰력의 ARN을 가져오려면 `get-insights` 명령을 실행합니다.

```
aws securityhub delete-insight --insight-arn <insight ARN>
```

예

```
aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

1. `Remove-SHUBInsight` cmdlet을 사용하십시오.
2. 사용자 지정 통찰력을 식별하려면 통찰력의 ARN을 제공하십시오. 사용자 지정 통찰력의 ARN을 가져오려면 `Get-SHUBInsight` cmdlet을 사용하십시오.

예

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

자동화

Security Hub 자동화를 통해 사양을 기반으로 조사 결과를 신속하게 수정하고 해결할 수 있는 방법을 알아봅니다.

Security Hub는 현재 다음과 같은 두 종류의 자동화를 지원합니다.

- 자동화 규칙 – 정의한 기준에 따라 거의 실시간으로 조사 결과를 자동으로 업데이트하고 숨깁니다.
- 자동 응답 및 해결 – 특정 조사 결과 및 인사이트에 대해 취해야 할 자동 조치를 정의하는 사용자 지정 EventBridge 규칙을 생성합니다.

자동화 규칙은 EventBridge 규칙보다 먼저 적용됩니다. 즉, EventBridge로 전송되기 전에 자동화 규칙이 트리거되고 조사 결과가 업데이트됩니다. 그러면 EventBridge 규칙이 업데이트된 조사 결과에 적용됩니다.

보안 제어 기능을 위한 자동화를 설정할 때는 제목이나 설명보다는 제어 ID를 기준으로 필터링하는 것을 권장합니다. Security Hub는 때때로 제어 기능의 제목과 설명을 업데이트할 수 있지만 제어 ID는 동일하게 유지됩니다.

주제

자동화 규칙

자동화 규칙을 사용하여 Security Hub의 조사 결과를 자동으로 업데이트할 수 있습니다. 조사 결과가 수집되면 Security Hub는 조사 결과 제외, 심각도 변경, 조사 결과에 메모 추가 등 다양한 규칙 작업을 적용할 수 있습니다. 이러한 규칙 작업은 조사 결과가 연결된 리소스 또는 계정 ID, 제목 등 지정된 기준과 일치할 때 적용됩니다.

자동화 규칙 사용 사례의 예는 다음과 같습니다.

- 조사 결과의 리소스 ID가 비즈니스에 중요한 리소스를 참조하는 경우 조사 결과의 심각도를 `CRITICAL`로 상향 조정합니다.
- 조사 결과가 특정 프로덕션 계정의 리소스에 영향을 미치는 경우 조사 결과의 심각도를 `HIGH`에서 `CRITICAL`로 상향 조정합니다.

- INFORMATIONAL 심각도를 지닌 특정 조사 결과를 SUPPRESSED 워크플로우 상태에 할당합니다.

자동화 규칙을 사용하여 AWS 보안 검색 형식 (ASFF) 에서 선택한 검색 필드를 업데이트할 수 있습니다. 규칙은 새 조사 결과와 업데이트된 조사 결과 모두에 적용됩니다.

사용자 지정 규칙을 처음부터 만들거나 Security Hub에서 제공하는 규칙 템플릿을 사용할 수 있습니다. 규칙 템플릿을 사용하는 경우 사용 사례에 맞게 필요에 따라 수정할 수 있습니다.

자동화 규칙 작동 방식

Security Hub 관리자는 규칙 기준을 정의하여 자동화 규칙을 생성할 수 있습니다. 조사 결과가 정의된 기준과 일치하면 Security Hub는 해당 결과에 규칙 작업을 적용합니다. 사용 가능한 기준 및 작업에 대한 자세한 내용은 사용 가능한 규칙 기준 및 규칙 작업 섹션을 참조하세요.

Security Hub 관리자 계정만 자동화 규칙을 만들고, 삭제하고, 편집하고, 볼 수 있습니다. 관리자가 생성하는 규칙은 관리자 계정 및 모든 구성원 계정의 조사 결과에 적용됩니다. 구성원 계정 ID를 규칙 기준으로 제공함으로써 Security Hub 관리자는 자동화 규칙을 사용하여 조사 결과를 업데이트하거나 특정 구성원 계정의 조사 결과에 대해 조치를 취할 수도 있습니다.

자동화 규칙은 생성된 AWS 리전 위치에만 적용됩니다. 여러 리전에 규칙을 적용하려면 위임된 관리자가 각 리전에 규칙을 생성해야 합니다. 이 작업은 Security Hub 콘솔, Security Hub API 또는 AWS CloudFormation을 통해 수행할 수 있습니다. 다중 리전 배포 스크립트를 사용할 수도 있습니다.

자동화 규칙으로 인해 결과가 어떻게 변경되었는지에 대한 기록을 보려면 검색 결과 기록 검토 섹션을 참조하세요.

> **Important**
>
> 자동화 규칙은 규칙을 만든 후 Security Hub에서 생성하거나 수집하는 신규 및 업데이트된 조사 결과에 적용됩니다. Security Hub는 12~24시간마다 또는 관련 리소스의 상태가 변경될 때마다 컨트롤 조사 결과를 업데이트합니다. 자세한 내용은 보안 검사 실행 일정을 참조하십시오. 자동화 규칙은 제공자가 제공한 원본 검색 필드를 평가합니다. 작업을 통해 규칙을 만든 후 검색 필드를 업데이트해도 규칙이 트리거되지 않습니다. BatchUpdateFindings

Security Hub는 현재 관리자 계정당 최대 100개의 자동화 규칙을 지원합니다.

규칙 순서

자동화 규칙을 생성할 때 각 규칙에 순서를 할당합니다. 이는 Security Hub에서 자동화 규칙을 적용하는 순서를 결정하며, 여러 규칙이 동일한 결과 또는 결과 필드와 관련된 경우 중요해집니다.

여러 규칙 작업이 동일한 결과 또는 결과 필드와 관련된 경우 규칙 순서의 숫자 값이 가장 높은 규칙이 마지막에 적용되어 궁극적인 효과를 발휘합니다.

Security Hub 콘솔에서 규칙을 생성하면 Security Hub는 규칙 생성 순서에 따라 규칙 순서를 자동으로 할당합니다. 가장 최근에 만든 규칙이 규칙 순서 숫자 값이 가장 낮으므로 먼저 적용됩니다. Security Hub는 후속 규칙을 오름차순으로 적용합니다.

Security Hub API 또는 AWS CLI을 통해 규칙을 생성하면 Security Hub는 가장 낮은 수치로 구성된 규칙을 먼저 적용합니다. `RuleOrder` 그런 다음 다음 규칙을 오름차순으로 적용합니다. 여러 조사 결과에 동일한 `RuleOrder`가 있는 경우 Security Hub는 `UpdatedAt` 필드에 이전 값이 있는 규칙을 먼저 적용합니다(즉, 가장 최근에 편집된 규칙이 마지막에 적용됨).

언제든지 규칙 순서를 변경할 수 있습니다.

규칙 순서의 예:

규칙 A(규칙 순서는 **1**):

- 규칙 A 기준
  - `ProductName` = `Security Hub`
  - `Resources.Type`은 `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState`은 `NEW`
  - `Workflow.Status` = `ACTIVE`
- 규칙 A 작업
  - `Confidence`이(가) `95`(으)로 업데이트되었습니다.
  - `Severity`이(가) `CRITICAL`(으)로 업데이트되었습니다.

규칙 B(규칙 순서는 **2**):

- 규칙 B 기준
  - `AwsAccountId` = `123456789012`
- 규칙 B 작업

- `Severity`이(가) `INFORMATIONAL`(으)로 업데이트되었습니다.

규칙 A 작업은 규칙 A 기준과 일치하는 Security Hub 조사 결과에 먼저 적용됩니다. 다음으로, 규칙 B 작업은 지정된 계정 ID를 가진 Security Hub 조사 결과에 적용됩니다. 이 예에서는 규칙 B가 마지막에 적용되므로 지정된 계정 ID의 조사 결과에서 `Severity`의 최종 값은 `INFORMATIONAL`입니다. 규칙 A 작업에 따라 일치하는 조사 결과에서 `Confidence`의 최종 값은 `95`입니다.

사용 가능한 규칙 기준 및 규칙 작업

다음 ASFF 필드는 현재 자동화 규칙의 기준으로 지원됩니다.

ASFF 필드	필터	필드 유형
`AwsAccountId`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	String
`AwsAccountName`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	문자열
`CompanyName`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	문자열
`ComplianceAssociatedStandardsId`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	문자열
`ComplianceSecurityControlId`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	String

ASFF 필드	필터	필드 유형
ComplianceStatus	Is, Is Not	Select: [FAILED, NOT_AVAILABLE , PASSED, WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	숫자
CreatedAt	Start, End, DateRange	날짜(2022-12-01T21:47:39.269Z 형식)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	숫자
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
FirstObservedAt	Start, End, DateRange	날짜(2022-12-01T21:47:39.269Z 형식)
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
LastObservedAt	Start, End, DateRange	날짜(2022-12-01T21:47:39.269Z 형식)

ASFF 필드	필터	필드 유형
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
NoteUpdatedAt	Start, End, DateRange	날짜(2022-12-01T21:47:39.269Z 형식)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	문자열
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	문자열
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	문자열
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	문자열

ASFF 필드	필터	필드 유형
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	문자열
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	문자열
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	맵
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	문자열
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

ASFF 필드	필터	필드 유형
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	맵
ResourceType	Is, Is Not	선택(ASFF에서 지원하는 리소스 참조)
SeverityLabel	Is, Is Not	Select: [CRITICAL, HIGH, MEDIUM, LOW, INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	문자열
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
UpdatedAt	Start, End, DateRange	날짜(2022-12-01T21:47:39.269Z 형식)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	맵

ASFF 필드	필터	필드 유형
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
WorkflowStatus	Is, Is Not	Select: [NEW, NOTIFIED, RESOLVED, SUPPRESSED]

현재 자동화 규칙에 대한 작업으로 지원되는 ASFF 필드는 다음과 같습니다.

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

특정 ASFF 필드에 대한 자세한 내용은 AWS 보안 결과 형식 (ASFF) 구문 및 ASFF 예를 참조하십시오.

> **Tip**
>
> Security Hub에서 특정 컨트롤에 대한 조사 결과 생성을 중지하도록 하려면 자동화 규칙을 사용하는 대신 컨트롤을 사용하지 않도록 설정하는 것이 좋습니다. 컨트롤을 사용하지 않도록 설정하면 Security Hub에서 해당 컨트롤에 대한 보안 검사 실행을 중지하고 해당 컨트롤에 대한 조사 결과 생성을 중지하므로 해당 컨트롤에 대한 요금이 발생하지 않습니다. 정의된 기준과 일치하는 조사 결과에 대한 특정 ASFF 필드 값을 변경하려면 자동화 규칙을 사용하는 것이 좋습니다. 컨트롤 비활성화에 대한 자세한 내용은 모든 표준에서 제어 활성화 및 비활성화을 참조하십시오.

자동화 규칙 생성

사용자 지정 규칙을 처음부터 새로 만들거나 미리 채워진 Security Hub 규칙 템플릿을 사용할 수 있습니다.

한 번에 하나의 자동화 규칙만 생성할 수 있습니다. 자동화 규칙을 여러 개 만들려면 콘솔 절차를 여러 번 따르거나 원하는 파라미터를 사용하여 API 또는 명령을 여러 번 직접 호출하십시오.

조사 결과에 규칙을 적용하려는 각 리전 및 계정에서 자동화 규칙을 생성해야 합니다.

Security Hub 콘솔에서 자동화 규칙을 만들면 Security Hub는 규칙이 적용되는 조사 결과의 미리 보기를 표시합니다. 규칙 기준에 CONTAINS 또는 NOT_CONTAINS 필터가 포함된 경우 미리보기는 현재 지원되지 않습니다. 맵 및 문자열 필드 유형에 대해 이러한 필터를 선택할 수 있습니다.

> **Important**
>
> AWS 규칙 이름, 설명 또는 기타 필드에 개인 식별 정보, 기밀 정보 또는 민감한 정보를 포함하지 말 것을 권장합니다.

템플릿에서 규칙 생성(콘솔만 해당)

현재는 Security Hub 콘솔에서만 규칙 템플릿을 지원합니다. 이러한 템플릿은 자동화 규칙의 일반적인 사용 사례를 반영하며 특성을 시작하는 데 도움이 될 수 있습니다. 다음 단계를 완료하여 콘솔의 템플릿에서 자동화 규칙을 생성합니다.

Console

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   Security Hub 관리자 계정에 로그인합니다.
2. 탐색 창에서 자동화를 선택합니다.
3. Create rule을 선택합니다. 규칙 유형에서 템플릿에서 규칙 생성을 선택합니다.
4. 드롭다운 메뉴에서 규칙 템플릿을 선택합니다.
5. (선택 사항) 사용 사례에 필요한 경우 규칙, 기준 및 자동 작업 단원을 수정하십시오. 규칙 기준과 규칙 작업을 하나 이상 지정해야 합니다.

   선택한 기준에 대해 지원되는 경우 콘솔에 기준과 일치하는 조사 결과의 미리보기가 표시됩니다.

6. 규칙 상태에서는 규칙을 생성한 후 해당 규칙을 활성화할지 또는 비활성화할지 선택합니다.
7. (선택 사항) 추가 설정 섹션을 확장합니다. 이 규칙을 규칙 기준과 일치하는 조사 결과에 마지막으로 적용하려면 이러한 기준과 일치하는 조사 결과에 대한 후속 규칙 무시를 선택합니다.
8. (선택 사항) 규칙을 쉽게 식별할 수 있도록 태그의 경우 태그를 키-값 쌍으로 추가합니다.
9. Create rule을 선택합니다.

사용자 지정 규칙 생성

원하는 방법을 선택하고 다음 단계를 완료하여 사용자 지정 자동화 규칙을 생성합니다.

Console

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   Security Hub 관리자 계정에 로그인합니다.
2. 탐색 창에서 자동화를 선택합니다.
3. Create rule을 선택합니다. 규칙 유형에서 사용자 지정 규칙생성을 선택합니다.
4. 규칙 단원에서 규칙에 대한 고유한 규칙 이름과 설명을 입력합니다.
5. 기준의 경우 키, 연산자 및 값 드롭다운 메뉴를 사용하여 규칙 기준을 지정합니다. 규칙 기준을 하나 이상 지정해야 합니다.

   선택한 기준에 대해 지원되는 경우 콘솔에 기준과 일치하는 조사 결과의 미리보기가 표시됩니다.
6. 자동 작업의 경우 드롭다운 메뉴를 사용하여 조사 결과가 규칙 기준과 일치할 때 업데이트할 조사 결과 필드를 지정합니다. 규칙 작업을 최소 하나 이상 지정해야 합니다.
7. 규칙 상태에서는 규칙을 생성한 후 해당 규칙을 활성화할지 또는 비활성화할지 선택합니다.
8. (선택 사항) 추가 설정 섹션을 확장합니다. 이 규칙을 규칙 기준과 일치하는 조사 결과에 마지막으로 적용하려면 이러한 기준과 일치하는 조사 결과에 대한 후속 규칙 무시를 선택합니다.
9. (선택 사항) 규칙을 쉽게 식별할 수 있도록 태그의 경우 태그를 키-값 쌍으로 추가합니다.
10. Create rule을 선택합니다.

API

1. Security Hub 관리자 계정에서 `CreateAutomationRule` (을)를 실행합니다. 이 API는 특정 Amazon 리소스 이름(ARN)을 사용하여 규칙을 생성합니다.

2. 규칙의 이름 및 설명을 입력합니다.
3. 이 규칙이 규칙 기준과 일치하는 조사 결과에 적용되는 마지막 규칙이 되도록 하려면 `IsTerminal` 파라미터를 `true`로 설정하십시오.
4. `RuleOrder` 파라미터에 대해 규칙의 순서를 입력합니다. Security Hub는 이 파라미터에 더 낮은 숫자 값의 규칙을 먼저 적용합니다.
5. `RuleStatus` 파라미터에 대해 Security Hub에서 조사 결과 생성 후 규칙을 활성화하고 적용을 시작할지 여부를 지정합니다. 값을 지정하지 않을 경우 기본값은 `ENABLED`입니다. `DISABLED` 값은 규칙이 생성된 후 일시 중지되는 것을 의미합니다.
6. Security Hub에서 조사 결과를 필터링하는 데 사용할 기준을 `Criteria` 파라미터에 입력합니다. 규칙 작업은 기준과 일치하는 조사 결과에 적용됩니다. 지원되는 기준 목록은 사용 가능한 규칙 기준 및 규칙 작업을 참조하십시오.
7. `Actions` 파라미터에는 조사 결과와 정의된 기준 간에 일치하는 항목이 있을 때 Security Hub에서 수행할 작업을 입력합니다. 지원되는 작업 목록은 사용 가능한 규칙 기준 및 규칙 작업을 참조하십시오.

API 요청 예:

```
{
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Known issue that is not a risk.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }],
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
```

```
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "GeneratorId": [{
            "Value": "aws-foundational-security-best-practices/v/1.0.0/IAM.1",
            "Comparison": "EQUALS"
        }]
    },
    "Description": "Sample rule description",
    "IsTerminal": false,
    "RuleName": "sample-rule-name",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
}
```

AWS CLI

1. Security Hub 관리자 계정에서 `create-automation-rule` 명령을 실행합니다. 이 명령은 특정 Amazon 리소스 이름(ARN)을 사용하여 규칙을 생성합니다.
2. 규칙의 이름 및 설명을 입력합니다.
3. 이 규칙이 규칙 기준과 일치하는 조사 결과에 적용되는 마지막 규칙이 되도록 하려면 `is-terminal` 파라미터를 포함시키십시오. 그렇지 않으면 `no-is-terminal` 파라미터를 포함시키십시오.
4. `rule-order` 파라미터에 대해 규칙의 순서를 입력합니다. Security Hub는 이 파라미터에 더 낮은 숫자 값의 규칙을 먼저 적용합니다.
5. `rule-status` 파라미터에 대해 Security Hub에서 조사 결과 생성 후 규칙을 활성화하고 적용을 시작할지 여부를 지정합니다. 값을 지정하지 않을 경우 기본값은 `ENABLED`입니다. `DISABLED` 값은 규칙이 생성된 후 일시 중지되는 것을 의미합니다.
6. Security Hub에서 조사 결과를 필터링하는 데 사용할 기준을 `criteria` 파라미터에 입력합니다. 규칙 작업은 기준과 일치하는 조사 결과에 적용됩니다. 지원되는 기준 목록은 사용 가능한 규칙 기준 및 규칙 작업을 참조하십시오.
7. `actions` 파라미터에는 조사 결과와 정의된 기준 간에 일치하는 항목이 있을 때 Security Hub에서 수행할 작업을 입력합니다. 지원되는 작업 목록은 사용 가능한 규칙 기준 및 규칙 작업을 참조하십시오.

명령 예:

```
aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

자동화 규칙 보기

원하는 방법을 선택하고 단계에 따라 자동화 규칙과 각 규칙의 세부 정보를 확인하십시오.

Console

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   Security Hub 관리자 계정에 로그인합니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 규칙 이름을 선택합니다. 아니면 규칙을 선택할 수도 있습니다.
4. 작업과 보기를 선택합니다.

API

1. 계정의 자동화 규칙을 보려면 Security Hub 관리자 계정에서 ListAutomationRules을 실행합니다. 이 API는 규칙에 대한 규칙 ARN 및 기타 메타데이터를 반환합니다. 이 API에는 입력 파라미터가 필요하지 않지만, 선택적으로 결과 수를 제한하기 위해 MaxResults을 제공하고 NextToken를 페이지 매김 파라미터로 제공할 수 있습니다. NextToken의 초기값은 NULL이어야 합니다.

   API 요청 예:

   ```
   {
    "MaxResults": 50,
    "NextToken": "cVpdnSampleTokenYcXgTockBW44c"
   }
   ```

2. 규칙의 기준 및 작업을 비롯한 추가 규칙 세부 정보를 보려면 Security Hub 관리자 계정에서 BatchGetAutomationRules을 실행합니다.

   API 요청 예:

   ```
   {
       "AutomationRulesArns": [
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
         "arn:aws:securityhub:us-east-1:123456789012:automation-
   rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
       ]
   }
   ```

AWS CLI

1. 계정의 자동화 규칙을 보려면 Security Hub 관리자 계정에서 list-automation-rules 명령을 실행합니다. 이 명령은 규칙에 대한 규칙 ARN 및 기타 메타데이터를 반환합니다. 이 명령에는 입력 파라미터가 필요하지 않지만 선택적으로 결과 수를 제한하기 위해 max-results을 제공하고 페이지 매김 파라미터로 next-token를 제공할 수 있습니다.

명령 예:

```
aws securityhub list-automation-rules  \
--max-results 5 \
--next-token cVpdnSampleTokenYcXgTockBW44c \
--region us-east-1
```

2. 규칙의 기준 및 작업을 비롯한 추가 규칙 세부 정보를 보려면 Security Hub 관리자 계정에서 batch-get-automation-rules 명령을 실행합니다.

   명령 예:

```
aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
 "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

자동화 규칙 편집

자동화 규칙을 편집하면 규칙 편집 후 Security Hub가 생성하거나 수집한 신규 및 업데이트된 조사 결과에 변경 사항이 적용됩니다.

원하는 방법을 선택하고 단계에 따라 자동화 규칙의 내용을 편집하십시오. 요청 한 번으로 하나 이상의 규칙을 편집할 수 있습니다. 규칙 순서 편집에 대한 지침은 규칙 순서 편집을 참조하십시오.

Console

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   Security Hub 관리자 계정에 로그인합니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 편집할 규칙을 선택합니다. 작업을 선택한 후 편집을 선택합니다.
4. 원하는 대로 규칙을 변경하고 변경 내용 저장을 선택합니다.

API

1. Security Hub 관리자 계정에서 BatchUpdateAutomationRules (을)를 실행합니다.
2. RuleArn 파라미터에는 편집하려는 규칙의 ARN을 입력합니다.
3. 편집하려는 파라미터의 새 값을 입력합니다. RuleArn를 제외한 모든 파라미터를 편집할 수 있습니다.

API 요청 예:

```
{
    "UpdateAutomationRulesRequestItems": [
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RuleOrder": 15,
            "RuleStatus": "Enabled"
        },
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "RuleStatus": "Disabled"
        }
    ]
}
```

AWS CLI

1. Security Hub 관리자 계정에서 batch-update-automation-rules 명령을 실행합니다.
2. RuleArn 파라미터에는 편집하려는 규칙의 ARN을 입력합니다.
3. 편집하려는 파라미터의 새 값을 입력합니다. RuleArn를 제외한 모든 파라미터를 편집할 수 있습니다.

명령 예:

```
aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
```

```
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

규칙 순서 편집

경우에 따라 규칙 기준과 작업은 그대로 유지하되 Security Hub에서 자동화 규칙을 적용하는 순서를 변경해야 할 수 있습니다. 원하는 방법을 선택하고 단계에 따라 규칙 순서를 편집합니다.

Console

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   Security Hub 관리자 계정에 로그인합니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 순서를 변경할 규칙을 선택합니다. 우선 순위 편집을 선택합니다.
4. 위로 이동을 선택하여 규칙의 우선 순위를 한 단위 높입니다. 아래로 이동을 선택하여 규칙 우선 순위를 한 단위 낮춥니다. 맨 위로 이동을 선택하여 규칙에 순서를 1로 지정합니다(이렇게 하면 해당 규칙이 다른 기존 규칙보다 우선함)

> **Note**
>
> Security Hub 콘솔에서 규칙을 생성하면 Security Hub는 규칙 생성 순서에 따라 규칙 순서를 자동으로 할당합니다. 가장 최근에 만든 규칙이 규칙 순서 숫자 값이 가장 낮으므로 먼저 적용됩니다.

API

1. Security Hub 관리자 계정에서 `BatchUpdateAutomationRules` (을)를 실행합니다.
2. `RuleArn` 파라미터에는 순서를 편집하려는 규칙의 ARN을 입력합니다.
3. `RuleOrder` 필드 값을 수정합니다.

> **Note**
>
> 여러 규칙에 동일한 `RuleOrder`가 있는 경우 Security Hub는 `UpdatedAt` 필드에 이전 값이 있는 규칙을 먼저 적용합니다(즉, 가장 최근에 편집된 규칙이 마지막에 적용됨).

AWS CLI

1. Security Hub 관리자 계정에서 `batch-update-automation-rules` 명령을 실행합니다.
2. `RuleArn` 파라미터에는 순서를 편집하려는 규칙의 ARN을 입력합니다.
3. `RuleOrder` 필드 값을 수정합니다.

> **Note**
>
> 여러 규칙에 동일한 `RuleOrder`가 있는 경우 Security Hub는 `UpdatedAt` 필드에 이전 값이 있는 규칙을 먼저 적용합니다(즉, 가장 최근에 편집된 규칙이 마지막에 적용됨).

자동화 규칙 삭제

자동화 규칙을 삭제하면 Security Hub는 계정에서 해당 규칙을 삭제하고 조사 결과에 더 이상 규칙을 적용하지 않습니다.

원하는 방법을 선택하고 단계에 따라 자동화 규칙을 삭제합니다. 단일 요청으로 하나 이상의 규칙을 삭제할 수 있습니다.

> **Tip**
>
> 규칙을 삭제하는 대신 규칙을 비활성화할 수 있습니다. 이렇게 하면 나중에 사용할 수 있도록 규칙이 유지되지만, Security Hub는 사용자가 사용하도록 활성화하기 전까지는 일치하는 조사 결과에 규칙을 적용하지 않습니다.

Console

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   Security Hub 관리자 계정에 로그인합니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 삭제할 규칙을 선택합니다. 작업 및 삭제를 선택합니다(규칙을 유지하지만 일시적으로 비활성화하려면 비활성화 선택).
4. 선택을 확인하고 삭제를 선택합니다.

API

1. Security Hub 관리자 계정에서 `BatchDeleteAutomationRules` (을)를 실행합니다.
2. `AutomationRulesArns` 파라미터에 삭제하려는 규칙의 ARN을 입력합니다(규칙을 유지하지만 일시적으로 비활성화하려면 `RuleStatus` 파라미터에 대한 `DISABLED`를 입력).

   API 요청 예:

```
{
    "AutomationRulesArns": [
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
```

```
    ]
}
```

AWS CLI

1. Security Hub 관리자 계정에서 batch-delete-automation-rules 명령을 실행합니다.
2. automation-rules-arns 파라미터에 삭제하려는 규칙의 ARN을 입력합니다(규칙을 유지하지만 일시적으로 비활성화하려면 RuleStatus 파라미터에 대한 DISABLED를 입력).

명령 예:

```
aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

자동화 규칙 예

이 단원에는 일반 사용 사례에 대한 몇 가지 자동화 규칙 예가 포함되어 있습니다. 이러한 예는 Security Hub 콘솔의 규칙 템플릿에 해당합니다.

S3 버킷과 같은 특정 리소스가 위험에 처한 경우 심각도를 Critical로 상향 조정합니다.

이 예제에서는 결과의 ResourceId이 특정 Amazon Simple Storage Service(S3) 버킷일 때 규칙 기준을 일치시킵니다. 규칙 작업은 일치하는 조사 결과의 심각도를 CRITICAL로 변경하는 것입니다. 이 템플릿을 수정하여 다른 리소스에 적용할 수 있습니다.

API 요청 예:

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
```

```
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI 명령 예:

```
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
```

```
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

프로덕션 계정의 리소스와 관련된 조사 결과의 심각도를 상향 조정합니다.

이 예에서는 특정 프로덕션 계정에서 HIGH 심각도 조사 결과가 생성될 때 규칙 기준을 일치시킵니다. 규칙 작업은 일치하는 조사 결과의 심각도를 CRITICAL로 변경하는 것입니다.

API 요청 예:

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
```

```
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI 명령 예:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
```

```
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

정보 조사 결과 표시 안 함

이 예시에서는 Amazon에서 Security Hub로 전송한 INFORMATIONAL 심각도 조사 결과와 규칙 기준을 일치시킵니다 GuardDuty. 규칙 작업은 일치하는 조사 결과의 워크플로 상태를 SUPPRESSED로 변경하는 것입니다.

API 요청 예:

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
```

```
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI 명령 예:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
```

```
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

자동 응답 및 해결

Amazon EventBridge를 사용하면 AWS 서비스를 자동화하여 애플리케이션 가용성 문제나 리소스 변경 같은 시스템 이벤트에 자동으로 대응할 수 있습니다. AWS 서비스의 이벤트는 거의 실시간으로 보장된 기준으로 EventBridge로 전송됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자동으로 트리거할 수 있는 작업은 다음과 같습니다.

- AWS Lambda 함수 호출
- Amazon EC2 실행 명령 간접 호출
- Amazon Kinesis Data Streams로 이벤트 릴레이
- AWS Step Functions 상태 머신 활성화
- Amazon SNS 주제 또는 Amazon SQS 대기열 알림
- 타사 티켓팅, 채팅, SIEM 또는 인시던트 대응 및 관리 도구에 결과 전송

Security Hub는 모든 새 조사 결과와 기존 조사 결과의 모든 업데이트를 EventBridge에 EventBridge 이벤트로 자동 전송합니다. 선택한 조사 결과와 인사이트 결과를 EventBridge로 전송할 수 있게 하는 사용자 지정 작업을 생성할 수도 있습니다.

그러면 각 유형의 이벤트에 대응하도록 EventBridge 규칙을 구성합니다.

EventBridge 사용에 대한 자세한 내용은 Amazon EventBridge User Guide를 참조하세요.

> **Note**
>
> EventBridge에 액세스하기 위해 사용자에게 부여된 권한이 최소 권한 IAM 정책을 사용하고 필요한 권한만 승인될 수 있도록 확인하는 것이 가장 좋습니다.
> 자세한 내용은 Amazon EventBridge의 Identity and Access Management를 참조하세요.

계정 간 자동 응답 및 해결을 위한 템플릿 세트는 AWS 솔루션에서도 사용할 수 있습니다. 템플릿은 EventBridge 이벤트 규칙 및 Lambda 함수를 활용합니다. AWS CloudFormation 및 AWS Systems Manager을 사용하여 솔루션을 배포합니다. 이 솔루션은 완전 자동 응답 및 해결 조치를 생성할 수 있습니다. 또한 Security Hub 사용자 지정 작업을 사용하여 사용자가 트리거하는 응답 및 해결 조치를 생성할 수 있습니다. 솔루션을 구성하고 사용하는 방법에 대한 자세한 내용은 AWS 솔루션 페이지의 자동 보안 대응을 참조하세요.

주제

Security Hub와 EventBridge의 통합 유형

Security Hub는 다음과 같은 EventBridge 이벤트 유형을 사용하여 다음과 같은 유형의 EventBridge와의 통합을 지원합니다.

Security Hub의 EventBridge 대시보드에서 모든 이벤트에는 이러한 이벤트 유형이 모두 포함됩니다.

모든 결과(Security Hub Findings - Imported)

Security Hub는 모든 새 조사 결과와 기존 조사 결과의 모든 업데이트를 EventBridge에 Security Hub Findings - Imported 이벤트로 자동 전송합니다. 각 Security Hub Findings - Imported 이벤트에는 단일 조사 결과가 포함됩니다.

모든 `BatchImportFindings` 및 `BatchUpdateFindings` 요청은 Security Hub Findings - Imported 이벤트를 트리거합니다.

관리자 계정의 경우 EventBridge의 이벤트 피드에는 관리자 계정과 회원 계정 모두에서 찾은 결과에 대한 이벤트가 포함됩니다.

집계 지역의 이벤트 피드에는 집계 지역 및 연결 지역의 조사 결과에 대한 이벤트가 포함됩니다. 지역 간 조사 결과는 거의 실시간으로 이벤트 피드에 포함됩니다. 조사 결과 집계를 구성하는 방법에 대한 자세한 내용은 크로스 리전 집계 활성화을 참조하세요.

결과를 Amazon S3 버킷, 문제 해결 워크플로우 또는 타사 도구로 자동 라우팅하는 규칙을 EventBridge에 정의할 수 있습니다. 조사 결과에 특정 속성 값이 있는 경우에만 규칙을 적용하는 필터가 규칙에 포함될 수 있습니다.

이 방법을 사용하여 모든 결과 또는 특정한 특성이 있는 모든 결과를 자동으로 응답 또는 문제 해결 워크플로우로 보냅니다.

the section called “자동으로 전송된 조사 결과에 대한 규칙 구성”를 참조하세요.

사용자 지정 작업에 대한 결과(Security Hub Findings - Custom Action)

또한 Security Hub는 사용자 지정 작업과 연결된 결과를 EventBridge에 Security Hub Findings - Custom Action 이벤트로 전송합니다.

이는 Security Hub 콘솔을 사용해 특정 결과나 작은 결과 세트를 응답 또는 문제 해결 워크플로우로 보내려는 분석가에게 유용합니다. 한 번에 최대 20개의 결과에 대해 사용자 지정 작업을 선택할 수 있습니다. 각 조사 결과는 별도의 EventBridge 이벤트로 EventBridge에 전송됩니다.

사용자 지정 작업을 생성할 때 사용자 지정 작업 ID를 할당합니다. 이 ID를 사용하여 사용자 지정 작업 ID와 관련된 결과를 수신한 후 지정된 작업을 수행하는 EventBridge 규칙을 생성할 수 있습니다.

the section called “사용자 지정 작업 구성 및 사용”를 참조하세요.

예를 들어 Security Hub에서 `send_to_ticketing`이라는 사용자 지정 작업을 생성할 수 있습니다. 그런 다음, EventBridge에서 `send_to_ticketing` 사용자 지정 작업 ID가 포함된 결과를 EventBridge

가 수신할 때 트리거되는 규칙을 생성합니다. 이 규칙에는 결과를 티켓팅 시스템에 전송하는 로직이 포함됩니다. 그런 다음 Security Hub 내에서 결과를 선택하고 Security Hub의 사용자 지정 작업을 사용하여 결과를 티켓팅 시스템에 수동으로 전송할 수 있습니다.

추가 처리를 위해 Security Hub 조사 결과를 EventBridge로 보내는 방법에 대한 예는 PagerDuty와 AWS Security Hub 사용자 지정 작업을 통합하는 방법 및 AWS 파트너 네트워크(APN) 블로그에서 AWS Security Hub에 사용자 지정 작업을 활성화하는 방법을 참조하세요.

사용자 지정 작업에 대한 통찰력 결과(Security Hub Insight Results)

또한 사용자 지정 작업을 사용하여 통찰력 결과 집합을 EventBridge에 Security Hub Insight Results 이벤트로 전송할 수 있습니다. 인사이트 결과는 인사이트와 일치하는 리소스입니다. 통찰력 결과를 EventBridge에 전송할 때는 결과를 EventBridge에 전송하는 것이 아닙니다. 통찰력 결과와 연결된 리소스 식별자만 전송합니다. 한 번에 최대 100개의 리소스 식별자를 전송할 수 있습니다.

결과에 대한 사용자 지정 작업과 마찬가지로, 먼저 Security Hub에서 사용자 지정 작업을 생성한 다음, EventBridge에서 규칙을 생성합니다.

the section called “사용자 지정 작업 구성 및 사용”를 참조하세요.

예를 들어, 동료와 공유하고 싶은 관심 대상 특정 인사이트 결과를 보았다고 가정해 보겠습니다. 이 경우 사용자 지정 작업을 사용하여 채팅 또는 티켓 시스템을 통해 해당 인사이트 결과를 동료에게 보낼 수 있습니다.

Security Hub용 EventBridge 이벤트 형식

Security Hub Findings - Imported, Security Findings - Custom Action 및 Security Hub Insight Results 이벤트 유형은 다음 이벤트 형식을 사용합니다.

이벤트 형식은 Security Hub가 EventBridge로 이벤트를 전송할 때 사용되는 형식입니다.

Security Hub Findings - Imported

Security Hub에서 EventBridge로 전송되는 Security Hub Findings - Imported 이벤트는 다음 형식을 사용합니다.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
```

```
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

*<finding content>*는 이벤트에서 전송한 조사 결과의 내용(JSON 형식)입니다. 각 이벤트는 단일 조사 결과를 전송합니다.

조사 결과의 전체 목록은 AWS 보안 검색 형식 (ASFF) 단원을 참조하세요.

이러한 이벤트에 의해 트리거되는 EventBridge 규칙 구성 방법에 대한 자세한 내용은 the section called “자동으로 전송된 조사 결과에 대한 규칙 구성” 섹션을 참조하세요.

Security Hub Findings - Custom Action

Security Hub에서 EventBridge로 전송되는 Security Hub Findings - Custom Action 이벤트는 다음 형식을 사용합니다. 각 조사 결과는 별도의 이벤트로 전송됩니다.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
```

```
      {
        <finding content>
      }
    ]
  }
}
```

*<finding content>*는 이벤트에서 전송한 조사 결과의 내용(JSON 형식)입니다. 각 이벤트는 단일 조사 결과를 전송합니다.

조사 결과의 전체 목록은 AWS 보안 검색 형식 (ASFF) 단원을 참조하세요.

이러한 이벤트에 의해 트리거되는 EventBridge 규칙 구성 방법에 대한 자세한 내용은 the section called “사용자 지정 작업 구성 및 사용” 섹션을 참조하세요.

Security Hub Insight Results

Security Hub에서 EventBridge로 전송되는 Security Hub Insight Results 이벤트는 다음 형식을 사용합니다.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
```

```
  }
}
```

이러한 이벤트에 의해 트리거되는 EventBridge 규칙 생성에 대한 자세한 내용은 the section called “사용자 지정 작업 구성 및 사용” 단원을 참조하세요.

자동으로 전송된 조사 결과에 대한 EventBridge 규칙 구성

EventBridge에서 Security Hub Findings - Imported 이벤트를 수신할 때 수행할 작업을 정의하는 규칙을 생성할 수 있습니다. Security Hub Findings - Imported 이벤트는 `BatchImportFindings` 및 `BatchUpdateFindings` 양쪽 모두의 업데이트에 의해 트리거됩니다.

각 규칙에는 규칙을 트리거하는 이벤트를 식별하는 이벤트 패턴이 포함되어 있습니다. 이벤트 패턴에는 항상 이벤트 소스(`aws.securityhub`)와 이벤트 유형(Security Hub 조사 결과 - 가져옴)이 포함됩니다. 이벤트 패턴은 규칙이 적용되는 결과를 식별하는 필터를 지정할 수도 있습니다.

그러면 규칙이 규칙 대상을 식별합니다. 대상은 EventBridge가 Security Hub 조사 결과 - 가져옴 이벤트를 수신하고 조사 결과가 필터와 일치할 때 취할 조치입니다.

여기에 제공된 지침은 EventBridge 콘솔을 사용합니다. 콘솔을 사용하면 EventBridge는 EventBridge가 CloudWatch Logs에 기록할 수 있도록 필요한 리소스 기반 정책을 자동으로 생성합니다.

EventBridge API의 `PutRule` API 작업을 사용할 수도 있습니다. 하지만 EventBridge API를 사용하는 경우 리소스 기반 정책을 생성해야 합니다. 필수 정책에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 CloudWatch Logs 권한을 참조하세요.

이벤트 패턴 형식

Security Hub 조사 결과 - 가져옴 이벤트의 이벤트 패턴 형식은 다음과 같습니다.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
```

```
  }
}
```

- `source`는 Security Hub를 이벤트를 생성하는 서비스로 식별합니다.
- `detail-type`은 이벤트 유형을 식별합니다.
- `detail`은 선택 사항이며 이벤트 패턴에 대한 필터 값을 제공합니다. 이벤트 패턴에 `detail` 필드가 없는 경우 모든 결과가 규칙을 트리거합니다.

모든 조사 결과 속성을 기준으로 결과를 필터링할 수 있습니다. 각 값에 대해 하나 이상의 값을 쉼표로 구분한 배열을 제공합니다.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

속성에 둘 이상의 값을 제공하면 해당 값이 `OR`로 결합됩니다. 조사 결과에 나열된 값 중 하나라도 있는 경우 조사 결과는 개별 속성의 필터와 일치합니다. 예를 들어, `INFORMATIONAL`과 `LOW`를 모두 `Severity.Label` 값으로 제공하면 심각도 레이블이 `INFORMATIONAL` 또는 `LOW`일 경우 조사 결과가 일치합니다.

속성은 `AND`로 결합됩니다. 제공된 모든 속성에 대한 필터 기준과 일치하면 조사 결과가 일치합니다.

속성 값을 제공할 때는 AWS 보안 조사 결과 형식(ASFF) 구조 내에서 해당 속성의 위치를 반영해야 합니다.

> **Tip**
>
> 제어 결과를 필터링할 때는 `Title` 또는 `Description` 대신 `SecurityControlId` 또는 `SecurityControlArn` ASFF 필드를 필터로 사용하는 것이 좋습니다. 후자의 필드는 때때로 변경될 수 있지만 제어 ID 및 ARN은 정적 식별자입니다.

다음 예제에서 이벤트 패턴은 `ProductArn` 및 `Severity.Label`에 대한 필터 값을 제공하므로 Amazon Inspector에서 생성되고 심각도 레이블이 `INFORMATIONAL` 또는 `LOW`인 경우 조사 결과가 일치합니다.

```
{
    "source": [
        "aws.securityhub"
     ],
```

```
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

이벤트 규칙 생성

사전 정의된 이벤트 패턴 또는 사용자 지정 이벤트 패턴을 사용하여 EventBridge에서 규칙을 생성할 수 있습니다. 사전 정의된 패턴을 선택하면 EventBridge가 자동으로 `source` 및 `detail-type`을 채웁니다. EventBridge는 다음과 같은 결과 속성에 대한 필터 값을 지정하는 필드도 제공합니다.

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

EventBridge 규칙을 생성하려면

1. Amazon EventBridge 콘솔(https://console.aws.amazon.com/events/)을 엽니다.
2. 다음 값을 사용하여 조사 결과 이벤트를 모니터링하는 EventBridge 규칙을 생성합니다.
   - 규칙 유형에서 이벤트 패턴이 있는 규칙을 선택합니다.
   - 이벤트 패턴 작성 방법을 선택합니다.

다음을 사용하여 이벤트 패턴을 만들려면...	수행할 작업	
템플릿	Event pattern(이벤트 패턴) 섹션에서 다음을 선택합니다. • 이벤트 소스에서 AWS 서비스를 선택합니다. • AWS 서비스에 대해 Security Hub를 선택합니다. • 이벤트 유형에서 Security Hub 조사 결과 - 가져오기를 선택합니다. • (선택 사항) 규칙을 더 구체적으로 만들려면 필터 값을 추가합니다. 예를 들어 규칙을 활성 레코드 상태의 조사 결과로 제한하려면 특정 레코드 상태에 대해 활성을 선택합니다.	

다음을 사용하여 이벤트 패턴을 만들려면...	수행할 작업	
사용자 지정 이벤트 패턴입니다. (EventBridge 콘솔에 표시되지 않은 속성을 기반으로 조사 결과를 필터링하려면 사용자 지정 패턴을 사용하십시오.)	• 이벤트 패턴(Event pattern) 섹션에서 사용자 지정 패턴(JSON 편집기)(Custom patterns (JSON editor))를 선택하고 다음 이벤트 패턴을 텍스트 영역에 붙여 넣습니다. `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>" ] } } }` • 필터로 사용할 속성 및 속성 값을 포함하도록 이벤트 패턴을 업데이트합니다. 예를 들어, 확인 상태 `TRUE_POSITIVE` 인 결과에 규칙을 적용하려면 다	

다음을 사용하여 이벤트 패턴을 만들려면...	수행할 작업	
	음 패턴 예제를 사용합니다. `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }`	

- 대상 유형(Target types)에서 AWS 서비스를 선택하고 대상 선택(Select a target)에서 Amazon SNS 주제 또는 AWS Lambda 함수와 같은 대상을 선택합니다. 규칙에 정의된 이벤트 패턴과 일치하는 이벤트를 수신할 때 대상이 트리거됩니다.

규칙 생성에 대한 자세한 내용은 Amazon EventBridge User Guide(Amazon EventBridge 사용 설명서)의 Creating Amazon EventBridge rules that react to events(이벤트에 대응하는 Amazon EventBridge 규칙 생성)를 참조하세요.

사용자 지정 작업을 사용하여 결과 및 인사이트 결과를 EventBridge로 전송

Security Hub 사용자 지정 작업을 사용하여 결과 또는 인사이트 결과를 EventBridge로 보내려면 먼저 Security Hub에서 사용자 지정 작업을 생성해야 합니다. 그런 다음 사용자 지정 작업에 적용되는 규칙을 EventBridge에서 정의하십시오.

최대 50개의 사용자 지정 작업을 생성할 수 있습니다.

크로스 리전 집계 활성화를 활성화하고 집계 영역의 결과를 관리하는 경우 집계 영역에서 사용자 지정 작업을 생성하십시오.

EventBridge의 규칙은 사용자 지정 작업의 ARN을 사용합니다.

사용자 지정 작업 생성(콘솔)

사용자 지정 작업을 생성할 때 이름, 설명, 고유 식별자를 지정합니다.

Security Hub(콘솔)에서 사용자 지정 작업을 생성하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 Custom actions(사용자 지정 작업)를 선택합니다.
3. Create custom action(사용자 지정 작업 생성)을 선택하십시오.
4. 작업에 대한 이름, 설명 및 Custom action ID(사용자 지정 작업 ID)를 입력하십시오.

   이름은 20자 미만이어야 합니다.

   Custom action ID(사용자 지정 작업 ID)는 각 AWS 계정에 대해 고유해야 합니다.
5. Create custom action(사용자 지정 작업 생성)을 선택하십시오.
6. 사용자 지정 작업 ARN을 기록해 둡니다. EventBridge에서 이 작업과 연결할 규칙을 생성할 때 ARN을 사용해야 합니다.

사용자 지정 작업 생성(Security Hub API, AWS CLI)

사용자 지정 작업을 생성하려면 API 직접 호출 또는 AWS Command Line Interface을 사용할 수 있습니다.

사용자 지정 작업(Security Hub API, AWS CLI)을 생성하려면

- Security Hub API - `CreateActionTarget` 작업을 사용합니다. 사용자 지정 작업을 생성할 때 이름, 설명 및 사용자 지정 작업 식별자를 제공합니다.
- AWS CLI – 명령줄에서 `create-action-target` 명령을 실행합니다.

```
create-action-target --name <customActionName> --
description <customActionDescription> --id <customActionidentifier>
```

예

```
aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

EventBridge에서의 규칙 정의

사용자 지정 작업을 처리하려면 EventBridge 내에 해당 규칙을 생성해야 합니다. 규칙 정의에는 사용자 지정 작업의 ARN이 포함됩니다.

Security Hub 조사 결과 - 사용자 지정 작업 이벤트의 이벤트 패턴은 다음과 같은 형식입니다.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Security Hub 인사이트 결과 이벤트의 이벤트 패턴은 다음과 같은 형식입니다.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

두 패턴 모두 *<custom action ARN>*이 사용자 지정 작업의 ARN입니다. 둘 이상의 사용자 지정 작업에 적용되는 규칙을 구성할 수 있습니다.

여기에 제공된 지침은 EventBridge 콘솔을 위한 것입니다. 콘솔을 사용하면 EventBridge는 EventBridge가 CloudWatch Logs에 기록할 수 있도록 필요한 리소스 기반 정책을 자동으로 생성합니다.

EventBridge API의 `PutRule` API 작업을 사용할 수도 있습니다. 하지만 EventBridge API를 사용하는 경우 리소스 기반 정책을 생성해야 합니다. 필수 정책에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 CloudWatch Logs 권한을 참조하세요.

EventBridge에서 규칙을 정의하려면

1. https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택합니다.
3. 규칙 생성을 선택합니다.
4. 규칙에 대해 이름과 설명을 입력하세요.
5. 이벤트 버스에서 이 규칙과 연결할 이벤트 버스를 선택합니다. 이 규칙이 자신의 계정에서 발생하는 이벤트와 일치하도록 하려면 기본을 선택합니다. 계정의 AWS 서비스가 이벤트를 출력하면 항상 계정의 기본 이벤트 버스로 이동합니다.
6. 규칙 유형에서 이벤트 패턴이 있는 규칙을 선택합니다.
7. 다음을 선택합니다.
8. 이벤트 소스(Event source)에서 AWS 이벤트(events)를 선택합니다.
9. 이벤트 패턴에서 이벤트 패턴 양식을 선택합니다.
10. 이벤트 소스에서 AWS 서비스를 선택합니다.
11. AWS 서비스를 받으려면 Security Hub를 선택합니다.
12. 이벤트 유형(Event type)에서 다음 중 하나를 수행합니다.
    - 조사 결과를 사용자 지정 작업에 보낼 때 적용할 규칙을 생성하려면 Security Hub 조사 결과 - 사용자 지정 작업을 선택합니다.
    - 사용자 지정 작업에 인사이트 결과를 보낼 때 적용할 규칙을 생성하려면 Security Hub Insight 결과를 선택합니다.
13. 특정 사용자 지정 작업 ARN을 선택하고 사용자 지정 작업 ARN을 추가합니다.

    규칙이 여러 사용자 지정 작업에 적용되는 경우 추가를 선택하여 사용자 지정 작업 ARN을 더 추가합니다.
14. 다음을 선택합니다.
15. 대상 선택에서 이 규칙이 일치할 때 간접적으로 호출할 대상을 선택하고 구상합니다.
16. 다음을 선택합니다.
17. (선택 사항)규칙에 대해 하나 이상의 태그를 입력하세요. 자세한 정보는 Amazon EventBridge 사용 설명서의 Amazon EventBridge 태그를 참조하세요.

18. 다음을 선택합니다.
19. 규칙의 세부 정보를 검토하고 규칙 생성을 선택합니다.

    계정의 조사 결과 또는 인사이트 결과에 대해 사용자 지정 작업을 수행하면 EventBridge에서 이벤트가 생성됩니다.

조사 결과 및 인사이트 결과에 대한 사용자 지정 작업 선택

Security Hub 사용자 지정 작업 및 EventBridge 규칙을 생성한 후에는 추가 관리 및 처리를 위한 결과와 인사이트 결과를 EventBridge에 보낼 수 있습니다.

이벤트는 해당 이벤트가 표시된 계정의 EventBridge에만 전송됩니다. 관리자 계정을 사용하여 결과를 보는 경우 이벤트는 관리자 계정으로 EventBridge에 전송됩니다.

AWS API 직접 호출을 적용하려면 대상 코드 구현이 역할을 멤버 계정으로 전환해야 합니다. 이는 전환해야 하는 역할을 작업이 필요한 각 구성원에게 배포해야 함을 의미합니다.

결과를 EventBridge로 보내려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 결과 목록 표시:

   - 조사 결과에서 활성화된 모든 제품 통합 및 제어의 결과를 볼 수 있습니다.
   - Security standards(보안 표준)에서는 선택한 컨트롤에서 생성된 결과 목록으로 이동할 수 있습니다. the section called “제어에 대한 세부 정보 보기”를 참조하세요.
   - Integrations(통합)에서는 활성화된 통합에 의해 생성된 결과 목록으로 이동할 수 있습니다. the section called “통합에서 조사 결과 보기”를 참조하세요.
   - Insights(인사이트)에서는 일치하는 인사이트 결과에 대한 결과 목록으로 이동할 수 있습니다. the section called “인사이트 결과 및 조사 결과 보기”를 참조하세요.
3. EventBridge로 전송할 결과를 선택합니다. 한 번에 최대 20개 결과까지 선택할 수 있습니다.
4. 작업에서 적용할 EventBridge 규칙과 일치하는 사용자 지정 작업을 선택하십시오.

   Security Hub는 각 조사 결과에 대해 별도의 Security Hub 조사 결과 - 사용자 지정 작업 이벤트를 보냅니다.

인사이트 결과를 EventBridge로 보내려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.

2. 탐색 창에서 Insights를 선택합니다.
3. Insights(통찰력) 페이지에서 EventBridge에 보낼 결과가 포함된 통찰력을 선택합니다.
4. EventBridge로 전송할 인사이트 결과를 선택합니다. 한 번에 최대 20개 결과까지 선택할 수 있습니다.
5. 작업에서 적용할 EventBridge 규칙과 일치하는 사용자 지정 작업을 선택하십시오.

AWS Security Hub에서의 제품 통합

AWS Security Hub는 여러 AWS 서비스 및 지원되는 AWS 파트너 네트워크(APN) 보안 솔루션에서 보안 검색 데이터를 집계할 수 있습니다. 이러한 집계를 통해 AWS 환경 전반의 보안 및 규정 준수를 포괄적으로 파악할 수 있습니다.

자체 사용자 지정 보안 제품에서 생성된 결과를 전송할 수도 있습니다.

> **Important**
>
> 지원되는 AWS 및 파트너 제품 통합에서 Security Hub는 AWS 계정에서 Security Hub를 활성화한 후 생성되는 결과만 수신하고 통합합니다.
> 이 서비스는 Security Hub를 활성화하기 전에 생성된 보안 결과를 소급하여 감지하고 통합하지 않습니다.

수집된 결과에 대한 Security Hub의 요금 부과 방법에 대한 세부 정보는 Security Hub 요금을 참조하십시오.

주제

- 제품 통합 관리
- AWS 서비스AWS Security Hub와의 통합
- 사용 가능한 타사 파트너 제품 통합
- 사용자 지정 제품 통합을 사용하여 AWS Security Hub에 결과 전송

제품 통합 관리

의 통합 페이지에서는 사용 가능한 모든 제품 통합 AWS 및 타사 제품 통합에 AWS Management Console 액세스할 수 있습니다. AWS Security Hub API는 통합을 관리할 수 있는 작업도 제공합니다.

> **Note**
>
> 일부 통합은 일부 리전에서 사용할 수 없습니다. 현재 리전에서 지원되지 않는 통합은 통합 페이지에 나열되지 않습니다.
> the section called “중국(베이징) 및 중국(닝샤)에서 지원되는 통합” 및 the section called “AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 에서 지원되는 통합”도 참조하십시오.

통합 목록 보기 및 필터링(콘솔)

통합 페이지에서 통합 목록을 보고 필터링할 수 있습니다.

통합 목록을 보려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. Security Hub 탐색 창에서 통합을 선택합니다.

통합 페이지에는 다른 AWS 서비스와의 통합이 먼저 나열되고 타사 제품과의 통합이 다음에 나열됩니다.

각 통합에 대해 통합 페이지는 다음 정보를 제공합니다.

- 회사의 이름
- 제품 이름
- 통합에 대한 설명
- 통합이 적용되는 범주
- 통합을 활성화하는 방법
- 통합의 현재 상태

다음 필드의 텍스트를 입력하여 목록을 필터링할 수 있습니다.

- 회사 이름
- 제품 이름
- 통합 설명
- 카테고리

제품 통합에 대한 정보 보기 (Security Hub API, AWS CLI)

제품 통합에 대한 정보를 보려면 API 직접 호출 또는 AWS Command Line Interface를 사용할 수 있습니다. 모든 제품 통합에 대한 정보 또는 활성화한 제품 통합에 대한 정보를 표시할 수 있습니다.

사용 가능한 모든 제품 통합에 대한 정보를 보려면(Security Hub API, AWS CLI)

- Security Hub API - `DescribeProducts` 작업을 사용합니다. 반환할 특정 제품 통합을 식별하려면 `ProductArn` 파라미터를 사용하여 통합 ARN을 제공하십시오.

- AWS CLI – 명령줄에서 describe-products 명령을 실행합니다. 반환할 특정 제품 통합을 식별하려면 통합 ARN을 제공하십시오.

```
aws securityhub describe-products --product-arn "<integrationARN>"
```

예

```
aws securityhub describe-products --product-arn "arn:aws:securityhub:us-
east-1::product/3coresec/3coresec"
```

활성화한 제품 통합에 대한 정보를 보려면(Security Hub API, AWS CLI)

- Security Hub API - ListEnabledProductsForImport 작업을 사용합니다.
- AWS CLI – 명령줄에서 list-enabled-products-for-import 명령을 실행합니다.

```
aws securityhub list-enabled-products-for-import
```

통합 활성화

통합 페이지에서 각 통합은 통합을 활성화하는 데 필요한 단계를 제공합니다.

대부분의 다른 서비스와의 통합에서 필요한 단계는 다른 AWS 서비스를 활성화하는 것뿐입니다. 통합 정보에는 서비스 홈 페이지에 대한 링크가 포함됩니다. 다른 서비스를 활성화하면 Security Hub가 서비스로부터 조사 결과를 받을 수 있는 리소스 수준 권한이 자동으로 생성되어 적용됩니다.

타사 제품 통합의 경우 에서 통합을 구매한 다음 통합을 구성해야 할 수 있습니다. AWS Marketplace통합 정보는 이러한 작업을 수행할 수 있는 링크를 제공합니다.

에서 AWS Marketplace사용할 수 있는 제품 버전이 두 개 이상인 경우 구독할 버전을 선택한 다음 구독 계속을 선택합니다. 예를 들어, 일부 제품은 표준 버전과 AWS GovCloud (US) 버전을 제공합니다.

제품 통합을 활성화하면 리소스 정책이 자동으로 해당 제품 구독에 연결됩니다. 이 리소스 정책은 Security Hub가 해당 제품에서 조사 결과를 수신하는 데 필요한 권한을 정의합니다.

통합에서 조사 결과의 흐름 사용 중지 및 사용 설정(콘솔)

통합 페이지에서 조사 결과를 전송하는 통합의 경우 상태 정보가 현재 조사 결과를 수락하고 있는지 여부를 표시합니다.

조사 결과 수락을 중지하려면 조사 결과 수락 중지를 선택합니다.

조사 결과 수락을 다시 시작하려면 조사 결과 수락을 선택합니다.

통합에서 검색 결과 흐름 비활성화 (Security Hub API, AWS CLI)

통합에서 조사 결과의 흐름을 해제하려면 API 호출 또는 AWS Command Line Interface를 사용할 수 있습니다.

통합에서 검색 결과 흐름을 비활성화하려면 (Security Hub API, AWS CLI)

- Security Hub API - `DisableImportFindingsForProduct` 작업을 사용합니다. 비활성화할 통합을 식별하려면 구독에 대한 ARN이 필요합니다. 활성화된 통합에 대한 구독 ARN을 가져오려면 `ListEnabledProductsForImport` 작업을 사용합니다.
- AWS CLI – 명령줄에서 `disable-import-findings-for-product` 명령을 실행합니다.

```
aws securityhub disable-import-findings-for-product --product-subscription-
arn <subscription ARN>
```

예

```
aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

통합을 통한 결과 흐름 활성화 (Security Hub API, AWS CLI)

통합에서 조사 결과의 흐름을 활성화하려면 API 직접 호출 또는 AWS Command Line Interface를 사용할 수 있습니다.

통합 결과 흐름을 활성화하려면 (Security Hub API, AWS CLI)

- Security Hub API - `EnableImportFindingsForProduct` 작업을 사용합니다. 통합에서 조사 결과를 수신하기 위해 Security Hub를 활성화려면 제품 ARN이 필요합니다. 사용 가능한 통합에 대한 ARN을 가져오려면 `DescribeProducts` 작업을 사용합니다.
- AWS CLI: 명령줄에서 `enable-import-findings-for-product` 명령을 실행합니다.

```
aws securityhub enable-import-findings-for-product --product-arn <integration ARN>
```

예

```
aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

통합에서 조사 결과 보기

조사 결과를 수락한 통합의 경우(상태가 조사 결과 수락인 경우) 조사 결과 목록을 보려면 조사 결과 보기를 선택합니다.

조사 결과 목록에는 워크플로 상태가 NEW 또는 NOTIFIED인 선택한 통합에 대한 활성 조사 결과가 표시됩니다.

크로스 리전 집계 활성화를 활성화한 경우 집계 영역의 목록에는 집계 영역 및 통합이 활성화된 연결된 리전에서 나온 조사 결과가 포함됩니다. Security Hub는 크로스 리전 집계 활성화 구성을 기반으로 통합을 자동으로 활성화하지 않습니다.

다른 리전의 경우 통합 조사 결과 목록에 현재 리전의 조사 결과만 포함됩니다.

리전 간 집계를 구성하는 방법에 대한 자세한 내용은 크로스 리전 집계 활성화 섹션을 참조하십시오.

조사 결과 목록에서 다음 작업을 수행할 수 있습니다.

- 목록 필터 및 그룹화 변경
- 개별 조사 결과에 대한 세부 정보 보기
- 조사 결과의 워크플로 상태 업데이트
- 사용자 지정 작업에 조사 결과 전송

AWS 서비스AWS Security Hub와의 통합

AWS Security Hub는 다른 AWS 서비스여러 제품과의 통합을 지원합니다.

> **Note**
>
> 일부 통합은 일부 지역에서만 사용할 수 있습니다. AWS 리전
> 특정 리전에서 지원되지 않는 통합은 Security Hub 콘솔의 통합 페이지에 나열되지 않습니다.

자세한 내용은 중국(베이징) 및 중국(닝샤)에서 지원되는 통합 및 AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 에서 지원되는 통합 섹션을 참조하세요.

아래에 명시되지 않는 한 Security Hub를 활성화한 후 Security Hub로 검색 결과를 보내는 AWS 서비스 통합이 자동으로 활성화됩니다. Security Hub 조사 결과를 받은 통합에는 활성화를 위한 추가 단계가 필요할 수 있습니다. 더 자세히 알아보려면 각 통합에 대한 정보를 검토해 보십시오.

Security Hub와의 AWS 서비스 통합 개요

다음은 Security Hub로 조사 결과를 보내거나 Security Hub에서 조사 결과를 수신하는 AWS 서비스의 개요입니다.

통합 AWS 서비스	Direction	
AWS Config	조사 결과를 전송합니다	
AWS Firewall Manager	조사 결과를 전송합니다	
아마존 GuardDuty	조사 결과를 전송합니다	
AWS Health	조사 결과를 전송합니다	
AWS Identity and Access Management Access Analyzer	조사 결과를 전송합니다	
Amazon Inspector	조사 결과를 전송합니다	
AWS IoT Device Defender	조사 결과를 전송합니다	
Amazon Macie	조사 결과를 전송합니다	
AWS Systems Manager 패치 관리자	조사 결과를 전송합니다	
AWS Audit Manager	조사 결과를 수신합니다	
AWS Chatbot	조사 결과를 수신합니다	
Amazon Detective	조사 결과를 수신합니다	

통합 AWS 서비스	Direction	
Amazon Security Lake	조사 결과를 수신합니다	
AWS Systems Manager 익스플로러 및 OpsCenter	조사 결과 수령 및 업데이트	
AWS Trusted Advisor	조사 결과를 수신합니다	

AWS Security Hub에 조사 결과를 전송하는 서비스

다음 AWS 서비스는 검색 결과를 Security Hub로 전송하여 Security Hub와 통합됩니다. Security Hub는 조사 결과를 AWS 보안 조사 결과 형식으로 변환합니다.

AWS Config (조사 결과 전송)

AWS Config AWS 리소스 구성을 평가, 감사 및 평가할 수 있는 서비스입니다. AWS Config AWS 리소스 구성을 지속적으로 모니터링 및 기록하고, 기록된 구성을 원하는 구성과 비교하여 평가하는 작업을 자동화할 수 있습니다.

와의 AWS Config통합을 사용하면 Security Hub에서 AWS Config 관리형 및 사용자 지정 규칙 평가 결과를 검색 결과로 볼 수 있습니다. 이러한 조사 결과는 다른 Security Hub 조사 결과와 함께 볼 수 있으며, 보안 상태에 대한 포괄적인 개요를 제공합니다.

AWS Config EventBridge Amazon을 사용하여 Security Hub에 AWS Config 규칙 평가를 전송합니다. Security Hub는 규칙 평가를 AWS 보안 조사 결과 형식을 따르는 조사 결과로 변환합니다. 그런 다음 Security Hub는 Amazon 리소스 이름(ARN) 및 생성 날짜 등 영향을 받는 리소스에 대한 추가 정보를 수집하여 BEB(best-effort basis) 방식으로 조사 결과를 보강합니다. AWS Config 규칙 평가의 리소스 태그는 Security Hub 조사 결과에 포함되지 않습니다.

이 통합에 대한 자세한 내용은 다음 단원을 참조하십시오.

결과를 AWS Config Security Hub로 보내는 방법

Security Hub의 모든 조사 결과는 표준 JSON 형식의 ASFF를 사용합니다. ASFF에는 검색 결과의 출처, 영향을 받는 리소스, 검색 결과의 현재 상태에 대한 세부 정보가 포함됩니다. AWS Config 를 통해 EventBridge 관리형 및 사용자 지정 규칙 평가를 Security Hub에 전송합니다. Security Hub는 규칙 평가를 ASFF를 따르는 조사 결과로 변환하고 BEB(best-effort basis) 방식으로 조사 결과를 강화합니다.

Security Hub로 AWS Config 보내는 검색 결과 유형

통합이 활성화되면 모든 AWS Config 관리형 규칙 및 사용자 지정 규칙에 대한 평가를 Security Hub로 AWS Config 보냅니다. 보안 제어 검사를 실행하는 데 사용되는 AWS Config 규칙과 같은 서비스 연결 규칙의 평가만 제외됩니다.

Security Hub에 AWS Config 조사 결과 보내기

통합이 활성화되면 Security Hub는 조사 결과를 수신하는 데 필요한 권한을 자동으로 AWS Config할당합니다. Security Hub는 이 통합을 활성화하고 Amazon을 AWS Config 통해 결과를 가져올 수 있는 안전한 방법을 제공하는 service-to-service 수준 권한을 사용합니다 EventBridge.

조사 결과 전송 지연 시간

새 검색 결과를 AWS Config 만들면 일반적으로 5분 이내에 Security Hub에서 검색 결과를 볼 수 있습니다.

Security Hub를 사용할 수 없을 때 다시 시도

AWS Config 를 통해 EventBridge 최선의 노력을 다해 Security Hub에 결과를 전송합니다. 이벤트가 Security Hub에 성공적으로 전달되지 않으면 최대 24시간 또는 185회 (둘 중 먼저 도래하는 날짜 기준) 동안 전송을 EventBridge 재시도합니다.

Security Hub의 기존 AWS Config 조사 결과 업데이트

Security Hub로 검색 결과를 AWS Config 보낸 후 검색 결과 활동에 대한 추가 관찰 내용을 반영하기 위해 동일한 검색 결과에 대한 업데이트를 Security Hub에 보낼 수 있습니다. 업데이트는 `ComplianceChangeNotification` 이벤트에 대해서만 전송됩니다. 규정 준수 변경 사항이 발생하지 않으면 업데이트가 Security Hub로 전송되지 않습니다. Security Hub는 조사 결과를 가장 최근 업데이트 후 90일 또는 업데이트가 없는 경우 생성일 이후 90일에 삭제됩니다.

Security Hub는 연결된 리소스를 AWS Config 삭제하더라도 보낸 결과를 보관하지 않습니다.

AWS Config 검색 결과가 존재하는 지역

AWS Config 조사 결과는 지역별로 발생합니다. AWS Config 탐지 결과가 발생한 지역과 동일한 지역 또는 지역의 Security Hub로 조사 결과를 보냅니다.

Security Hub에서 AWS Config 조사 결과 보기

AWS Config 결과를 보려면 Security Hub 탐색 창에서 검색 결과를 선택합니다. 검색 결과만 표시하도록 검색 AWS Config 결과를 필터링하려면 검색 창 드롭다운에서 제품 이름을 선택합니다. 구성을 입력하고 적용을 선택합니다.

Security Hub에서 AWS Config 찾은 이름 해석하기

Security Hub는 AWS Config 규칙 평가를 다음 조사 결과로 변환합니다. AWS 보안 검색 형식 (ASFF) AWS Config 규칙 평가는 ASFF와 다른 이벤트 패턴을 사용합니다. 다음 표는 AWS Config 규칙 평가 필드를 Security Hub에 표시된 ASFF 대응 필드와 매핑합니다.

구성 규칙 평가 조사 결과 유형	ASFF 결과 유형	하드코딩된 값
세부 정보. awsAccountId	AwsAccountId	
세부 묘사. newEvaluationResult. resultRecordedTime	CreatedAt	
세부 묘사. newEvaluationResult. resultRecordedTime	UpdatedAt	
	ProductArn	"arn:<partition>:securityhub:<region>::product/aws/config"
	ProductName	"Config"
	CompanyName	"AWS"
	Region	"eu-central-1"
configRuleArn	GeneratorId, ProductFields	
세부 묘사. ConfigRuleARN/파인딩/해시	Id	
세부 정보. configRuleName	제목, ProductFields	
세부 정보. configRuleName	설명	“이 조사 결과는 구성 규칙 (`${detail.ConfigRuleName}`)의 리소스 규정 준수 변경을 위해 작성되었습니다.”

구성 규칙 평가 조사 결과 유형	ASFF 결과 유형	하드코딩된 값
구성 항목 “ARN” 또는 Security Hub가 계산한 ARN	Resources[i].id	
detail.resourceType	Resources[i].Type	"AwsS3Bucket"
	Resources[i].Partition	"aws"
	Resources[i].Region	"eu-central-1"
구성 항목 "configuration"	Resources[i].Details	
	SchemaVersion	"2018-10-08"
	Severity.Label	아래 “심각도 레이블 해석”을 참고하십시오
	타입	["소프트웨어 및 구성 점검"]
세부 묘사. newEvaluationResult. 규정 준수 유형	Compliance.Status	"실패함", "사용할 수 없음", "통과함" 또는 "경고"
	Workflow.Status	규정 준수 상태가 “통과”인 상태로 AWS Config 검색 결과가 생성되거나 규정 준수 상태가 “실패”에서 “통과”로 변경되는 경우 “해결됨”입니다. 그렇지 않은 경우에는 Workflow.Status가 “신규”가 됩니다. API 작업을 통해 이 값을 변경할 수 있습니다. BatchUpdateFindings

심각도 레이블 해석

AWS Config 규칙 평가의 모든 결과에는 ASFF의 기본 심각도 레이블이 MEDIUM으로 지정되어 있습니다. `BatchUpdateFindings` API 작업을 통해 조사 결과의 심각도 레이블을 업데이트할 수 있습니다.

일반적인 결과는 다음과 같습니다. AWS Config

Security Hub는 AWS Config 규칙 평가를 ASFF를 따르는 조사 결과로 변환합니다. 다음은 AWS Config ASFF에서 발견된 일반적인 결과의 예입니다.

> **Note**
>
> 설명이 1024자를 초과하면 1024자에서 잘리고 끝에 “(잘림)"이라고 표시됩니다.


```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
```

```
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::config-integration-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```


통합 활성화 및 구성

Security Hub를 활성화하면 이 통합이 자동으로 활성화됩니다. AWS Config 검색 결과를 Security Hub에 즉시 보내기 시작합니다.

Security Hub로의 결과 게시 중지

Security Hub로 조사 결과를 전송하는 작업을 중지하려면 Security Hub 콘솔 API 또는 AWS CLI를 사용하면 됩니다.

통합에서 조사 결과의 흐름 사용 중지 및 사용 설정(콘솔) 또는 통합에서 검색 결과 흐름 비활성화(Security Hub API, AWS CLI)을 참조하세요.

AWS Firewall Manager (조사 결과 전송)

Firewall Manager는 리소스에 대한 웹 애플리케이션 방화벽(WAF) 정책이나 웹 액세스 제어 목록(웹 ACL) 규칙이 규정을 준수하지 않을 경우 조사 결과를 Security Hub로 보냅니다. 또한 Firewall AWS Shield Advanced Manager는 리소스를 보호하고 있지 않거나 공격이 식별될 때 탐지 결과를 전송합니다.

Security Hub를 활성화하면 이 통합이 자동으로 활성화됩니다. Firewall Manager는 즉시 Security Hub로 조사 결과를 전송하기 시작합니다.

통합에 대해 자세히 알아보려면 Security Hub 콘솔의 통합 페이지를 확인하십시오.

Firewall Manager에 대해 자세히 알아보려면 AWS WAF 개발자 안내서를 참조하십시오.

Amazon GuardDuty (조사 결과 전송)

GuardDuty 생성된 모든 결과를 Security Hub에 보냅니다.

에서 GuardDuty 새로 찾은 결과는 5분 이내에 Security Hub로 전송됩니다. 검색 결과에 대한 업데이트는 EventBridge 설정에서 Amazon에 대한 업데이트된 검색 결과 GuardDuty 설정을 기반으로 전송됩니다.

GuardDuty 설정 페이지를 사용하여 GuardDuty 샘플 검색 결과를 생성하면 Security Hub는 샘플 검색 결과를 수신하고 검색 결과 `[Sample]` 유형에서 접두사를 생략합니다. 예를 들어 샘플 검색 결과는 Security `Recon:IAMUser/ResourcePermissions` Hub에서와 같이 표시됩니다. GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions`

Security Hub를 활성화하면 이 통합이 자동으로 활성화됩니다. GuardDuty 검색 결과를 Security Hub에 즉시 보내기 시작합니다.

GuardDuty 통합에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 AWS Security Hub와의 통합을 참조하십시오.

AWS Health (조사 결과 전송)

AWS Health 리소스 성능과 AWS 서비스 및 계정의 가용성에 대한 지속적인 가시성을 제공합니다. AWS Health 이벤트를 사용하여 서비스 및 리소스 변경이 AWS에서 실행 중인 애플리케이션에 어떤 영향을 미칠 수 있는지 알아볼 수 있습니다.

와의 통합은 사용되지 AWS Health 않습니다`BatchImportFindings`. 대신 service-to-service 이벤트 메시징을 AWS Health 사용하여 Security Hub에 결과를 전송합니다.

이 통합에 대한 자세한 내용은 다음 단원을 참조하십시오.

결과를 AWS Health Security Hub로 보내는 방법

Security Hub의 경우 보안 문제를 조사 결과와 같이 추적합니다. 일부 결과는 다른 AWS 서비스나 타사 파트너가 감지한 문제에서 비롯됩니다. Security Hub에는 보안 문제를 감지하고 조사 결과를 생성하는 데 사용하는 규칙 집합도 있습니다.

Security Hub는 이러한 모든 출처를 총망라하여 조사 결과를 관리할 도구를 제공합니다. 사용자는 조사 결과 목록을 조회하고 필터링할 수 있으며 주어진 조사 결과의 세부 정보를 조회할 수도 있습니다. 검색 결과 세부 정보 및 기록 관리 및 검토 섹션을 참조하십시오. 또한 주어진 결과에 대한 조사 상태를 추적할 수도 있습니다. 조사 결과에 대한 조치 취하기 AWS Security Hub 섹션을 참조하십시오.

Security Hub의 모든 조사 결과는 표준 JSON 형식을 사용합니다. 이를 AWS 보안 검색 형식 (ASFF)라고 합니다. ASFF에는 문제의 출처, 영향을 받은 리소스와 결과의 현재 상태 등에 관한 세부 정보가 포함됩니다.

AWS Health Security Hub에 조사 결과를 보내는 AWS 서비스 중 하나입니다.

Security Hub로 AWS Health 보내는 검색 결과 유형

통합이 활성화되면 생성되는 모든 보안 관련 결과를 Security Hub로 AWS Health 보냅니다. 조사 결과는 AWS 보안 검색 형식 (ASFF)를 사용하여 Security Hub로 전송됩니다. 보안 관련 조사 결과는 다음과 같이 정의됩니다.

- 보안 서비스와 관련된 모든 결과 AWS
- `securityabuse`, 또는 AWS Health TypeCode로 **`certificate`** 검색된 모든 결과
- AWS Health 서비스 위치 검색 결과 또는 `risk abuse`

Security Hub에 AWS Health 조사 결과 보내기

검색 결과를 수락하도록 선택하면 Security Hub는 검색 결과를 수신하는 데 필요한 권한을 자동으로 AWS Health할당합니다. AWS Health Security Hub는 service-to-service 수준 권한을 사용하여 이러한 통합을 활성화하고 사용자를 대신하여 Amazon을 AWS Health 통해 결과를 가져올 수 EventBridge 있는 안전하고 쉬운 방법을 제공합니다. 검색 결과 수락을 선택하면 Security Hub에 검색 결과를 사용할 수 있는 권한이 AWS Health부여됩니다.

조사 결과 전송 지연 시간

새 검색 결과가 AWS Health 생성되면 일반적으로 5분 이내에 Security Hub로 전송됩니다.

Security Hub를 사용할 수 없을 때 다시 시도

AWS Health 를 통해 EventBridge 최선의 노력을 다해 Security Hub에 결과를 전송합니다. 이벤트가 Security Hub에 성공적으로 전달되지 않으면 24시간 동안 이벤트 전송을 EventBridge 재시도합니다.

Security Hub에서 기존 조사 결과 업데이트

검색 결과를 Security Hub로 AWS Health 보낸 후 검색 결과 활동에 대한 추가 관찰 내용을 Security Hub에 반영하기 위해 동일한 검색 결과에 업데이트를 보낼 수 있습니다.

조사 결과가 존재하는 리전

글로벌 이벤트의 경우, Security Hub에 us-east-1 AWS (파티션), cn-northwest-1 (중국 파티션) 및 -1 (파티션) 으로 결과를 AWS Health 전송합니다. gov-us-west GovCloud AWS Health 이벤트가 발생한 동일한 지역 또는 지역의 Security Hub에 지역별 이벤트를 전송합니다.

Security Hub에서 AWS Health 조사 결과 보기

Security Hub에서 결과를 보려면 탐색 패널에서 검색 결과를 선택합니다. AWS Health 검색 결과를 필터링하여 결과만 AWS Health 표시하려면 제품 이름 필드에서 Health를 선택합니다.

Security Hub에서 AWS Health 찾은 이름 해석하기

AWS Health 를 사용하여 Security Hub에 결과를 AWS 보안 검색 형식 (ASFF) 전송합니다. AWS Health 찾기는 Security Hub ASFF 형식과 다른 이벤트 패턴을 사용합니다. 아래 표에는 Security Hub에 나타나는 ASFF 대응 필드와 함께 모든 AWS Health 검색 필드가 자세히 나와 있습니다.

상태 결과 유형	ASFF 결과 유형	하드코딩된 값
account	AwsAccountId	
detail.startTime	CreatedAt	
detail.eventDescription.latestDescription	설명	
세부 정보. eventTypeCode	GeneratorId	
detail.eventArn (including account) + hash of detail.startTime	Id	

상태 결과 유형	ASFF 결과 유형	하드코딩된 값
"arn:aws:securityhub:<region>::product/aws/health"	ProductArn	
account 또는 resourceId	Resources[i].id	
	Resources[i].Type	“기타”
	SchemaVersion	"2018-10-08"
	Severity.Label	아래 “심각도 레이블 해석”을 참고하십시오
“AWS Health -” 세부 정보. eventTypeCode	Title	
-	타입	["소프트웨어 및 구성 점검"]
event.time	UpdatedAt	
Health 콘솔의 이벤트 URL	SourceUrl	

심각도 레이블 해석

ASFF 조사 결과의 심각도 레이블은 다음 논리를 사용하여 결정됩니다.

- 심각도 심각인 경우:
  - AWS Health 검색 결과의 `service` 필드는 다음과 같은 값을 가집니다. `Risk`
  - AWS Health 검색 결과의 `typeCode` 필드는 다음과 같은 값을 가집니다. `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - AWS Health 검색 결과의 `typeCode` 필드는 다음과 같은 값을 가집니다. `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - AWS Health 검색 결과의 `typeCode` 필드는 다음과 같은 값을 가집니다. `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  다음과 같은 경우 심각도 높음:
  - AWS Health 검색 결과의 `service` 필드는 다음과 같은 값을 가집니다. `Abuse`

- AWS Health 검색 결과의 typeCode 필드에는 값이 포함됩니다. SECURITY_NOTIFICATION
- AWS Health 검색 결과의 typeCode 필드에는 값이 포함됩니다. ABUSE_DETECTION

심각도 중간인 경우:

- 조사 결과의 service 필드는 ACM, ARTIFACT, AUDITMANAGER, BACKUP,CLOUDENDURE, CLOUDHSM, CLOUDTRAIL, CLOUDWATCH, CODEGURGU, COGNITO, CONFIG, CONTROLTOWER, DETECTIVE, DIRECTORYSERVICE, DRS, EVENTS, FIREWALLMANAGER, GUARDDUTY, IAM, INSPECTOR, INSPECTOR2, IOTDEVICEDEFENDER, KMS, MACIE, NETWORKFIREWALL, ORGANIZATIONS, RESILIENCEHUB, RESOURCEMANAGER, ROUTE53, SECURITYHUB, SECRETSMANAGER, SES, SHIELD, SSO 또는 WAF이 될 수 있습니다.
- AWS Health 조사 결과의 typeCode 필드는 CERTIFICATE 값을 가집니다.
- AWS Health 조사 결과의 typeCode 필드는 END_OF_SUPPORT 값을 가집니다.

일반적인 결과는 다음과 같습니다. AWS Health

AWS Health 를 사용하여 Security Hub에 결과를 보냅니다AWS 보안 검색 형식 (ASFF). 다음은 에서 찾은 일반적인 결과의 예입니다 AWS Health.

> **Note**
>
> 설명이 1024자를 초과하면 1024자에서 잘리고 끝에 (잘림) 라고 표시됩니다.

```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
```

```
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
```

```
}
```

통합 활성화 및 구성

Security Hub를 활성화하면 이 통합이 자동으로 활성화됩니다. AWS Health 검색 결과를 Security Hub에 즉시 보내기 시작합니다.

Security Hub로의 결과 게시 중지

검색 결과를 Security Hub로 보내는 것을 중지하려면 Security Hub 콘솔, Security Hub API 또는 을 사용할 수 AWS CLI있습니다.

통합에서 조사 결과의 흐름 사용 중지 및 사용 설정(콘솔) 또는 통합에서 검색 결과 흐름 비활성화(Security Hub API, AWS CLI)을 참조하세요.

AWS Identity and Access Management Access Analyzer (조사 결과 전송)

IAM 액세스 분석기를 사용하면 모든 조사 결과가 Security Hub로 전송됩니다.

IAM 액세스 분석기는 논리 기반 추론을 통해 계정에서 지원되는 리소스에 적용되는 리소스 기반 정책을 분석합니다. IAM 액세스 분석기는 외부 보안 주체가 사용자 계정의 리소스에 액세스할 수 있도록 하는 정책 문을 감지할 때 결과를 생성합니다.

IAM Access Analyzer에서는 관리자 계정만 조직에 적용되는 분석기에 대한 조사 결과를 볼 수 있습니다. 조직 분석기의 경우, `AwsAccountId` ASFF 필드는 관리자 계정 ID를 반영합니다. `ProductFields`에서 `ResourceOwnerAccount` 필드는 조사 결과가 발견된 계정을 나타냅니다. 각 계정에 대해 분석기를 개별적으로 활성화하면, Security Hub는 관리자 계정 ID를 식별하는 조사 결과와 리소스 계정 ID를 식별하는 조사 결과 등 여러 조사 결과를 생성합니다.

자세한 내용은 IAM 사용 설명서에 있는 AWS Security Hub와의 통합을 참고하십시오.

Amazon Inspector(조사 결과를 전송함)

Amazon Inspector는 AWS 워크로드에서 취약성을 지속적으로 검사하는 취약성 관리 서비스입니다. Amazon Inspector는 Amazon Elastic 컨테이너 레지스트리에 상주하는 Amazon EC2 인스턴스와 컨테이너 이미지를 자동으로 검색하고 스캔합니다. 이 검사는 소프트웨어 취약성과 의도하지 않은 네트워크 노출을 찾습니다.

Security Hub를 활성화하면 이 통합이 자동으로 활성화됩니다. Amazon Inspector는 생성한 모든 조사 결과를 즉시 Security Hub로 보내기 시작합니다.

통합에 대한 자세한 내용은 Amazon Inspector 사용 설명서의 AWS Security Hub와의 통합을 참조하십시오.

Security Hub는 Amazon Inspector Classic에서 조사 결과를 받을 수도 있습니다. Amazon Inspector Classic에서는 지원되는 모든 규칙 패키지에 대한 평가 실행을 통해 생성된 조사 결과를 Security Hub로 전송합니다.

통합에 대한 자세한 내용은 Amazon Inspector Classic 사용 설명서의 AWS Security Hub와의 통합을 참조하십시오.

Amazon Inspector 및 Amazon Inspector Classic의 조사 결과는 동일한 제품 ARN을 사용합니다. Amazon Inspector 조사 결과에는 `ProductFields`에 다음과 같은 항목이 있습니다.

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender (조사 결과 전송)

AWS IoT Device Defender IoT 장치의 구성을 감사하고, 연결된 장치를 모니터링하여 비정상적인 동작을 탐지하고, 보안 위험을 완화하는 데 도움이 되는 보안 서비스입니다.

Security Hub를 모두 AWS IoT Device Defender 활성화한 후 Security Hub 콘솔의 통합 페이지로 이동하여 감사 결과 수락, 탐지 또는 둘 다를 선택합니다. AWS IoT Device Defender 감사 및 탐지는 모든 결과를 Security Hub로 보내기 시작합니다.

AWS IoT Device Defender Audit는 특정 감사 검사 유형 및 감사 작업에 대한 일반 정보가 포함된 검사 요약을 Security Hub에 보냅니다. AWS IoT Device Defender Detect는 기계 학습 (ML), 통계 및 정적 동작에 대한 위반 결과를 Security Hub에 보냅니다. 또한, 감사는 Security Hub로 조사 결과 업데이트를 전송합니다.

이 통합에 대한 자세한 내용은 AWS IoT 개발자 안내서의 AWS Security Hub와의 통합을 참조하십시오.

Amazon Macie(조사 결과를 전송합니다)

Macie의 결과는 잠재적 정책 위반 사항이 있거나 조직이 Amazon S3에 저장하는 데이터에 개인 식별 정보(PII)와 같은 민감한 데이터가 있음을 나타낼 수 있습니다.

Security Hub를 활성화하면 Macie는 자동으로 Security Hub에 정책 조사 결과를 보내기 시작합니다. 민감한 데이터 조사 결과를 Security Hub로 전송하도록 통합을 구성할 수도 있습니다.

Security Hub에서 정책 또는 민감한 데이터 조사 결과에 대한 조사 결과 유형이 ASFF와 호환되는 값으로 변경됩니다. 예를 들어, Macie에서 `Policy:IAMUser/S3BucketPublic` 조사 결과 유형은

Security Hub에서 `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic`으로 표시됩니다.

또한, Macie는 생성된 샘플 조사 결과를 Security Hub로 전송합니다. 샘플 조사 결과의 경우 영향을 받는 리소스의 이름은 `macie-sample-finding-bucket`이고 `Sample` 필드의 값은 `true`입니다.

자세한 내용은 Amazon Macie 사용 설명서에 있는 Amazon Macie와 AWS Security Hub와의 통합을 참고하십시오.

AWS Systems Manager 패치 관리자 (결과 전송)

AWS Systems Manager Patch Manager는 고객 플릿의 인스턴스가 패치 규정 준수 표준을 위반하는 경우 Security Hub에 결과를 보냅니다.

패치 관리자는 보안 관련 및 기타 유형의 업데이트로 관리형 인스턴스에 패치를 적용하는 프로세스를 자동화해 줍니다.

Security Hub를 활성화하면 이 통합이 자동으로 활성화됩니다. Systems Manager Patch Manager가 즉시 Security Hub로 조사 결과를 전송하기 시작합니다.

패치 관리자 사용에 대한 자세한 내용은AWS Systems Manager 사용자 설명서의 AWS Systems Manager 패치 관리자를 참조하십시오.

AWS Security Hub로부터 조사 결과를 받는 서비스

다음 AWS 서비스는 Security Hub와 통합되어 있으며 Security Hub로부터 조사 결과를 받습니다. 별도로 명시되어 있는 경우, 통합 서비스는 조사 결과를 업데이트할 수도 있습니다. 이 경우, 통합 서비스에 조사 결과를 업데이트하면 Security Hub에도 반영됩니다.

AWS Audit Manager (조사 결과 수신)

AWS Audit Manager Security Hub로부터 조사 결과를 받습니다. 이러한 조사 결과는 Audit Manager 사용자가 감사를 준비하는 데 도움이 됩니다.

Audit Manager에 대한 자세한 내용은 AWS Audit Manager 사용 설명서를 참조하십시오. AWSAWS Audit Manager에서 지원하는 Security Hub 검사 Security Hub가 감사 관리자로 조사 결과를 보내는 데 사용되는 제어 기능이 나열되어 있습니다.

AWS Chatbot (조사 결과 수신)

AWS Chatbot Slack 채널 및 Amazon Chime 채팅방에서 AWS 리소스를 모니터링하고 상호 작용할 수 있도록 도와주는 대화형 에이전트입니다.

AWS Chatbot Security Hub로부터 조사 결과를 받습니다.

Security AWS Chatbot Hub와의 통합에 대해 자세히 알아보려면 AWS Chatbot 관리자 안내서의 Security Hub 통합 개요를 참조하십시오.

Amazon Detective(조사 결과를 수신합니다)

Detective는 AWS 리소스에서 로그 데이터를 자동으로 수집하고 기계 학습, 통계 분석 및 그래프 이론을 사용하여 보다 빠르고 효율적인 보안 조사를 시각화하고 수행할 수 있도록 지원합니다.

Security Hub와 Detective의 통합을 통해 Security Hub의 GuardDuty Amazon 조사 결과를 Detective로 전환할 수 있습니다. 그런 다음 조사 도구와 시각화를 사용하여 이 결과를 조사할 수 있습니다. 통합에는 Security Hub 또는 탐지에서 추가 구성이 필요하지 않습니다.

다른 AWS 서비스사람으로부터 받은 조사 결과에 대해서는 Security Hub 콘솔의 검색 결과 세부 정보 패널에 Detective 내 조사 하위 섹션이 포함되어 있습니다. 해당 하위 섹션에는 Detective로 연결되는 링크가 포함되어 있으며, 이 링크를 통해 조사 결과에서 보고된 보안 문제를 추가로 조사할 수 있습니다. 또한, Security Hub 조사 결과를 기반으로 Detective에서 동작 그래프를 작성하여 보다 효과적인 조사를 수행할 수 있습니다. 자세한 내용은 Amazon Detective 관리 설명서의 AWS 보안 조사 결과를 참고하십시오.

리전 간 집계가 활성화된 경우 집계 리전에서 피벗하면 조사 결과가 발생한 리전에서 Detective가 열립니다.

링크가 작동하지 않는 경우 문제 해결 방법은 피벗 문제 해결을 참조하십시오.

Amazon Security Lake(조사 결과를 수신합니다)

Security Lake는 완전 관리형 보안 데이터 레이크 서비스입니다. Security Lake는 클라우드, 온프레미스 및 사용자 지정 소스의 보안 데이터를 계정에 저장된 데이터 레이크로 자동 중앙 집중화합니다. 구독자는 조사 및 분석 사용 사례에 Security Lake의 데이터를 사용할 수 있습니다.

이 통합을 활성화하려면 두 서비스를 모두 활성화하고 Security Lake 콘솔, Security Lake API 또는 Security Hub를 소스로 추가해야 AWS CLI합니다. 이 단계를 완료하면 Security Hub가 모든 조사 결과를 Security Lake로 보내기 시작합니다.

Security Lake는 Security Hub의 조사 결과를 자동으로 정규화하고 이를 개방형 사이버 보안 스키마 프레임워크(OCSF)로 불리는 표준화된 오픈 소스 스키마로 변환합니다. Security Lake에서는 구독자를 한 명 이상 추가하여 Security Hub의 조사 결과를 사용할 수 있습니다.

Security Hub를 소스로 추가하고 구독자를 생성하는 방법에 대한 지침을 포함하여 이 통합에 대한 자세한 내용은 Amazon AWS Security Lake 사용 설명서의 Security Hub와의 통합을 참조하십시오.

AWS Systems Manager 탐색기 및 OpsCenter (결과 수신 및 업데이트)

AWS Systems Manager 탐색하고 Security Hub에서 결과를 OpsCenter 수신하고 Security Hub에서 해당 결과를 업데이트합니다.

Explorer는 사용자 지정 가능한 대시보드를 제공하여 사용자의 AWS 환경에 대한 운영 상태 및 성능에 주요 인사이트와 분석을 제공합니다.

OpsCenter 운영 작업 항목을 보고, 조사하고, 해결할 수 있는 중앙 위치를 제공합니다.

Explorer 및 OpsCenter 에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 작업 관리를 참조하십시오.

AWS Trusted Advisor (조사 결과 수신)

Trusted Advisor 수십만 명의 AWS 고객에게 서비스를 제공하면서 배운 모범 사례를 활용합니다. Trusted Advisor AWS 환경을 검사한 다음 비용을 절감하고, 시스템 가용성 및 성능을 개선하거나, 보안 격차를 줄이는 데 도움이 되는 기회가 있을 때 권장 사항을 제시합니다.

Security Trusted Advisor Hub와 둘 다 활성화하면 통합이 자동으로 업데이트됩니다.

Security Hub는 AWS 기본 보안 모범 사례 검사 결과를 에 보냅니다. Trusted Advisor

Security Hub 통합에 대한 자세한 내용은 AWS 지원 사용 설명서의 AWS Security Hub 컨트롤 보기를 참조하십시오. Trusted Advisor AWS Trusted Advisor

사용 가능한 타사 파트너 제품 통합

AWS Security Hub는 여러 타사 파트너 제품과 통합됩니다. 통합은 다음 작업 중 하나 이상을 수행할 수 있습니다.

- 생성된 조사 결과를 Security Hub로 전송합니다.
- Security Hub에서 조사 결과를 수신합니다.
- Security Hub에서 조사 결과를 업데이트합니다.

조사 결과를 Security Hub로 보내는 모든 통합에는 Amazon 리소스 이름(ARN)이 있습니다.

> **Note**
>
> 일부 통합은 일부 지역에서만 사용할 수 있습니다. AWS 리전
> Security Hub 콘솔의 통합 페이지에는 현재 리전에서 지원되는 모든 통합이 나열됩니다.

자세한 정보는 중국(베이징) 및 중국(닝샤)에서 지원되는 통합 및 AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 에서 지원되는 통합 섹션을 참조하십시오.

보안 솔루션이 있고 Security Hub 파트너가 되는 데 관심이 있다면 <securityhub-partners@amazon.com>으로 이메일을 보내주십시오. 자세한 내용은 AWS Security Hub 파트너 통합 가이드를 참조하십시오.

타사와 Security Hub의 통합 개요

다음은 조사 결과를 Security Hub로 전송하거나 Security Hub에서 조사 결과를 수령하는 타사 통합의 개요입니다.

통합	Direction	ARN(해당하는 경우)
3CORESec – 3CORESec NTA	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/aqua-security/kube-bench
Armor – Armor Anywhere	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:679703615338:product/armor

통합	Direction	ARN(해당하는 경우)
		defense/armoranywhere
AttackIQ – AttackIQ	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:151784055945:product/barracuda/cloudsecurityguardian
BigID – BigID Enterprise	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/blue-hexagon/blue-hexagon-for-aws
Capitis Solutions – C2VS	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/capitis/c2vs
Check Point – CloudGuard IaaS	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:758245563457:product/checkpoint/cloudguard-iaas

통합	Direction	ARN(해당하는 경우)
Check Point – CloudGuard Posture Management	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/claroty/xdome
Cloud Storage Security – Antivirus for Amazon S3	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/data-theorem/api-cloud-web-secure

통합	Direction	ARN(해당하는 경우)
Drata	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/drata/drata-integration
Forcepoint – Forcepoint CASB	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-casb
Forcepoint – Forcepoint Cloud Security Gateway	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/fugue/fugue

통합	Direction	ARN(해당하는 경우)
Guardicore – Centra 4.0	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/guardicore/guardicore
HackerOne – Vulnerability Intelligence	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/hackerone/vulnerability-intelligence
JFrog – Xray	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/k9-security/access-analyzer
Lacework – Lacework	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/mcafee-skyhigh/mcafee-mvision-cloud-aws

통합	Direction	ARN(해당하는 경우)
NETSCOUT – NETSCOUT Cyber Investigator	조사 결과를 전송합니다	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator
Palo Alto Networks – Prisma Cloud Compute	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:496947949261:product/twistlock/twistlock-enterprise
Palo Alto Networks – Prisma Cloud Enterprise	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/plerion/cloud-security-platform
Prowler – Prowler	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/prowler/prowler
Qualys – Vulnerability Management	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:805950163170:product/qualys/qualys-vm
Rapid7 – InsightVM	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:336818582268:product/rapid7/insightvm

통합	Direction	ARN(해당하는 경우)
SecureCloudDB – SecureCloudDB	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/securecloudd b/securecloudd b
SentinelOne – SentinelOne	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/sentinelone/endpoint-protection
Snyk	조사 결과를 전송합니다	arn:aws:securityhub: *<region>*::product/snyk/snyk
Sonrai Security – Sonrai Dig	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/sonrai-security/sonrai-dig
Sophos – Server Protection	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:064897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:956882708938:product/sumologicinc/sumologic-mda

통합	Direction	ARN(해당하는 경우)
Symantec – Cloud Workload Protection	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:754237914691:product/symantec-corp/symantec-cwp
Tenable – Tenable.io	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/trend-micro/cloud-one
Vectra – Cognito Detect	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*:978576646331:product/vectra-ai/cognito-detect
Wiz	조사 결과를 전송합니다	arn:aws:securityhub: *<REGION>*::product/wiz-security/wiz-security
Atlassian - Jira Service Management	조사 결과 수령 및 업데이트	해당 사항 없음
Atlassian - Jira Service Management Cloud	조사 결과 수령 및 업데이트	해당 사항 없음
Atlassian – Opsgenie	조사 결과를 수신합니다	해당 사항 없음
Fortinet – FortiCNP	조사 결과를 수신합니다	해당 사항 없음
IBM – QRadar	조사 결과를 수신합니다	해당 사항 없음

통합	Direction	ARN(해당하는 경우)
Logz.io Cloud SIEM	조사 결과를 수신합니다	해당 사항 없음
MetricStream	조사 결과를 수신합니다	해당 사항 없음
MicroFocus – MicroFocus Arcsight	조사 결과를 수신합니다	해당 사항 없음
New Relic Vulnerability Management	조사 결과를 수신합니다	해당 사항 없음
PagerDuty – PagerDuty	조사 결과를 수신합니다	해당 사항 없음
Palo Alto Networks – Cortex XSOAR	조사 결과를 수신합니다	해당 사항 없음
Palo Alto Networks – VM-Series	조사 결과를 수신합니다	해당 사항 없음
Rackspace Technology – Cloud Native Security	조사 결과를 수신합니다	해당 사항 없음
Rapid7 – InsightConnect	조사 결과를 수신합니다	해당 사항 없음
RSA – RSA Archer	조사 결과를 수신합니다	해당 사항 없음
ServiceNow – ITSM	조사 결과 수령 및 업데이트	해당 사항 없음
Slack – Slack	조사 결과를 수신합니다	해당 사항 없음
Splunk – Splunk Enterprise	조사 결과를 수신합니다	해당 사항 없음
Splunk – Splunk Phantom	조사 결과를 수신합니다	해당 사항 없음
ThreatModeler	조사 결과를 수신합니다	해당 사항 없음
Trellix – Trellix Helix	조사 결과를 수신합니다	해당 사항 없음

통합	Direction	ARN(해당하는 경우)
Caveonix – Caveonix Cloud	조사 결과 전송 및 수신	arn:aws:securityhub: *<REGION>*::product/caveonix/caveonix-cloud
Cloud Custodian – Cloud Custodian	조사 결과 전송 및 수신	arn:aws:securityhub: *<REGION>*::product/cloud-custodian/cloud-custodian
DisruptOps, Inc. – DisruptOPS	조사 결과 전송 및 수신	arn:aws:securityhub: *<REGION>*::product/disruptops-inc/disruptops
Kion	조사 결과 전송 및 수신	arn:aws:securityhub: *<REGION>*::product/cloudtamerio/cloudtamerio
Turbot – Turbot	조사 결과 전송 및 수신	arn:aws:securityhub: *<REGION>*:453761072151:product/turbot/turbot

Security Hub로 조사 결과를 전송하는 타사 통합

다음 타사 파트너 제품 통합은 Security Hub로 조사 결과를 전송합니다. Security Hub는 조사 결과를 AWS 보안 조사 결과 형식으로 변환합니다.

3CORESec – 3CORESec NTA

통합 유형: 전송

제품 ARN: arn:aws:securityhub:*<REGION>*::product/3coresec/3coresec

3CORESec은 온프레미스와 AWS 시스템 모두에 대한 관리형 탐지 서비스를 제공합니다. Security Hub와의 통합을 통해 멀웨어, 권한 에스컬레이션, 수평 이동, 부적절한 네트워크 분할 등의 위협을 파악할 수 있습니다.

제품 링크

파트너 설명서

Alert Logic – SIEMless Threat Management

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

취약성 및 자산 가시성, 위협 탐지 및 사고 관리 AWS WAF, 지정된 SOC 분석가 옵션 등 적절한 수준의 적용 범위를 확보하십시오.

제품 링크

파트너 설명서

Aqua Security – Aqua Cloud Native Security Platform

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)은 CI/CD 파이프라인부터 실행 시간 프로덕션 환경에 이르기까지 컨테이너 기반 및 서버리스 애플리케이션에 대한 전체 수명 주기 보안을 제공합니다.

제품 링크

파트너 설명서

Aqua Security – Kube-bench

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench는 사용자 환경에서 인터넷 보안 센터(CIS) Kubernetes 벤치마크를 실행하는 오픈 소스 도구입니다.

제품 링크

파트너 설명서

Armor – Armor Anywhere

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere에 대한 관리형 보안 및 규정 준수를 제공합니다. AWS

제품 링크

파트너 설명서

AttackIQ – AttackIQ

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform은 MITRE ATT&CK 프레임워크에 따른 실제 적대적 동작을 에뮬레이션하여 전체 보안 태세를 검증하고 개선하는 데 도움이 됩니다.

제품 링크

파트너 설명서

Barracuda Networks – Cloud Security Guardian

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry는 조직이 퍼블릭 클라우드에 애플리케이션을 구축하고 워크로드를 이동하는 동안 보안을 유지할 수 있도록 지원합니다.

AWS 마켓플레이스 링크

제품 링크

BigID – BigID Enterprise

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management Platform은 기업이 모든 시스템에서 민감한 데이터(PII)를 관리하고 보호하는 데 도움이 됩니다.

제품 링크

파트너 설명서

Blue Hexagon— Blue Hexagon 용 AWS

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon은 실시간 위협 탐지 플랫폼입니다. 딥 러닝 원리를 사용하여 멀웨어 및 네트워크 이상을 포함하여 알려진 위협과 알려지지 않은 위협을 탐지합니다.

AWS 마켓플레이스 링크

파트너 설명서

Capitis Solutions – C2VS

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/capitis/c2vs`

C2VS는 애플리케이션별 구성 오류 및 이에 대한 근본 원인을 자동으로 식별하도록 설계된 맞춤형 규정 준수 솔루션입니다.

제품 링크

파트너 설명서

Check Point – CloudGuard IaaS

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard포괄적인 위협 방지 보안을 클라우드의 자산을 보호하는 AWS 동시에 포괄적 위협 방지 보안을 쉽게 확장할 수 있습니다.

제품 링크

파트너 설명서

Check Point – CloudGuard Posture Management

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

검증 가능한 클라우드 네트워크 보안, 향상된 IAM 보호, 포괄적인 규정 준수와 거버넌스를 제공하는 SaaS 플랫폼입니다.

제품 링크

파트너 설명서

Claroty – xDome

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome은 조직이 산업(OT), 의료(IoMT) 및 엔터프라이즈(IoT) 환경 내의 확장된 사물 인터넷(xIOT)을 통해 사이버 물리 시스템을 보호할 수 있도록 지원합니다.

제품 링크

파트너 설명서

Cloud Storage Security – Antivirus for Amazon S3

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security은 Amazon S3 객체에 대한 클라우드 네이티브 멀웨어 방지 및 안티바이러스 스캐닝을 제공합니다.

Antivirus for Amazon S3는 Amazon S3에 있는 객체와 파일에 대한 멀웨어 및 위협에 대한 실시간 및 예약 스캔을 제공합니다. 문제 및 감염된 파일에 대한 가시성과 해결책을 제공합니다.

제품 링크

파트너 설명서

Contrast Security – Contrast Assess

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess은 웹 앱, API 및 마이크로서비스에서 실시간 취약성 탐지를 제공하는 IAST 도구입니다. Contrast Assess는 Security Hub와 통합되어 모든 워크로드에 대한 중앙 집중식 가시성과 응답을 제공합니다.

제품 링크

파트너 설명서

CrowdStrike – CrowdStrike Falcon

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

CrowdStrike Falcon 단일 경량 센서는 차세대 안티바이러스, 엔드포인트 감지 및 응답, 클라우드를 통한 24/7 관리형 헌팅을 통합합니다.

제품 링크

파트너 설명서

CyberArk – Privileged Threat Analytics

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics는 권한 있는 계정의 고위험 활동 및 동작을 수집, 감지하고 이에 대해 경고하고 대응하여 진행 중인 공격을 억제합니다.

제품 링크

파트너 설명서

Data Theorem – Data Theorem

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theorem웹 애플리케이션, API 및 클라우드 리소스를 지속적으로 스캔하여 보안 결함과 데이터 프라이버시 격차를 찾아 데이터 침해를 방지합니다. AppSec

제품 링크

파트너 설명서

Drata

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata는 SOC2, ISO, GDPR과 같은 다양한 프레임워크를 준수하고 유지할 수 있도록 지원하는 규정 준수 자동화 플랫폼입니다. Drata와 Security Hub 간의 통합을 통해 보안 조사 결과를 한 곳에서 중앙 집중화할 수 있습니다.

AWS 마켓플레이스 링크

파트너 설명서

Forcepoint – Forcepoint CASB

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB를 사용하면 클라우드 애플리케이션 사용을 검색하고, 위험을 분석하며, SaaS 및 사용자 지정 애플리케이션에 대한 적절한 제어를 적용할 수 있습니다.

제품 링크

파트너 설명서

Forcepoint – Forcepoint Cloud Security Gateway

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway은 어디에 있든 사용자와 데이터에 대한 가시성, 제어 및 위협 보호를 제공하는 융합 클라우드 보안 서비스입니다.

제품 링크

파트너 설명서

Forcepoint – Forcepoint DLP

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP는 사용자가 작업하고 데이터가 상주하는 모든 곳에서 가시성과 제어 기능을 통해 사용자로 인해 발생한 위험을 해결합니다.

제품 링크

파트너 설명서

Forcepoint – Forcepoint NGFW

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW네트워크를 관리하고 위협에 대응하는 데 필요한 확장성, 보호 및 통찰력을 갖춘 AWS 환경을 엔터프라이즈 네트워크에 연결할 수 있습니다.

제품 링크

파트너 설명서

Fugue – Fugue

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue에이전트가 필요 없고 확장 가능한 클라우드 네이티브 플랫폼으로, 동일한 정책을 사용하여 클라우드 런타임 환경의 지속적인 검증을 자동화합니다. infrastructure-as-code

제품 링크

파트너 설명서

Guardicore – Centra 4.0

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra는 최신 데이터 센터 및 클라우드의 워크로드에 대한 흐름 시각화, 마이크로 분할 및 위반 감지 기능을 제공합니다.

제품 링크

파트너 설명서

HackerOne – Vulnerability Intelligence

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

이 HackerOne 플랫폼은 전 세계 해커 커뮤니티와 협력하여 가장 관련성이 높은 보안 문제를 찾아냅니다. Vulnerability Intelligence는 조직이 자동 스캔에서 더 나아갈 수 있도록 지원합니다. HackerOne 윤리적 해커가 검증하고 재현 단계를 제공한 취약성을 공유합니다.

AWS 마켓플레이스 링크

파트너 설명서

JFrog – Xray

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray는 바이너리에서 라이선스 규정 준수 및 보안 취약성을 지속적으로 스캔하여 안전한 소프트웨어 공급망을 운영할 수 있도록 하는 범용 애플리케이션 보안 소프트웨어 구성 분석(SCA) 도구입니다.

AWS 마켓플레이스 링크

파트너 설명서

Juniper Networks – vSRX Next Generation Firewall

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks' vSRX 가상 차세대 방화벽은 고급 보안, 안전한 SD-WAN, 강력한 네트워킹 및 내장된 자동화를 갖춘 완벽한 클라우드 기반 가상 방화벽을 제공합니다.

AWS 마켓플레이스 링크

파트너 설명서

제품 링크

k9 Security – Access Analyzer

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security AWS Identity and Access Management 계정에 중요한 액세스 변경이 발생하면 알려줍니다. 를 통해 k9 Security 사용자 및 IAM 역할이 중요 AWS 서비스 데이터와 데이터에 대해 갖는 액세스 권한을 이해할 수 있습니다.

k9 Security지속적인 전송을 위해 구축되었으므로 실행 가능한 액세스 감사와 Terraform에 대한 간단한 정책 자동화를 통해 IAM을 운영할 수 있습니다. AWS CDK

제품 링크

파트너 설명서

Lacework – Lacework

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework은 클라우드를 위한 데이터 기반 보안 플랫폼입니다. Lacework 클라우드 보안 플랫폼은 대규모 클라우드 보안을 자동화하여 빠르고 안전하게 혁신할 수 있도록 합니다.

제품 링크

파트너 설명서

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)은 AWS 환경에 맞는 클라우드 보안 상태 관리(CSPM) 및 클라우드 워크로드 보호 플랫폼(CWPP)을 제공합니다.

제품 링크

파트너 설명서

NETSCOUT – NETSCOUT Cyber Investigator

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator은 사이버 위협이 기업에 미치는 영향을 줄이는 데 도움이 되는 전사적 네트워크 위협, 위험 조사 및 포렌식 분석 플랫폼입니다.

제품 링크

파트너 설명서

Palo Alto Networks – Prisma Cloud Compute

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute은 VM, 컨테이너 및 서버리스 플랫폼을 보호하는 클라우드 네이티브 사이버 보안 플랫폼입니다.

제품 링크

파트너 설명서

Palo Alto Networks – Prisma Cloud Enterprise

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

클라우드 보안 분석, 고급 위협 탐지 및 규정 준수 모니터링으로 AWS 배포를 보호합니다.

제품 링크

파트너 설명서

Plerion – Cloud Security Platform

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion은 워크로드 전반에 걸쳐 예방, 탐지 및 시정 조치를 제공하는 위협 중심의 고유한 위험 기반 접근 방식을 갖춘 클라우드 보안 플랫폼입니다. Plerion과 Security Hub 간의 통합을 통해 고객은 보안 조사 결과를 한 곳에서 중앙 집중화하고 조치를 취할 수 있습니다.

AWS 마켓플레이스 링크

파트너 설명서

Prowler – Prowler

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler보안 모범 사례, 강화 및 지속적인 모니터링과 관련된 AWS 검사를 수행하는 오픈 소스 보안 도구입니다.

제품 링크

파트너 설명서

Qualys – Vulnerability Management

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM)은 취약성을 지속적으로 스캔하고 식별하여 자산을 보호합니다.

제품 링크

파트너 설명서

Rapid7 – InsightVM

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM 은 최신 환경에 대한 취약성 관리 기능을 제공하므로 취약성을 효율적으로 찾고, 우선 순위를 지정하고, 문제를 해결할 수 있습니다.

제품 링크

파트너 설명서

SecureCloudDB – SecureCloudDB

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/securecloudddb/securecloudddb`

SecureCloudDB은 내부 및 외부 보안 태세와 활동에 대한 포괄적인 가시성을 제공하는 클라우드 네이티브 데이터베이스 보안 도구입니다. 보안 위반을 알리고 악용 가능한 데이터베이스 취약성에 대한 해결책을 제공합니다.

제품 링크

파트너 설명서

SentinelOne – SentinelOne

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne은 엔드포인트, 컨테이너, 클라우드 워크로드 및 IoT 기기 전반에서 AI 기반 예방, 탐지, 대응 및 헌팅을 포함하는 자율 확장 탐지 및 대응(XDR) 플랫폼입니다.

AWS 마켓플레이스 링크

제품 링크

Snyk

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk은 AWS에서 실행 중인 워크로드의 보안 위험에 대해 앱 구성 요소를 스캔하는 보안 플랫폼을 제공합니다. 이러한 위험은 Security Hub에 조사 결과로 전송되므로 개발자와 보안 팀이 나머지 AWS 보안 결과와 함께 해당 위험을 시각화하고 우선 순위를 정하는 데 도움이 됩니다.

AWS 마켓플레이스 링크

파트너 설명서

Sonrai Security – Sonrai Dig

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig은 클라우드 구성 오류 및 정책 위반을 모니터링하고 수정하여 보안 및 규정 준수 태세를 개선할 수 있습니다.

제품 링크

파트너 설명서

Sophos – Server Protection

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection포괄적인 defense-in-depth 기술을 사용하여 조직의 핵심에 있는 중요한 애플리케이션과 데이터를 보호합니다.

제품 링크

파트너 설명서

StackRox – StackRox Kubernetes Security

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox은 기업이 전체 컨테이너 수명 주기(구축, 배포, 실행)에 걸쳐 규정 준수 및 보안 정책을 적용하여 규모에 따라 컨테이너 및 Kubernetes 배포를 보호할 수 있도록 지원합니다.

제품 링크

파트너 설명서

Sumo Logic – Machine Data Analytics

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic은 개발 및 보안 운영 팀이 AWS 애플리케이션을 구축, 실행하고 보호할 수 있게 해주는 안전한 머신 데이터 분석 플랫폼입니다.

제품 링크

파트너 설명서

Symantec – Cloud Workload Protection

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection은 멀웨어 방지, 침입 방지 및 파일 무결성 모니터링을 통해 Amazon EC2 인스턴스를 완벽하게 보호합니다.

제품 링크

파트너 설명서

Tenable – Tenable.io

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

취약성을 정확하게 식별, 조사하고 우선 순위를 지정합니다. 클라우드에서 관리됩니다.

제품 링크

파트너 설명서

Trend Micro – Cloud One

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One은 적절한 시기와 장소에서 팀에 적절한 보안 정보를 제공합니다. 이 통합은 보안 결과를 Security Hub에 실시간으로 전송하여 Security Hub의 AWS 리소스 및 Trend Micro Cloud One 이벤트 세부 정보에 대한 가시성을 향상시킵니다.

AWS 마켓플레이스 링크

파트너 설명서

Vectra – Cognito Detect

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra는 고급 AI를 적용하여 숨어 있는 사이버 공격자가 도용하거나 피해를 입히기 전에 이를 감지하고 대응하여 사이버 보안을 변화시키고 있습니다.

AWS 마켓플레이스 링크

파트너 설명서

Wiz – Wiz Security

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz사용자, 워크로드 전반의 구성, 취약성, 네트워크, IAM 설정 AWS 계정, 비밀 등을 지속적으로 분석하여 실제 위험을 나타내는 중요한 문제를 발견합니다. Wiz와 Security Hub를 통합하여 Wiz가 Security Hub 콘솔에서 감지한 문제를 시각화하고 이에 대응하십시오.

AWS 마켓플레이스 링크

파트너 설명서

Security Hub에서 조사 결과를 수령하는 타사 통합

Security Hub에서 조사 결과를 수령하는 타사 파트너 제품 통합은 다음과 같습니다. 명시된 경우, 제품이 조사 결과를 업데이트할 수도 있습니다. 이 경우 파트너 제품에서 업데이트한 조사 결과도 Security Hub에 반영됩니다.

Atlassian - Jira Service Management

통합 유형: 수령 및 업데이트

For는 AWS Service Management Connector Security Hub의 결과를 로 Jira 보냅니다Jira. Jira발견한 내용을 기반으로 문제가 생성됩니다. Jira 문제가 업데이트되면 Security Hub에서 해당 조사 결과가 업데이트됩니다.

이 통합은 Jira 서버 및 Jira 데이터 센터만 지원합니다.

통합 및 작동 방식에 대한 개요는 AWS Security Hub - Atlassian Jira Service Management과의 양방향 통합 동영상을 시청하십시오.

제품 링크

파트너 설명서

Atlassian - Jira Service Management Cloud

통합 유형: 수령 및 업데이트

Jira Service Management Cloud은 Jira 서비스 관리의 클라우드 구성 요소입니다.

For는 AWS Service Management Connector Security Hub의 결과를 로 Jira 보냅니다Jira. 이 조사 결과로 인해 Jira Service Management Cloud에서 문제가 발생합니다. Jira Service Management Cloud에서 이러한 문제를 업데이트하면 Security Hub에도 해당 조사 결과가 업데이트됩니다.

제품 링크

파트너 설명서

Atlassian – Opsgenie

통합 유형: 수령

Opsgenie는 상시 작동 서비스를 작동하는 데 필요한 최신 인시던트 관리 솔루션으로, 개발 운영 팀이 서비스 중단에 대비하고 인시던트 발생 중 제어 유지할 수 있도록 합니다.

Security Hub와 통합하면 미션 크리티컬한 보안 관련 인시던트를 즉시 해결할 수 있도록 해당 팀으로 전달합니다.

제품 링크

파트너 설명서

Fortinet – FortiCNP

통합 유형: 수령

FortiCNP은 보안 조사 결과를 실행 가능한 인사이트로 집계하고 위험 점수를 기반으로 보안 인사이트의 우선 순위를 지정하여 알림으로 인한 피로를 줄이고 문제 해결을 가속화하는 클라우드 네이티브 보호 제품입니다.

AWS 마켓플레이스 링크

파트너 설명서

IBM – QRadar

통합 유형: 수령

IBM QRadar SIEM은 보안 팀이 위협을 신속하고 정확하게 감지하여 우선 순위를 정하고 조사하여 대응할 수 있는 기능을 제공합니다.

제품 링크

파트너 설명서

Logz.io Cloud SIEM

통합 유형: 수령

Logz.io은 보안 팀이 보안 위협을 실시간으로 탐지, 분석 및 대응할 수 있도록 로그 및 이벤트 데이터의 고급 상관 관계를 제공하는 Cloud SIEM의 공급자입니다.

제품 링크

파트너 설명서

MetricStream – CyberGRC

통합 유형: 수령

MetricStream CyberGRC은 사이버 보안 위험을 관리, 측정 및 완화하는 데 도움이 됩니다. Security Hub 조사 결과 수령하면 CyberGRC은 이러한 위험에 대한 더 많은 가시성을 제공하므로 사이버 보안 투자의 우선 순위를 정하고 IT 정책을 준수할 수 있습니다.

AWS 마켓플레이스 링크

제품 링크

MicroFocus – MicroFocus Arcsight

통합 유형: 수령

ArcSight은 이벤트 상관 관계 및 감독/비감독 분석을 대응 자동화 및 오케스트레이션과 통합하여 효과적인 위협 탐지 및 대응을 실시간으로 가속화합니다.

제품 링크

파트너 설명서

New Relic Vulnerability Management

통합 유형: 수령

New Relic Vulnerability Management은 Security Hub로부터 보안 조사 결과를 수령하므로 스택 전체의 상황에 따른 성능 원격 측정과 함께 보안에 대한 중앙 집중식 보기를 얻을 수 있습니다.

AWS 마켓플레이스 링크

파트너 설명서

PagerDuty – PagerDuty

통합 유형: 수령

PagerDuty 디지털 작업 관리 플랫폼은 모든 신호를 적절한 통찰력과 조치로 자동 변환하므로 고객에게 영향을 미치는 문제를 사전에 완화할 수 있는 역량을 조직에 부여합니다.

AWS 사용자는 AWS 통합 PagerDuty 세트를 사용하여 자신 있게 AWS 자신과 하이브리드 환경을 확장할 수 있습니다.

체계적으로 집계된 Security Hub의 보안 경고와 통합될 경우, PagerDuty은 팀이 위협 대응 프로세스를 자동화하고 잠재적인 문제를 방지할 사용자 지정 작업을 빠르게 설정하도록 합니다.

클라우드 마이그레이션 프로젝트를 수행하는 PagerDuty 사용자는 마이그레이션 수명 주기 내내 발생하는 문제의 영향을 줄이면서 신속하게 이동할 수 있습니다.

제품 링크

파트너 설명서

Palo Alto Networks – Cortex XSOAR

통합 유형: 수령

Cortex XSOAR는 전체 보안 제품 스택과 통합하여 인시던트 응답 및 보안 작업을 가속화하는 보안 오케스트레이션, 자동화 및 응답(SOAR) 플랫폼입니다.

제품 링크

파트너 설명서

Palo Alto Networks – VM-Series

통합 유형: 수령

Security Hub와의 Palo Alto VM-Series 통합은 위협 인텔리전스를 수집하여 악의적인 IP 주소 활동을 차단하는 자동 보안 정책 업데이트로 VM-Series 차세대 방화벽에 전송합니다.

제품 링크

파트너 설명서

Rackspace Technology – Cloud Native Security

통합 유형: 수령

Rackspace Technology 은 Rackspace SOC, 고급 분석 및 위협 해결을 통한 연중무휴 모니터링을 위해 네이티브 AWS 보안 제품에 더해 관리형 보안 서비스를 제공합니다.

제품 링크

Rapid7 – InsightConnect

통합 유형: 수령

Rapid7 InsightConnect는 코드를 거의 사용하지 않고 SOC 작업을 최적화할 수 있는 보안 오케스트레이션 및 자동화 솔루션입니다.

제품 링크

파트너 설명서

RSA – RSA Archer

통합 유형: 수령

RSA Archer IT 및 보안 위험 관리를 통해 비즈니스에 중요한 자산을 파악하고, 보안 정책 및 표준을 수립 및 전달하고, 공격을 탐지 및 대응하고, 보안 결함을 식별 및 해결하고, 명확한 IT 위험 관리 모범 사례를 수립할 수 있습니다.

제품 링크

파트너 설명서

ServiceNow – ITSM

통합 유형: 수령 및 업데이트

ServiceNow와 Security Hub의 통합을 통해 ServiceNow ITSM 안에서 Security Hub의 조사 결과를 볼 수 있습니다. Security Hub에서 조사 결과를 수령할 때 인시던트 또는 문제를 자동으로 생성하도록 ServiceNow을 구성할 수도 있습니다.

이러한 인시던트 및 문제가 업데이트되면 Security Hub의 조사 결과도 업데이트됩니다.

통합 및 작동 방식에 대한 개요는 AWS Security Hub - ServiceNow ITSM과의 양방향 통합 동영상을 시청하십시오.

제품 링크

파트너 설명서

Slack – Slack

통합 유형: 수령

Slack은 사람, 데이터 및 애플리케이션을 하나로 통합하는 비즈니스 기술 스택 계층입니다. 효율적으로 협업하고, 중요한 정보를 검색하고, 수십만 개의 중요한 애플리케이션 및 서비스에 액세스하여 최상의 작업을 수행할 수 있는 단일 공간입니다.

제품 링크

파트너 설명서

Splunk – Splunk Enterprise

통합 유형: 수령

Splunk는 Amazon CloudWatch Events를 Security Hub 조사 결과의 소비자로 사용합니다. 고급 보안 분석 및 SIEM을 위해 Splunk에 데이터를 보냅니다.

제품 링크

파트너 설명서

Splunk – Splunk Phantom

통합 유형: 수령

AWS Security Hub Splunk Phantom 애플리케이션을 사용하면 추가 위협 인텔리전스 정보가 포함된 자동화된 컨텍스트 강화 또는 자동 대응 조치를 수행하기 위해 탐지 결과가 전송됩니다. Phantom

제품 링크

파트너 설명서

ThreatModeler

통합 유형: 수령

ThreatModeler은 엔터프라이즈 소프트웨어 및 클라우드 개발 수명 주기를 보호하고 규모를 조정하는 자동화된 위협 모델링 솔루션입니다.

제품 링크

파트너 설명서

Trellix – Trellix Helix

통합 유형: 수령

Trellix Helix는 조직이 알림에서 수정까지 모든 인시던트를 제어할 수 있도록 지원하는 클라우드 호스팅 보안 운영 플랫폼입니다.

제품 링크

파트너 설명서

Security Hub로 조사 결과를 보내고 Security Hub에서 조사 결과를 수령하는 타사 통합

다음 타사 파트너 제품 통합은 Security Hub에 조사 결과를 보내고 Security Hub에서 조사 결과를 수령합니다.

Caveonix – Caveonix Cloud

통합 유형: 전송 및 수령

제품 ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Caveonix AI 기반 플랫폼은 클라우드 네이티브 서비스, VM 및 컨테이너를 다루면서 하이브리드 클라우드의 가시성, 평가 및 완화를 자동화합니다. AWS Security Hub와 통합되어 AWS 데이터와 고급 분석을 통합하여 보안 경고 및 규정 준수에 대한 통찰력을 제공합니다. Caveonix

AWS 마켓플레이스 링크

파트너 설명서

Cloud Custodian – Cloud Custodian

통합 유형: 전송 및 수령

제품 ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian을 사용하면 클라우드에서 사용자를 잘 관리할 수 있습니다. 간단한 YAML DSL을 통해 쉽게 정의된 규칙이 안전하고 최적화된 비용으로 관리성이 뛰어난 클라우드 인프라를 사용할 수 있도록 합니다.

제품 링크

파트너 설명서

DisruptOps, Inc. – DisruptOPS

통합 유형: 전송 및 수령

제품 ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

DisruptOps 보안 작업 플랫폼은 조직이 자동화된 가드레일을 사용하여 클라우드에서 보안 모범 사례를 유지할 수 있도록 도와줍니다.

제품 링크

파트너 설명서

Kion

통합 유형: 전송 및 수령

제품 ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(이전 명칭은 cloudtamer.io) 는 를 위한 완벽한 클라우드 거버넌스 솔루션입니다. AWSKion이해관계자에게 클라우드 운영에 대한 가시성을 제공하고 클라우드 사용자가 계정을 관리하고, 예산 및 비용을 관리하고, 지속적인 규정 준수를 보장할 수 있도록 지원합니다.

제품 링크

파트너 설명서

Turbot – Turbot

통합 유형: 전송 및 수령

제품 ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot은 클라우드 인프라가 안전하고, 규정을 준수하며, 확장 가능하고, 비용에 최적화된 상태를 유지하도록 보장합니다.

제품 링크

파트너 설명서

사용자 지정 제품 통합을 사용하여 AWS Security Hub에 결과 전송

Security Hub는 통합 AWS 서비스 및 타사 제품에서 생성된 결과 외에도 다른 사용자 지정 보안 제품에서 생성된 결과를 사용할 수 있습니다.

`BatchImportFindings`API 작업을 사용하여 이러한 결과를 Security Hub에 수동으로 보낼 수 있습니다.

사용자 지정 통합을 설정할 때는 Security Hub 파트너 통합 가이드에 제공된 지침과 체크리스트를 사용하십시오.

사용자 지정 보안 제품에서 조사 결과를 전송하기 위한 요구 사항 및 권장 사항

`BatchImportFindings` API 작업을 성공적으로 간접 호출하려면 Security Hub를 활성화해야 합니다.

the section called "결과 형식"를 사용하여 결과 세부 정보를 제공해야 합니다. 사용자 지정 통합의 조사 결과를 보려면 다음 요구 사항 및 권장 사항을 사용하십시오.

제품 ARN 설정

Security Hub를 활성화하면 현재 계정에 Security Hub의 기본 제품 Amazon 리소스 이름(ARN)이 생성됩니다.

이 제품 ARN의 형식은 `arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`입니다. 예를 들어 `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`입니다.

`BatchImportFindings` API 작업을 간접적으로 호출할 때 이 제품 ARN을 `ProductArn` 속성 값으로 사용하십시오.

회사 및 제품 이름 정의

조사 결과를 Security Hub로 보내는 사용자 지정 통합에 사용할 선호하는 회사 이름 및 제품 이름을 설정하는 데 `BatchImportFindings`을 사용할 수 있습니다.

지정된 이름은 각각 개인 이름 및 기본 이름이라고 하는 사전 구성된 회사 이름 및 제품 이름을 대체하며 Security Hub 콘솔 및 각 조사 결과의 JSON에 표시됩니다. 조사 결과 생성 및 업데이트에 BatchImportFindings 사용 섹션을 참조하십시오.

결과 ID 설정

`Id` 속성을 사용하여 자체 결과 ID를 공급하고, 관리하고, 증분해야 합니다.

각각의 새 검색 결과에는 고유한 검색 ID가 있어야 합니다. 사용자 지정 제품이 동일한 검색 결과 ID로 여러 검색 결과를 보내는 경우 Security Hub는 첫 번째 검색 결과만 처리합니다.

계정 ID 설정

`AwsAccountId` 속성을 사용하여 자체 계정 ID를 지정해야 합니다.

생성 날짜 및 업데이트 날짜 설정

`CreatedAt` 및 `UpdatedAt` 속성에 자체 타임스탬프를 제공해야 합니다.

사용자 지정 제품의 조사 결과 업데이트

사용자 지정 제품에서 새 조사 결과를 전송할 뿐만 아니라 `BatchImportFindings` API 작업을 사용하여 사용자 지정 제품에서 기존 조사 결과를 업데이트할 수도 있습니다.

기존 조사 결과를 업데이트하려면 `Id` 속성을 통해 기존 조사 결과 ID를 사용합니다. 수정된 `UpdatedAt` 타임스탬프를 포함하여 요청에서 업데이트된 적절한 정보로 전체 결과를 다시 보냅니다.

사용자 지정 통합 예제

다음 예제 사용자 지정 제품 통합을 지침으로 사용하여 고유한 사용자 지정 솔루션을 생성할 수 있습니다.

조사 결과를 Chef InSpec 스캔에서 Security Hub로 전송

Chef InSpec규정 준수 검사를 실행하는 AWS CloudFormation 템플릿을 만든 다음 검색 결과를 Security Hub로 보낼 수 있습니다.

자세한 내용은 Chef InSpec 및 AWS Security Hub를 사용한 지속적인 규정 준수 모니터링을 참조하십시오.

Trivy에서 탐지한 컨테이너 취약성을 Security Hub로 전송

컨테이너의 취약성을 검사하는 AquaSecurity Trivy 데 사용하는 AWS CloudFormation 템플릿을 만든 다음 해당 취약성 결과를 Security Hub로 보낼 수 있습니다.

자세한 내용은 Security TrivyAWS Hub를 사용하여 컨테이너 취약성 검사를 위한 CI/CD 파이프라인을 구축하는 방법을 참조하십시오.

Security Hub의 AWS 보안 제어 및 표준

AWS Security Hub는 지원되는 다양한 제품 및 타사 제품의 보안 결과를 사용, 집계 AWS 및 분석합니다.

Security Hub는 또한 규칙에 대해 자동화되고 지속적인 보안 검사를 실행하여 자체 조사 결과를 생성합니다. 규칙은 보안 제어로 표시됩니다. 제어는 차례로 하나 이상의 보안 표준에 따라 활성화될 수 있습니다. 제어를 통해 표준의 요구 사항이 충족되고 있는지 확인할 수 있습니다.

제어 항목에 대한 보안 검사를 통해 보안 상태를 모니터링하고 주의가 필요한 특정 리소스 AWS 계정 또는 리소스를 식별하는 데 사용할 수 있는 결과가 생성됩니다. 각 컨트롤은 AWS 서비스 및 리소스와 관련이 있습니다. 예를 들어, CloudTrail.4 컨트롤에 대한 보안 검사는 로그에 로그 파일 검증을 구성했는지 여부를 결정합니다. AWS CloudTrail 제어에 대한 자세한 내용은 보안 제어 보기 및 관리을 참조하십시오.

하나 이상의 활성화된 Security Hub 표준에서 제어를 활성화할 수 있습니다. 표준을 활성화하면 Security Hub는 표준에 적용되는 제어를 자동으로 활성화합니다. 보안 표준을 사용하면 특정 규정 준수 프레임워크에 집중할 수 있습니다. Security Hub는 각 표준에 적용되는 제어를 정의합니다. 보안 표준에 대한 자세한 정보는 보안 표준 보기 및 관리을 참조하십시오.

보안 검사 결과에 따라 Security Hub는 전체 보안 점수와 표준별 보안 점수를 계산합니다. 이 점수는 보안 상태를 이해하는 데 도움이 됩니다. 점수에 대한 자세한 내용은 보안 점수 계산 방법을 참조하십시오.

보안 검사의 Security Hub 요금에 대한 자세한 내용은 Security Hub 요금을 참조하십시오.

주제

- 표준 및 제어를 구성하기 위한 IAM 권한
- Security Hub의 보안 검사 및 보안 점수
- Security Hub 표준 참조
- 보안 표준 보기 및 관리
- Security Hub 제어 참조
- 보안 제어 보기 및 관리

표준 및 제어를 구성하기 위한 IAM 권한

보안 제어에 대한 정보를 확인하고 표준에서 보안 제어를 활성화 및 비활성화하려면 액세스에 사용하는 AWS Identity and Access Management (IAM) 역할에 다음 API 작업을 호출할 수 있는 권한이 AWS Security Hub 필요합니다. 이러한 작업에 대한 권한을 추가하지 않으면 이러한 API를 호출할 수 없습니다. 필요한 권한을 얻으려면 Security Hub 관리형 정책을 사용할 수 있습니다. 또는 이러한 작업에 대한 권한을 포함하도록 사용자 지정 IAM 정책을 업데이트할 수 있습니다. 사용자 지정 정책에는 `DescribeStandardsControls` 및 `UpdateStandardsControl` API에 대한 권한도 포함되어야 합니다.

- **`BatchGetSecurityControls`**— 현재 계정 및 AWS 리전에 대한 보안 제어 일괄 처리에 대한 정보를 반환합니다.
- **`ListSecurityControlDefinitions`** - 지정된 표준에 적용되는 보안 제어에 대한 정보를 반환합니다.
- **`ListStandardsControlAssociations`** - 계정에서 활성화된 각 표준에서 보안 제어가 현재 활성화되어 있는지 또는 비활성화되어 있는지 식별합니다.
- **`BatchGetStandardsControlAssociations`** - 보안 제어 배치의 경우 각 제어가 현재 지정된 표준에서 활성화되었는지 또는 비활성화되었는지 식별합니다.
- **`BatchUpdateStandardsControlAssociations`** - 제어를 포함하는 표준에서 보안 제어를 활성화하거나 표준에서 제어를 비활성화하는 데 사용됩니다. 이는 관리자가 구성원 계정에서 제어를 활성화하거나 비활성화하는 것을 허용하지 않으려는 경우 기존 `UpdateStandardsControl` API를 일괄적으로 대체할 수 있습니다.

위의 API 외에도 IAM 역할에 **`BatchGetControlEvaluations`**을 호출할 권한을 추가해야 합니다. 이 권한은 Security Hub 콘솔에서 제어 활성화 및 규정 준수 상태, 제어에 대한 조사 결과 수, 제어에 대한 전체 보안 점수를 보는 데 필요합니다. 콘솔 **`BatchGetControlEvaluations`**호출만 가능하므로 이 IAM 권한은 공개적으로 문서화된 Security Hub API 또는 명령에 직접 대응하지 않습니다. AWS CLI

제어 및 표준과 관련된 API에 대한 자세한 내용은 AWS Security Hub API 참조를 참조하십시오.

Security Hub의 보안 검사 및 보안 점수

활성화한 각 컨트롤에 대해 보안 검사를 AWS Security Hub 실행합니다. 보안 검사는 AWS 리소스가 컨트롤에 포함된 규칙을 준수하는지 여부를 결정합니다.

일부 검사는 주기적 일정에 따라 실행됩니다. 리소스 상태가 변경될 때만 실행되는 검사도 있습니다. 자세한 정보는 the section called “보안 검사 실행 예약”을 참조하세요.

많은 보안 검사는 AWS Config 관리형 규칙 또는 사용자 지정 규칙을 사용하여 규정 준수 요구 사항을 설정합니다. 이러한 검사를 실행하려면 를 설정해야 합니다 AWS Config. 자세한 정보는 the section called “AWS Config 규칙 및 보안 검사”을 참조하세요. 다른 경우 Security Hub에서 관리하고 고객에게 표시되지 않는 사용자 지정 Lambda 함수를 사용합니다.

Security Hub는 보안 검사를 실행할 때 조사 결과를 생성하고 규정 준수 상태를 할당합니다. 규정 준수 상태에 대한 자세한 내용은 조사 결과의 규정 준수 상태 값을 참조하십시오.

Security Hub는 제어 조사 결과의 규정 준수 상태를 사용하여 전체 제어 상태를 결정합니다. 또한 Security Hub는 활성화된 모든 제어와 특정 표준에 대한 보안 점수를 계산합니다. 자세한 내용은 the section called “규정 준수 상태 및 제어 상태” 및 the section called “보안 점수 결정”을 참조하십시오.

통합 제어 조사 결과를 활성화한 경우 Security Hub는 제어가 둘 이상의 표준과 연결된 경우에도 단일 조사 결과를 생성합니다. 자세한 정보는 통합 제어 조사 결과을 참조하세요.

주제

- Security Hub에서 AWS Config 규칙을 사용하여 보안 검사를 실행하는 방법
- AWS Config 제어 결과를 생성하는 데 필요한 리소스
- 보안 검사 실행 예약
- 제어 조사 결과 생성 및 업데이트
- 규정 준수 상태 및 제어 상태
- 보안 점수 결정

Security Hub에서 AWS Config 규칙을 사용하여 보안 검사를 실행하는 방법

환경 리소스에 대한 보안 검사를 실행하려면 표준에서 지정한 단계를 AWS Security Hub 사용하거나 특정 AWS Config 규칙을 사용합니다. 일부 규칙은 AWS Config에서 관리하는 관리형 규칙입니다. 다른 규칙은 Security Hub에서 개발하는 사용자 지정 규칙입니다.

AWS Config Security Hub에서 제어에 사용하는 규칙은 Security Hub 서비스에 의해 활성화되고 제어되므로 서비스 연결 규칙이라고 합니다.

이러한 AWS Config 규칙에 대한 검사를 활성화하려면 먼저 계정을 활성화하고 필수 리소스에 AWS Config 대한 리소스 기록을 활성화해야 합니다. 활성화하는 방법에 대한 자세한 내용은 AWS Config을 참조하십시오구성 AWS Config. 필수 리소스 기록에 대한 자세한 내용은 AWS Config 제어 결과를 생성하는 데 필요한 리소스을 참조하십시오.

Security Hub에서 서비스 연결 규칙을 생성하는 방법

Security Hub는 AWS Config 서비스 연결 규칙을 사용하는 모든 컨트롤에 대해 사용자 환경에 필요한 규칙의 인스턴스를 AWS 만듭니다.

이러한 서비스 연결 규칙은 Security Hub에 특정합니다. 동일한 규칙의 다른 인스턴스가 이미 존재하는 경우에도 이러한 서비스 연결 규칙이 생성됩니다. 서비스 연결 규칙은 원래 규칙 이름 앞에 `securityhub`를 추가하고 규칙 이름 뒤에 고유 식별자를 추가합니다. 예를 들어 원래 AWS Config 관리형 규칙의 `vpc-flow-logs-enabled` 경우 서비스 연결 규칙 이름은 다음과 같습니다. `securityhub-vpc-flow-logs-enabled-12345`

제어를 평가하는 데 사용할 수 있는 AWS Config 규칙의 수에는 제한이 있습니다. Security Hub에서 생성하는 사용자 지정 AWS Config 규칙은 이 한도에 포함되지 않습니다. 계정의 관리형 규칙 AWS Config 한도에 이미 도달했더라도 보안 표준을 활성화할 수 있습니다. AWS Config 규칙 제한에 대해 자세히 알아보려면 AWS Config 개발자 안내서의 서비스 제한을 참조하십시오.

제어의 AWS Config 규칙에 대한 세부 정보 보기

AWS Config 관리형 규칙을 사용하는 컨트롤의 경우 컨트롤 설명에 AWS Config 규칙 세부 정보로 연결되는 링크가 포함되어 있습니다. 사용자 지정 규칙은 제어 설명과 연결되지 않습니다. 제어 설명은 Security Hub 제어 참조을 참조하십시오. 목록에서 제어를 선택하면 해당 설명을 볼 수 있습니다.

이러한 컨트롤에서 생성된 결과의 경우 검색 결과 세부 정보에는 관련 AWS Config 규칙으로 연결되는 링크가 포함됩니다. 검색 세부 정보에서 AWS Config 규칙으로 이동하려면 탐색할 수 있는 선택한 계정의 IAM 권한도 있어야 한다는 점에 유의하십시오. AWS Config

조사 결과 페이지, 인사이트 페이지 및 통합 페이지의 조사 결과 세부 정보에는 AWS Config 규칙 세부 정보로 연결되는 규칙 링크가 포함되어 있습니다. 검색 결과 세부 정보 검토을 참조하십시오.

제어 세부 정보 페이지의 결과 목록의 Investive 열에는 AWS Config 규칙 세부 정보로 연결되는 링크가 있습니다. 검색 리소스의 AWS Config 규칙 보기 섹션을 참조하십시오.

AWS Config 제어 결과를 생성하는 데 필요한 리소스

AWS Security Hub Security Hub 컨트롤에 대한 보안 검사를 수행하여 제어 결과를 생성합니다. 일부 컨트롤은 특정 리소스의 규정 준수를 평가하는 AWS Config 규칙을 사용합니다. Security Hub에서 변경 트리거 일정 유형을 갖는 제어에 대한 조사 결과를 생성하려면 AWS Config에서 필요한 리소스에 대한 기록을 켜야 합니다. 주기적 일정 유형이 있는 대부분의 제어에 대해서는 리소스를 기록할 필요가 없습니다. 하지만 일부 주기적 제어의 경우 규정 준수 변경 사항을 감지하려면 리소스 기록이 필요합니다.

이 페이지는 표준별 필수 리소스 목록과 표준별로 구분된 필수 리소스 목록을 제공합니다. 첫 번째 테이블에는 각 리소스를 사용하는 Security Hub 제어도 나열되어 있습니다.

규칙을 기반으로 하는 보안 검사를 통해 검색 결과를 생성하는 경우 검색 결과 세부 정보에는 관련 AWS Config 규칙으로 연결되는 규칙 링크가 포함됩니다. AWS Config AWS Config 규칙으로 이동하려면 계정에 AWS Config 규칙을 볼 수 있는 AWS Identity and Access Management (IAM) 권한이 있어야 합니다.

> **Note**
>
> 컨트롤을 사용할 수 없는 경우 해당 리소스는 에서 AWS Config사용할 수 없습니다. AWS 리전 Security Hub 제어에 대한 리전별 제한 목록은 리전별 제어 기능 사용 가능 여부을 참조하십시오.

AWS Config 모든 컨트롤에 필요한 리소스

Security Hub에서 AWS Config 규칙을 사용하는 활성화된 Security Hub 변경 트리거 컨트롤에 대한 결과를 생성하려면 이러한 리소스를 에 기록해야 합니다 AWS Config. 또한 이 테이블에는 특정 리소스가 필요한 제어도 나와 있습니다. 제어에는 리소스가 두 개 이상 필요할 수 있습니다.

Service	필수 리소스	관련 제어
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2. AppSync4.

Service	필수 리소스	관련 제어
		AppSync5.
AWS Backup (AWS Backup)	`AWS::Backup::BackupPlan`	백업.5
	`AWS::Backup::BackupVault`	백업.3
	`AWS::Backup::RecoveryPoint`	Backup.1 백업.2
	`AWS::Backup::ReportPlan`	백업.4
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 에이씨.3
Amazon Athena	`AWS::Athena::DataCatalog`	아테나.2
	`AWS::Athena::WorkGroup`	아테나.3
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation2.

Service	필수 리소스	관련 제어
아마존 CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1. CloudFront3. CloudFront4. CloudFront5. CloudFront6. CloudFront.7 CloudFront.8. CloudFront9. CloudFront1.0 CloudFront1.3 CloudFront1.4
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail9.
아마존 CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch1.5 CloudWatch.17
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1.
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1. CodeBuild2. CodeBuild3. CodeBuild4.

Service	필수 리소스	관련 제어
Amazon Detective	`AWS::Detective::Graph`	형사.1
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`	DMS.2

	`AWS::DMS::Endpoint`	`DMS.9`
		`DMS.10`
		`DMS.11`
		`DMS.12`

	`AWS::DMS::EventSubscription`	DMS.3
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 다이나모드 B.5 DynamoDB.6

Service	필수 리소스	관련 제어
Amazon Elastic Compute Cloud(EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::CustomerGateway`	EC2.36
	`AWS::EC2::EIP`	EC2.12 EC2.37
	`AWS::EC2::FlowLog`	EC2.48
	`AWS::EC2::Instance`	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	`AWS::EC2::InternetGateway`	EC2.39
	`AWS::EC2::LaunchTemplate`	EC2.25

Service	필수 리소스	관련 제어
	AWS::EC2::NatGateway	EC2.40
	AWS::EC2::NetworkAcl	EC2.16 EC2.21 EC2.41
	AWS::EC2::NetworkInterface	EC2.22 EC2.35
	AWS::EC2::RouteTable	EC2.42
	AWS::EC2::SecurityGroup	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	AWS::EC2::Subnet	EC2.15 EC2.44 ElastiCache7.
	AWS::EC2::TransitGateway	EC2.23 EC2.52

Service	필수 리소스	관련 제어
	AWS::EC2::TransitGatewayAttachment	EC2.33
	AWS::EC2::TransitGatewayRouteTable	EC2.34
	AWS::EC2::Volume	EC2.3 EC2.45
	AWS::EC2::VPC	EC2.6 EC2.46
	AWS::EC2::VPCEndpointService	EC2.47
	AWS::EC2::VPCPeeringConnection	EC2.49
	AWS::EC2::VPNConnection	EC2.20
	AWS::EC2::VPNGateway	EC2.50

Service	필수 리소스	관련 제어
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling.1. AutoScaling2. AutoScaling6. AutoScaling9. AutoScaling1.0
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling3. Autoscaling.5
Amazon EC2 Systems Manager(SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3

Service	필수 리소스	관련 제어
Amazon Elastic Container Service(Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 엑시.14
	`AWS::ECS::Service`	ECS.2 ECS.10 EC.13
	`AWS::ECS::TaskDefinition`	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 엑시.15
Amazon Elastic File System(Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS.5
Amazon Elastic Kubernetes Service(Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 예: 6 EKS.8
	`AWS::EKS::IdentityProviderConfig`	엑세스 7

Service	필수 리소스	관련 제어
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1. ElasticBeanstalk2. ElasticBeanstalk3.
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16

Service	필수 리소스	관련 제어
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 예. 9
아마존 EventBridge	`AWS::Events::EventBus`	EventBridge2. EventBridge3.
	`AWS::Events::Endpoint`	EventBridge4.
`AWS Global Accelerator`	`AWS::GlobalAccelerator::Accelerator`	GlobalAccelerator.1.
`AWS Glue`	`AWS::Glue::Job`	접착제.1
`Amazon GuardDuty`	`AWS::GuardDuty::Detector`	GuardDuty4.
	`AWS::GuardDuty::Filter`	GuardDuty2.
	`AWS::GuardDuty::IPSet`	GuardDuty3.

Service	필수 리소스	관련 제어
AWS Identity and Access Management (IAM)	`AWS::IAM::Group`	이엠.27 KMS.2
	`AWS::IAM::Policy`	IAM.1 IAM.21 KMS.1
	`AWS::IAM::Role`	아이엠.24 아이엠.27 KMS.2
	`AWS::IAM::User`	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 아이엠.25 아이엠.27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	이엠.23
AWS IoT	`AWS::IoT::Authorizer`	IoT.4

Service	필수 리소스	관련 제어
	`AWS::IoT::Dimension`	IoT.3
	`AWS::IoT::MitigationAction`	IoT.2
	`AWS::IoT::Policy`	IoT.6
	`AWS::IoT::RoleAlias`	IoT.5
	`AWS::IoT::SecurityProfile`	IoT.1
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias`	S3.17
	`AWS::KMS::Key`	KMS.3 S3.17
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 중국어.2
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 람다.6

Service	필수 리소스	관련 제어
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.3 MQ.4 MQ.5 MQ.6
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall1. NetworkFirewall7. NetworkFirewall9.
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall3. NetworkFirewall4. NetworkFirewall5. NetworkFirewall.8.
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall6.

Service	필수 리소스	관련 제어
아마존 OpenSearch 서비스	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 오픈서치.9 Opensearch.10 검색을 여십시오.11

Service	필수 리소스	관련 제어
Amazon Relational Database Service(Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB.1 DocumentDB.2 DocumentDB.4 DocumentDB.5 Neptune.1 Neptune.2 Neptune.4 Neptune.5 Neptune.7 Neptune.8 Neptune.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34 RDS.35

Service	필수 리소스	관련 제어
	`AWS::RDS::DBClusterSnapshot`	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29
	`AWS::RDS::DBInstance`	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.18 RDS.23 RDS.25 RDS.30

Service	필수 리소스	관련 제어
	`AWS::RDS::DBSecurityGroup`	RDS.31
	`AWS::RDS::DBSnapshot`	RDS.1 RDS.4 RDS.32
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
Amazon Redshift	`AWS::Redshift::Cluster`	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.9 Redshift.10 레드시프트.11

Service	필수 리소스	관련 제어
	`AWS::Redshift::ClusterParameterGroup`	Redshift.2
	`AWS::Redshift::ClusterSnapshot`	레드시프트.13
	`AWS::Redshift::ClusterSubnetGroup`	레드시프트.14
	`AWS::Redshift::EventSubscription`	레드시프트.12
Amazon Route 53	`AWS::Route53::HostedZone`	Route53.2
	`AWS::Route53::HealthCheck`	루트 53.1
Amazon Simple Storage Service(S3)	`AWS::S3::AccessPoint`	S3.19
	`AWS::S3::AccountPublicAccessBlock`	S3.2 S3.3

Service	필수 리소스	관련 제어
	`AWS::S3::Bucket`	S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager.1. SecretsManager2. SecretsManager5.
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog.1.

Service	필수 리소스	관련 제어
Amazon Simple Email Service(Amazon SES)	`AWS::SES::ConfigurationSet`	섹스. 2
	`AWS::SES::ContactList`	섹스.1
Amazon Simple Notification Service(Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`	SQS.1 평방.2
아마존 SageMaker	`AWS::SageMaker::NotebookInstance`	SageMaker2. SageMaker3.
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1.
	`AWS::StepFunctions::Activity`	StepFunctions2.
AWS Transfer Family	`AWS::Transfer::Workflow`	전송.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7

Service	필수 리소스	관련 제어
	`AWS::WAF::WebACL`	WAF.1 WAF.8
	`AWS::WAFRegional::Rule`	WAF.2
	`AWS::WAFRegional::RuleGroup`	WAF.3
	`AWS::WAFRegional::WebACL`	WAF.4
	`AWS::WAFv2::RuleGroup`	WAF.12
	`AWS::WAFv2::WebACL`	WAF.10 WAF.11

FSBP 표준에 필요한 리소스

Security Hub가 AWS Config 규칙을 사용하는 AWS 기본 보안 모범 사례 (FSBP) 변경 트리거 제어에 대한 결과를 정확하게 보고하려면 이러한 리소스를 에 기록해야 합니다. AWS Config이 표준에 대한 자세한 내용은 AWS 기본 보안 모범 사례 (FSBP) 표준을 참조하십시오.

Service	필수 리소스
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`

Service	필수 리소스
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
아마존 CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon EC2 Systems Manager(SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Service	필수 리소스

Amazon Elastic Compute Cloud(EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry(Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service(Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System(Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`

Service	필수 리소스
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

아마존 OpenSearch 서비스	`AWS::OpenSearch::Domain`

Service	필수 리소스

Amazon Relational Database Service(Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`

Amazon Simple Storage Service(S3)	`AWS::S3::AccessPoint`
	`AWS::S3::AccountPublicAccessBlock`
	`AWS::S3::Bucket`

Amazon Simple Notification Service(SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`
아마존 SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`

Service	필수 리소스

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

CIS AWS 재단 벤치마크에 필요한 리소스

인터넷 보안 센터 (CIS) AWS 기반 벤치마크에 적용되는 활성화된 컨트롤에 대해 보안 검사를 실행하기 위해 Security Hub는 Amazon Web Services 보안 검사에 규정된 정확한 감사 단계를 수행하거나 특정 AWS Config 관리형 규칙을 사용합니다.

이 표준에 대한 자세한 내용은 CIS AWS 기반 벤치마크을 참조하십시오.

CIS v3.0.0의 필수 리소스

Security Hub가 AWS Config 규칙을 사용하는 활성화된 CIS v3.0.0 변경 트리거 제어에 대한 결과를 정확하게 보고하려면 이러한 리소스를 에 기록해야 합니다. AWS Config

Service	필수 리소스

Amazon Elastic Compute Cloud(Amazon EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::SecurityGroup`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`

Service	필수 리소스

	`AWS::IAM::User`
	
	`AWS::IAM::Role`

Amazon Relational Database Service(Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service(S3)	`AWS::S3::Bucket`

CIS v1.4.0에 필요한 리소스

Security Hub가 AWS Config 규칙을 사용하는 활성화된 CIS v1.4.0 변경 트리거 제어에 대한 결과를 정확하게 보고하려면 이러한 리소스를 에 기록해야 합니다. AWS Config

Service	필수 리소스

Amazon Elastic Compute Cloud(EC2)	`AWS::EC2::NetworkAcl`
	
	`AWS::EC2::SecurityGroup`

AWS Identity and Access Management (IAM)	`AWS::IAM::Policy`
	
	`AWS::IAM::User`

Amazon Relational Database Service(Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service(S3)	`AWS::S3::Bucket`

CIS v1.2.0에 필요한 리소스

Security Hub가 AWS Config 규칙을 사용하는 활성화된 CIS v1.2.0 변경 트리거 제어에 대한 결과를 정확하게 보고하려면 이러한 리소스를 에 기록해야 합니다. AWS Config

Service	필수 리소스
Amazon Elastic Compute Cloud(EC2)	`AWS::EC2::SecurityGroup`

Service	필수 리소스
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`

NIST SP 800-53 개정판 5에 필요한 리소스

Security Hub가 AWS Config 규칙을 사용하는 활성화된 미국 국립 표준 기술 연구소 (NIST) SP 800-53 Rev. 5 변경 유발 제어에 대한 결과를 정확하게 보고하려면 이러한 리소스를 에 기록해야 합니다. AWS Config변경 트리거 스케줄 유형의 변경이 있는 제어의 리소스만 기록하면 됩니다. 이 표준에 대한 자세한 내용은 NIST(국립 표준 기술 연구소) SP 800-53 개정 5을 참조하십시오.

Service	필수 리소스
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
아마존 CloudFront	`AWS::CloudFront::Distribution`
아마존 CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon DynamoDB	`AWS::DynamoDB::Table`

Service	필수 리소스

Amazon Elastic Compute Cloud(EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry(Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service(Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System(Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`

Service	필수 리소스
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
아마존 EventBridge	`AWS::Events::Endpoint` `AWS::Events::EventBus`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`

Service	필수 리소스

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

아마존 OpenSearch 서비스	`AWS::OpenSearch::Domain`

Amazon Relational Database Service(Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`

Amazon Simple Storage Service(S3)	`AWS::S3::AccountPublicAccessBlock`
	`AWS::S3::AccessPoint`
	`AWS::S3::Bucket`

AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service(SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`

Service	필수 리소스

Amazon EC2 Systems Manager(SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

아마존 SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

PCI DSS v3.2.1에 필요한 리소스

Security Hub가 AWS Config 규칙을 사용하는 활성화된 PCI DSS (지불 카드 산업 데이터 보안 표준) 제어에 대한 결과를 정확하게 보고하려면 이러한 리소스를 기록해야 합니다. AWS Config이 표준에 대한 자세한 내용은 Payment Card Industry Data Security Standard(PCI DSS)을 참조하십시오.

Service	필수 리소스
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon Elastic Compute Cloud(EC2)	`AWS::EC2::EIP`

Service	필수 리소스

	`AWS::EC2::Instance`
	
	`AWS::EC2::SecurityGroup`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`

AWS Identity and Access Management (IAM)	`AWS::IAM::Policy`
	
	`AWS::IAM::User`

AWS Lambda	`AWS::Lambda::Function`
아마존 OpenSearch 서비스	`AWS::OpenSearch::Domain`

Amazon Relational Database Service(Amazon RDS)	`AWS::RDS::DBClusterSnapshot`
	
	`AWS::RDS::DBInstance`
	
	`AWS::RDS::DBSnapshot`

Amazon Redshift	`AWS::Redshift::Cluster`

Amazon Simple Storage Service(S3)	`AWS::S3::AccountPublicAccessBlock`
	
	`AWS::S3::Bucket`

Amazon EC2 Systems Manager(SSM)	`AWS::SSM::AssociationCompliance`
	
	`AWS::SSM::ManagedInstanceInventory`
	
	`AWS::SSM::PatchCompliance`

리소스 태깅 AWS 표준에 필요한 리소스

AWS 리소스 태깅 표준의 모든 컨트롤은 변경이 트리거되며 규칙을 사용합니다. AWS Config Security Hub가 이러한 제어에 대한 결과를 정확하게 보고하려면 다음 리소스를 에 기록해야 합니다 AWS

Config. 변경 트리거 스케줄 유형의 변경이 있는 제어의 리소스만 기록하면 됩니다. 이 표준에 대한 자세한 내용은 AWS 리소스 태깅 표준을 참조하십시오.

Service	필수 리소스
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog` `AWS::Athena::WorkGroup`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`

AWS Backup (AWS Backup)	`AWS::Backup::BackupPlan`
	`AWS::Backup::BackupVault`
	`AWS::Backup::RecoveryPlan`
	`AWS::Backup::ReportPlan`

AWS CloudFormation	`AWS::CloudFormation::Stack`
아마존 CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon Detective	`AWS::Detective::Graph`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`
	`AWS::DMS::EventSubscription`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationSubnetGroup`

Amazon DynamoDB	`AWS::DynamoDB::Trail`
Amazon Elastic Compute Cloud(EC2)	`AWS::EC2::CustomerGateway`

Service	필수 리소스
	AWS::EC2::EIP AWS::EC2::FlowLog AWS::EC2::Instance AWS::EC2::InternetGateway AWS::EC2::NatGateway AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::RouteTable AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::TransitGateway AWS::EC2::TransitGatewayAttachment AWS::EC2::TransitGatewayRouteTable AWS::EC2::Volume AWS::EC2::VPC AWS::EC2::VPCEndpointService AWS::EC2::VPCPeeringConnection AWS::EC2::VPNGateway
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup

Service	필수 리소스
Amazon Elastic Container Registry(Amazon ECR)	`AWS::ECR::PublicRepository`

Amazon Elastic Container Service(Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System(Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service(Amazon EKS)	`AWS::EKS::Cluster` `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk (Elastic Beanstalk)	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
아마존 EventBridge	`AWS::Events::EventBus`
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`

아마존 GuardDuty	`AWS::GuardDuty::Detector`
	`AWS::GuardDuty::Filter`
	`AWS::GuardDuty::IPSet`

AWS Identity and Access Management (IAM)	`AWS::IAM::Role` `AWS::IAM::User`
AWS Identity and Access Management Access Analyzer (IAM 액세스 애널라이저)	`AWS::AccessAnalyzer::Analyzer`

Service	필수 리소스

AWS IoT	`AWS::IoT::Authorizer`
	`AWS::IoT::Dimension`
	`AWS::IoT::MitigationAction`
	`AWS::IoT::Policy`
	`AWS::IoT::RoleAlias`
	`AWS::IoT::SecurityProfile`

Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` `AWS::NetworkFirewall::FirewallPolicy`
아마존 OpenSearch 서비스	`AWS::OpenSearch::Domain`

Amazon Relational Database Service	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSecurityGroup`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::DBSubnetGroup`

Service	필수 리소스

Amazon Redshift	`AWS::Redshift::Cluster`
	`AWS::Redshift::ClusterSnapshot`
	`AWS::Redshift::ClusterSubnetGroup`
	`AWS::Redshift::EventSubscription`

Amazon Route 53	`AWS::Route53::HealthCheck`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service(Amazon SES)	`AWS::SES::ConfigurationSet` `AWS::SES::ContactList`
Amazon Simple Notification Service(Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Transfer Family	`AWS::Transfer::Workflow`

서비스 관리형 표준에 필요한 리소스: AWS Control Tower

Security Hub가 활성화된 서비스 관리 표준: AWS Config 규칙을 사용하는 AWS Control Tower 변경 트리거 제어에 대한 결과를 정확하게 보고하려면 다음 리소스를 에 기록해야 합니다. AWS Config이 표준에 대한 자세한 내용은 서비스 관리형 표준: AWS Control Tower을 참조하십시오.

Service	필수 리소스
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`

Service	필수 리소스
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud(EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry(Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service(Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System(Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`

Service	필수 리소스
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` `AWS::NetworkFirewall::RuleGroup`
아마존 OpenSearch 서비스	`AWS::OpenSearch::Domain`

Service	필수 리소스

Amazon Relational Database Service(Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service(S3)	`AWS::S3::AccountPublicAccessBlock` `AWS::S3::Bucket`
Amazon Simple Notification Service(SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service(Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager(SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::WebACL`

보안 검사 실행 예약

보안 표준을 활성화하면 2시간 이내에 모든 검사를 AWS Security Hub 실행하기 시작합니다. 대부분의 검사는 25분 이내에 실행되기 시작합니다. Security Hub는 제어의 기반이 되는 규칙을 평가하여 검사를 실행합니다. 제어가 첫 번째 검사 실행을 완료할 때까지 상태는 데이터 없음입니다.

새 표준을 사용하도록 설정하면 Security Hub에서 다른 사용 가능한 표준에서 사용하도록 설정한 컨트롤과 동일한 기본 AWS Config 서비스 연결 규칙을 사용하는 컨트롤에 대한 검색 결과를 생성하는 데 최대 24시간이 걸릴 수 있습니다. 예를 들어 AWS 기본 보안 모범 사례 (FSBP) 표준에서 Lambda.1을 활성화하면 Security Hub가 서비스 연결 규칙을 생성하고 일반적으로 몇 분 안에 결과를 생성합니다. 이후 PCI DSS(지불 카드 산업 데이터 보안 표준)에서 Lambda.1을 활성화하면 Security Hub는 Lambda.1과 동일한 서비스 연결 규칙을 사용하기 때문에 이 제어에 대한 조사 결과를 생성하는 데 최대 24시간이 걸릴 수 있습니다.

초기 검사 후 각 제어에 대한 일정은 주기적이거나 변경으로 트리거될 수 있습니다.

- 주기적 검사 - 이 검사는 가장 최근 실행 후 12~24시간 이내에 자동으로 실행됩니다. Security Hub는 주기를 결정하며 사용자는 이를 변경할 수 없습니다. 주기적 제어에는 검사가 실행되는 시점의 평가가 반영됩니다. 주기적 제어 결과의 워크플로 상태를 업데이트하고 다음 검사에서 결과의 규정 준수 상태가 동일하게 유지되는 경우 워크플로 상태는 수정된 상태로 유지됩니다. 예를 들어 KMS.4 검색에 실패한 경우 - AWS KMS key 순환을 활성화한 다음 결과를 수정해야 하는 경우 Security Hub는 워크플로우 상태를 에서 로 변경합니다. `NEW` `RESOLVED` 다음 정기 검사 전에 KMS 키 교체를 비활성화해도 검색 결과의 워크플로 상태는 `RESOLVED`로 유지됩니다.
- 변경 트리거 검사 — 이러한 검사는 관련 리소스의 상태가 변경될 때 실행됩니다. AWS Config 리소스 상태의 변경 사항을 지속적으로 기록하는 것과 매일 기록하는 것 중에서 선택할 수 있습니다. 일별 기록을 선택하면 리소스 상태가 변경될 경우 각 24시간 기간이 끝날 때 리소스 구성 데이터를 AWS Config 제공합니다. 변경 사항이 없는 경우에는 데이터가 제공되지 않습니다. 이로 인해 24시간이 완료될 때까지 Security Hub 결과 생성이 지연될 수 있습니다. 선택한 녹화 기간에 관계없이 Security Hub는 18시간마다 리소스 업데이트를 확인하여 AWS Config 누락된 리소스 업데이트가 없는지 확인합니다.

일반적으로 Security Hub는 가능한 경우 항상 변경으로 트리거되는 규칙을 사용합니다. 리소스가 변경 트리거 규칙을 사용하려면 AWS Config 구성 항목을 지원해야 합니다.

관리형 AWS Config 규칙을 기반으로 하는 컨트롤의 경우 컨트롤 설명에는 AWS Config 개발자 안내서의 규칙 설명 링크가 포함됩니다. 이 설명에는 규칙이 변경으로 트리거되는지 또는 주기적인지 여부가 포함됩니다.

Security Hub 사용자 지정 Lambda 함수를 사용하는 점검은 주기적입니다.

제어 조사 결과 생성 및 업데이트

AWS Security Hub 보안 제어에 대한 검사를 실행하여 결과를 생성합니다. 이러한 검색 결과는 AWS 보안 검색 결과 형식 (ASFF) 을 사용합니다. 단, 검색 결과 크기가 최대 240KB를 초과하면 `Resource.Details` 객체가 제거됩니다. AWS Config 리소스가 뒷받침되는 컨트롤의 경우 AWS Config 콘솔에서 리소스 세부 정보를 볼 수 있습니다.

Security Hub는 일반적으로 제어에 대한 각 보안 검사에 대해 요금을 부과합니다. 그러나 여러 컨트롤에서 동일한 AWS Config 규칙을 사용하는 경우 Security Hub는 AWS Config 규칙을 검사할 때마다 요금을 한 번만 청구합니다. 통합 제어 조사 결과를 켜면 Security Hub는 제어가 여러 사용 표준에 포함되어 있더라도 보안 검사를 위한 단일 조사 결과를 생성합니다.

예를 들어, `iam-password-policy` 이 AWS Config 규칙은 CIS (인터넷 보안 센터) AWS 기반 벤치마크 표준 및 기본 보안 모범 사례 표준의 여러 제어 항목에서 사용됩니다. Security Hub에서 해당 AWS Config 규칙에 대해 검사를 실행할 때마다 관련 컨트롤 각각에 대해 별도의 검색 결과가 생성되지만 검사 요금은 한 번만 청구됩니다.

통합 제어 조사 결과

계정에서 통합 제어 조사 결과를 켜면 Security Hub는 제어가 활성화된 여러 표준에 적용되는 경우에도 제어의 각 보안 검사에 대해 하나의 새로운 조사 결과 또는 조사 결과 업데이트를 생성합니다. 제어 목록과 해당 제어가 적용되는 표준을 보려면 Security Hub 제어 참조을 참조하십시오. 통합 제어 조사 결과를 켜거나 끌 수 있습니다. 결과의 노이즈를 줄이려면 이 기능을 켜는 것이 좋습니다.

2023년 2월 23일 AWS 계정 이전에 Security Hub를 활성화한 경우 이 섹션 뒷부분의 지침에 따라 통합 제어 탐지 결과를 활성화해야 합니다. 2023년 2월 23일 또는 그 이후에 Security Hub를 활성화하면 계정에서 통합 제어 탐지 조사 결과가 자동으로 켜집니다. 하지만 AWS Organizations과의 Security Hub 통합을 사용하거나 수동 초대 과정을 통해 초대된 회원 계정을 사용하는 경우에는 관리자 계정에서 활성화된 경우에만 회원 계정에서 통합 제어 조사 결과가 활성화됩니다. 관리자 계정에서 이 기능을 끄면 멤버 계정에서도 해당 기능이 꺼집니다. 이 동작은 신규 및 기존 구성원 계정에 적용됩니다.

계정에서 통합 제어 조사 결과를 끄면 Security Hub는 제어를 포함하는 활성화된 각 표준에 대해 보안 검사별로 별도의 조사 결과를 생성합니다. 예를 들어, 네 개의 사용 표준이 동일한 기본 AWS Config 규칙을 가진 컨트롤을 공유하는 경우 컨트롤에 대한 보안 검사 후 네 개의 개별 결과를 받게 됩니다. 통합 제어 조사 결과를 켜면 조사 결과가 하나만 수신됩니다. 통합이 조사 결과에 미치는 영향에 대한 자세한 내용은 샘플 제어 조사 결과을 참조하십시오.

통합 제어 조사 결과를 켜면 Security Hub는 표준에 구애받지 않는 새로운 조사 결과를 생성하고 원래 표준 기반 조사 결과를 보관합니다. 일부 제어 결과 필드 및 값이 변경되어 기존 워크플로에 영향을 미칠 수 있습니다. 이러한 변경에 대한 내용은 통합 제어 조사 결과 - ASFF 변경 섹션을 참조하세요.

통합 제어 조사 결과를 켜면 타사 통합이 Security Hub에서 수신하는 조사 결과에도 영향을 미칠 수 있습니다. AWS v2.0.0의 자동 보안 대응은 통합 제어 결과를 지원합니다.

통합 제어 조사 결과 활성화

통합 제어 조사 결과를 활성화하려면 관리자 계정 또는 독립형 계정으로 로그인해야 합니다.

> **Note**
>
> 통합 제어 조사 결과를 활성화한 후 Security Hub가 새로운 통합 조사 결과를 생성하고 원본 표준 기반 조사 결과를 보관하는 데 최대 24시간이 걸릴 수 있습니다. 이 기간 동안 계정에서 표준에 구애받지 않는 조사 결과와 표준 기반 조사 결과가 혼합되어 표시될 수 있습니다.

Security Hub console

1. https://console.aws.amazon.com/securityhub/ 에서 콘솔을 엽니다. AWS Security Hub
2. 탐색 창에서 설정을 선택합니다.
3. 일반 탭을 선택합니다.
4. 제어의 경우 통합 제어 조사 결과를 켜십시오.
5. 저장을 선택합니다.

Security Hub API

1. `UpdateSecurityHubConfiguration`를 실행합니다.
2. `ControlFindingGenerator`를 `SECURITY_CONTROL`와 같도록 설정합니다.

   요청 예:

```
{
   "ControlFindingGenerator": "SECURITY_CONTROL"
}
```

AWS CLI

1. update-security-hub-configuration 명령을 실행합니다.
2. control-finding-generator를 SECURITY_CONTROL와 같도록 설정합니다.

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

통합 제어 조사 결과 끄기

통합 제어 조사 결과를 끄려면 관리자 계정 또는 독립형 계정으로 로그인해야 합니다.

> **Note**
>
> 통합 제어 조사 결과를 해제한 후 Security Hub에서 새로운 표준 기반 조사 결과를 생성하고 통합 조사 결과를 보관하는 데 최대 24시간이 걸릴 수 있습니다. 이 기간 동안에는 계정에 표준 기반 조사 결과와 통합 조사 결과가 혼합되어 표시될 수 있습니다.

Security Hub console

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 일반 탭을 선택합니다.
4. 제어의 경우 편집을 선택하고 통합 제어 조사 결과를 끕니다.
5. 저장을 선택합니다.

Security Hub API

1. UpdateSecurityHubConfiguration를 실행합니다.
2. ControlFindingGenerator를 STANDARD_CONTROL와 같도록 설정합니다.

   요청 예:

```
{
   "ControlFindingGenerator": "STANDARD_CONTROL"
}
```

AWS CLI

1. update-security-hub-configuration 명령을 실행합니다.
2. control-finding-generator를 STANDARD_CONTROL와 같도록 설정합니다.

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

제어 조사 결과에 대한 **Compliance** 세부 정보

제어 항목의 보안 검사를 통해 생성된 결과의 경우, AWS 보안 탐지 결과 형식 (ASFF) Compliance필드에 제어 결과와 관련된 세부 정보가 포함됩니다. Compliance 필드에는 다음 정보가 포함됩니다.

AssociatedStandards

제어가 활성화되는 활성화된 표준.

RelatedRequirements

사용 가능한 모든 표준의 제어 관련 요구 사항 목록. 요구 사항은 PCI DSS(지불 카드 산업 데이터 보안 표준)와 같은 제어를 위한 타사 보안 프레임워크에서 나온 것입니다.

SecurityControlId

Security Hub가 지원하는 보안 표준 전반의 제어를 위한 식별자입니다.

Status

특정 제어에 대해 Security Hub가 실행된 가장 최근 검사 결과입니다. 이전 검사의 결과는 아카이브 상태로 90일 동안 보관됩니다.

StatusReasons

Compliance.Status 값의 사유 목록을 포함합니다. StatusReasons에는 각 사유의 사유 코드와 설명이 포함됩니다.

다음 테이블에는 사용 가능한 상태 코드 및 설명이 나와 있습니다. 수정 단계는 원인 코드와 함께 결과를 생성한 제어에 따라 달라집니다. Security Hub 제어 참조에서 제어를 선택하면 해당 제어의 수정 단계를 볼 수 있습니다.

사유 코드	Compliance.Status	설명
CLOUDTRAIL_METRIC_FILTER_NOT_VALID	FAILED	다중 지역 CloudTrail 트레일에는 유효한 지표 필터가 없습니다.
CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT	FAILED	멀티 CloudTrail 리전 트레일에는 지표 필터가 없습니다.
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	계정에는 필수 구성의 다중 지역 CloudTrail 트레일이 없습니다.
CLOUDTRAIL_REGION_INVAILD	WARNING	다중 지역 CloudTrail 트레일은 현재 지역에 없습니다.
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	유효한 경보 작업이 없습니다.
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch 계정에 알람이 없습니다.
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config 상태는 ConfigError	AWS Config 액세스가 거부되었습니다. AWS Config 활성화되어 있고 충분한 권한이 부여되었는지 확인하십시오.
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config 규칙을 기반으로 리소스를 평가했습니다. 규칙이 해당 범위의 AWS 리소스에 적용되지 않았거나, 지정된 리소스가 삭제되었거나, 평가 결과가 삭제되었습니다.
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	규정 준수 상태는 해당 없음 상태가 NOT_AVAILABLE AWS Config 반환되었기 때문입니다.

사유 코드	Compliance.Status	설명
		AWS Config 상태에 대한 이유를 제공하지 않습니다. 해당 없음 상태가 될 수 있는 몇 가지 이유는 다음과 같습니다. • 리소스가 AWS Config 규칙 범위에서 제거되었습니다. • AWS Config 규칙이 삭제되었습니다. • 리소스가 삭제되었습니다. • AWS Config 규칙 로직은 해당 없음 상태를 생성할 수 있습니다.

사유 코드	Compliance.Status	설명
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config 상태는 다음과 같습니다. ConfigError	이 사유 코드는 여러 가지 유형의 평가 오류에 사용됩니다. 설명에 구체적인 사유 정보가 나와 있습니다. 오류 유형은 다음 중 하나일 수 있습니다. • 권한 부족으로 인해 평가를 수행할 수 없습니다. 설명에 누락된 특정 권한이 나와 있습니다. • 파라미터의 값이 누락되었거나 잘못되었습니다. 설명에 파라미터 및 파라미터 값 요구 사항이 나와 있습니다. • S3 버킷에서 읽는 중 오류가 발생했습니다. 설명에 해당 버킷이 식별되어 있고 구체적인 오류가 나와 있습니다. • AWS 구독이 누락되었습니다. • 평가에 대한 전체 시간이 초과되었습니다. • 일시 중지된 계정입니다.
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config 상태는 다음과 같습니다. ConfigError	AWS Config 규칙을 만드는 중입니다.

사유 코드	Compliance.Status	설명
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	알 수 없는 오류가 발생했습니다.
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	Security Hub는 사용자 지정 Lambda 런타임에 대해 검사를 수행할 수 없습니다.
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	이 규칙과 연결된 S3 버킷이 다른 리전 또는 계정에 있기 때문에 결과가 WARNING 상태입니다. 이 규칙은 크로스 리전 또는 교차 계정 확인을 지원하지 않습니다. 이 리전 또는 계정에서 이 제어를 비활성화하는 것이 좋습니다. 리소스가 있는 리전 또는 계정에서만 실행하세요.
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	CloudWatch 로그 지표 필터에는 유효한 Amazon SNS 구독이 없습니다.
SNS_TOPIC_CROSS_ACCOUNT	WARNING	검색 결과가 WARNING 상태에 있습니다. 이 규칙과 관련된 SNS 주제는 다른 계정에서 소유하고 있습니다. 현재 계정으로는 구독 정보를 얻을 수 없습니다. SNS 주제를 소유한 계정은 현재 계정에 해당 SNS 주제에 대한 sns:ListSubscriptionsByTopic 권한을 부여해야 합니다.

사유 코드	Compliance.Status	설명
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	이 규칙과 연결된 SNS 주제가 다른 리전 또는 계정에 있기 때문에 결과가 WARNING 상태입니다. 이 규칙은 크로스 리전 또는 교차 계정 확인을 지원하지 않습니다. 이 리전 또는 계정에서 이 제어를 비활성화하는 것이 좋습니다. 리소스가 있는 리전 또는 계정에서만 실행하세요.
SNS_TOPIC_INVALID	FAILED	이 규칙과 관련된 SNS 주제는 유효하지 않습니다.
THROTTLING_ERROR	NOT_AVAILABLE	관련 API 작업이 허용된 속도를 초과했습니다.

제어 조사 결과에 대한 **ProductFields** 세부 정보

Security Hub가 보안 검사를 실행하고 제어 조사 결과를 생성할 때 ASFF의 ProductFields 속성에는 다음 필드가 포함됩니다.

ArchivalReasons:0/Description

Security Hub가 기존 조사 결과를 보관하는 이유를 설명합니다.

예를 들어 Security Hub는 제어 또는 표준을 비활성화할 때와 통합 제어 조사 결과를 켜거나 끌 때 기존 조사 결과를 보관합니다.

ArchivalReasons:0/ReasonCode

Security Hub가 기존 조사 결과를 보관하는 이유를 제공합니다.

예를 들어 Security Hub는 제어 또는 표준을 비활성화할 때와 통합 제어 조사 결과를 켜거나 끌 때 기존 조사 결과를 보관합니다.

StandardsGuideArn 또는 StandardsArn

제어와 관련된 표준의 ARN입니다.

CIS AWS 재단 벤치마크 표준의 경우 필드는 입니다. `StandardsGuideArn`

PCI DSS 및 AWS 기본 보안 모범 사례 표준의 경우 필드는 다음과 같습니다. `StandardsArn`

통합 제어 조사 결과를 켜면 이러한 필드는 `Compliance.AssociatedStandards`에 맞게 제거됩니다.

`StandardsGuideSubscriptionArn` 또는 `StandardsSubscriptionArn`

표준에 대한 계정 구독의 ARN입니다.

CIS AWS 재단 벤치마크 표준의 경우 필드는 다음과 같습니다. `StandardsGuideSubscriptionArn`

PCI DSS 및 AWS 기본 보안 모범 사례 표준의 경우 필드는 다음과 같습니다. `StandardsSubscriptionArn`

통합 제어 조사 결과를 켜면 이러한 필드는 제거됩니다.

`RuleId` 또는 `ControlId`

제어의 식별자입니다.

CIS AWS 재단 벤치마크 표준의 경우 필드는 다음과 같습니다. `RuleId`

기타 표준의 경우 필드는 `ControlId`입니다.

통합 제어 조사 결과를 켜면 이러한 필드는 `Compliance.SecurityControlId`에 맞게 제거됩니다.

`RecommendationUrl`

제어에 대한 수정 정보의 URL입니다. 통합 제어 조사 결과를 켜면 이러한 필드는 `Remediation.Recommendation.Url`에 맞게 제거됩니다.

`RelatedAWSResources:0/name`

결과와 연결된 리소스의 이름입니다.

`RelatedAWSResource:0/type`

제어에 연결된 리소스 유형입니다.

`StandardsControlArn`

제어의 ARN입니다. 통합 제어 조사 결과를 켜면 이 필드는 제거됩니다.

`aws/securityhub/ProductName`

제어 기반 조사 결과의 경우 제품 이름은 Security Hub입니다.

`aws/securityhub/CompanyName`

통제 기반 조사 결과의 경우 회사 이름은 입니다. AWS

`aws/securityhub/annotation`

제어를 통해 발견된 문제에 대한 설명입니다.

`aws/securityhub/FindingId`

결과의 식별자입니다. 통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

제어 조사 결과에 심각도 할당

Security Hub 제어 기능에 할당된 심각도는 해당 제어 기능의 중요성을 식별합니다. 제어의 심각도에 따라 제어 조사 결과에 할당되는 심각도 레이블이 결정됩니다.

심각도 기준

제어의 심각도는 다음 기준에 대한 평가를 기반으로 결정됩니다.

- 위협 행위자가 제어와 관련된 구성 약점을 악용하는 것은 얼마나 어려운가요?

  난이도는 취약점을 이용해 위협 시나리오를 수행하는 데 필요한 정교함이나 복잡성의 정도에 따라 결정됩니다.
- 이러한 취약점으로 인해 AWS 계정 귀사 또는 리소스가 손상될 가능성은 얼마나 됩니까?

  사용자 AWS 계정 또는 리소스가 손상되면 데이터 또는 AWS 인프라의 기밀성, 무결성 또는 가용성이 어떤 식으로든 손상됩니다.

  침해 가능성은 위협 시나리오로 인해 서비스 또는 AWS 리소스가 중단되거나 침해될 가능성을 나타냅니다.

예를 들어 다음 구성 약점을 고려해 보십시오.

- 사용자 액세스 키는 90일마다 교체되지 않습니다.
- IAM 루트 사용자 키가 존재합니다.

두 약점 모두 공격자가 악용하기 어렵습니다. 두 경우 모두 공격자는 보안 인증 도용이나 다른 방법을 사용하여 사용자 키를 획득할 수 있습니다. 그런 다음 이를 사용하여 무단으로 리소스에 액세스할 수 있습니다.

그러나 위협 행위자가 루트 사용자 액세스 키를 획득하면 액세스 권한이 더 커지므로 보안 침해 가능성이 훨씬 높아집니다. 따라서 루트 사용자 키 취약점의 심각도가 더 높습니다.

심각도는 기본 리소스의 중요도를 고려하지 않습니다. 중요도는 결과와 관련된 리소스의 중요도 수준입니다. 예를 들어 미션 크리티컬 애플리케이션과 관련된 리소스와 비프로덕션 테스트와 관련된 리소스보다 더 중요합니다. 리소스 중요도 정보를 캡처하려면 AWS 보안 검색 결과 형식 (ASFF) `Criticality` 필드를 사용하십시오.

다음 표에는 보안 레이블에 대한 악용 난이도과 손상 가능성이 나와 있습니다.

	침해 가능성이 매우 높음	침해 가능성이 있음	침해 가능성이 낮음	침해 가능성이 매우 낮음
악용하기 매우 쉬움	심각	심각	높음	중간
악용하기 다소 쉬움	심각	높음	중간	중간
악용하기가 다소 어려움	높음	중간	중간	낮음
악용하기가 매우 어려움	중간	중간	낮음	낮음

심각도 정의

심각도 레이블은 다음과 같이 정의됩니다.

심각 – 문제가 확대되는 것을 방지하려면 문제를 즉시 해결해야 합니다.

> 예를 들어 개방형 S3 버킷은 심각한 결과로 간주됩니다. 개방형 S3 버킷은 수많은 위협 행위자가 검색하기 때문에 노출된 S3 버킷의 데이터를 다른 사용자가 검색하고 액세스할 가능성이 있습니다.

일반적으로 공개적으로 액세스할 수 있는 리소스는 중요한 보안 문제로 간주됩니다. 중요한 발견은 최대한 긴급하게 처리해야 합니다. 리소스의 중요도도 고려해야 합니다.

높음 – 우선적으로 해결해야 할 문제입니다.

예를 들어 기본 VPC 보안 그룹이 인바운드 및 아웃바운드 트래픽에 개방되어 있는 경우 심각도가 높은 것으로 간주됩니다. 위협 행위자가 이 방법을 사용하면 VPC를 손상시키기가 다소 쉽습니다. 또한 위협 행위자가 VPC에 침투한 후에는 리소스를 방해하거나 외부로 유출할 수 있습니다.

Security Hub에서는 심각도가 높은 결과를 단기 우선순위로 처리할 것을 권장합니다. 즉각적인 개선 조치를 취해야 합니다. 리소스의 중요도도 고려해야 합니다.

중간 - 이 문제는 중기 우선 순위로 다루어야 합니다.

예를 들어 전송 중인 데이터에 대한 암호화가 이루어지지 않으면 심각도가 보통인 것으로 간주됩니다. 이 약점을 악용하려면 정교한 man-in-the-middle 공격이 필요합니다. 바꿔 말하면 다소 어렵습니다. 위협 시나리오가 성공하면 일부 데이터가 손상될 수 있습니다.

Security Hub에서는 최대한 빨리 관련 리소스를 조사할 것을 권장합니다. 리소스의 중요도도 고려해야 합니다.

낮음 - 자체적으로 조치가 필요하지 않은 문제입니다.

예를 들어, 포렌식 정보를 수집하지 못하면 심각도가 낮은 것으로 간주됩니다. 이러한 제어는 향후 손상을 방지하는 데 도움이 될 수 있지만 포렌식이 없다고 해서 손상으로 직접 이어지지는 않습니다.

심각도가 낮은 조사 결과에 대해 즉각적인 조치를 취할 필요는 없지만, 다른 문제와 연관시킬 때 컨텍스트를 제공할 수 있습니다.

정보 - 구성 약점은 발견되지 않았습니다.

즉, `PASSED`, `WARNING` 또는 `NOT AVAILABLE` 상태입니다.

권장되는 조치는 없습니다. 정보 조사 결과는 고객이 규정 준수 상태에 있음을 입증하는 데 도움이 됩니다.

제어 조사 결과 업데이트 규칙

특정 규칙에 대한 후속 검사에서는 새로운 결과가 생성될 수 있습니다. 예를 들어, “루트 사용자 사용 금지” 상태가 `FAILED`에서 `PASSED`로 변경될 수 있습니다. 이 경우 최신 결과가 포함된 새 결과가 생성됩니다.

특정 규칙에 대한 후속 점검에서 현재 결과와 동일한 결과를 생성하는 경우 기존 결과가 업데이트됩니다. 새로운 결과는 생성되지 않습니다.

Security Hub는 연결된 리소스가 삭제되거나, 리소스가 존재하지 않거나, 제어가 비활성화된 경우 제어에서 찾은 조사 결과를 자동으로 보관합니다. 연결된 서비스가 현재 사용되지 않기 때문에 리소스가 더 이상 존재하지 않을 수 있습니다. 조사 결과는 다음 기준 중 하나에 따라 자동으로 보관됩니다.

- 결과는 3~5일 동안 업데이트되지 않습니다(이는 최선의 노력이며 보장되지는 않습니다).
- 관련 AWS Config 평가가 반환되었습니다`NOT_APPLICABLE`.

규정 준수 상태 및 제어 상태

AWS 보안 검색 결과 형식 `Compliance.Status` 필드는 규제 탐지 결과의 결과를 설명합니다. Security Hub는 제어 조사 결과의 규정 준수 상태를 사용하여 전체 제어 상태를 결정합니다. 제어 상태는 Security Hub 콘솔에 있는 컨트롤의 세부 정보 페이지에 표시됩니다.

관리자 계정의 경우 제어 상태는 관리자 계정 및 구성원 계정의 제어 상태를 반영합니다. 특히, 컨트롤의 관리자 계정이나 구성원 계정에서 하나 이상의 실패 결과가 있는 경우 컨트롤의 전체 상태는 실패로 표시됩니다. 집계 영역을 설정한 경우 집계 영역의 제어 상태는 집계 영역 및 연결 영역의 제어 상태를 반영합니다. 특히, 콘트롤의 집계 영역 또는 연결된 영역에서 하나 이상의 실패 결과가 있는 경우 컨트롤의 전체 상태는 실패로 표시됩니다.

Security Hub는 일반적으로 Security Hub 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 초기 제어 상태를 생성합니다. 제어 상태가 표시되려면 AWS Config 리소스 기록이 구성되어 있어야 합니다. 제어 상태가 처음으로 생성된 후 Security Hub는 이전 24시간 동안의 결과를 기반으로 24시간마다 제어 상태를 업데이트합니다. 제어 세부 정보 페이지의 타임스탬프는 제어 상태가 마지막으로 업데이트된 시기를 나타냅니다.

> **Note**
>
> 중국 리전 및 AWS GovCloud (US) Region에서 최초 제어 상태가 생성되는 경우 제어 활성화 후 최대 24시간이 소요될 수 있습니다.

조사 결과의 규정 준수 상태 값

각 검색 결과의 규정 준수 상태에는 다음 값 중 하나가 할당됩니다.

- PASSED— 컨트롤이 이 검색 결과에 대한 보안 검사를 통과했음을 나타냅니다. Security Workflow.Status Hub를 로 자동 설정합니다RESOLVED.

  검색 결과가 에서 FAILED WARNINGNOT_AVAILABLE, 또는 PASSED 로 변경되고 Workflow.Status 또는 로 변경되면 Compliance.Status Security Hub는 자동으로 Workflow.Status 로 설정됩니다NEW. NOTIFIED RESOLVED

  컨트롤에 해당하는 리소스가 없는 경우 Security Hub는 계정 수준에서 PASSED 검색 결과를 생성합니다. 컨트롤에 해당하는 리소스가 있지만 리소스를 삭제하면 Security Hub에서 NOT_AVAILABLE 검색 결과를 만들어 즉시 보관합니다. 18시간이 지나면 컨트롤에 해당하는 리소스가 더 이상 없으므로 PASSED 검색 결과를 받게 됩니다.
- FAILED— 컨트롤이 이 검색 결과에 대한 보안 검사를 통과하지 못했음을 나타냅니다.
- WARNING— 확인이 완료되었음을 나타내지만 Security Hub는 리소스가 PASSED or FAILED 상태인지 여부를 확인할 수 없습니다.
- NOT_AVAILABLE— 서버에 장애가 발생했거나, 리소스가 삭제되었거나, AWS Config 평가 결과가 다음과 같아서 검사를 완료할 수 없음을 나타냅니다NOT_APPLICABLE.

  AWS Config 평가 결과가 다음과 NOT_APPLICABLE 같으면 Security Hub는 검색 결과를 자동으로 보관합니다.

제어 상태 값

Security Hub는 제어 결과의 규정 준수 상태에서 전체 제어 상태를 도출합니다. 제어 상태를 결정할 때 Security Hub는 RecordState a가 있는 검색 ARCHIVED 결과와 a가 있는 검색 결과를 무시합니다. Workflow.Status SUPPRESSED

제어 상태에는 다음 값 중 하나가 할당됩니다.

- 합격 - 모든 검색 결과가 규정 준수 상태임을 나타냅니다PASSED.
- 실패 - 최소한 하나의 검색 결과가 규정 준수 상태임을 나타냅니다FAILED.
- 알 수 없음 - 하나 이상의 검색 결과가 WARNING 또는 규정 준수 상태임을 나타냅니다NOT_AVAILABLE. 규정 준수 상태가 인 검색 결과는 없습니다FAILED.
- 데이터 없음 - 제어에 대한 조사 결과가 없음을 나타냅니다. 예를 들어 새로 활성화된 컨트롤은 Security Hub에서 검색 결과를 생성하기 시작할 때까지 이 상태를 유지합니다. 검색 결과가 모두 SUPPRESSED 같거나 현재 지역에서 사용할 수 없는 경우에도 컨트롤은 이 상태가 됩니다.

- 비활성화됨 — 현재 계정 및 지역에서 컨트롤이 비활성화되었음을 나타냅니다. 현재 계정 및 지역에서는 이 컨트롤에 대한 보안 검사가 현재 수행되고 있지 않습니다. 하지만 비활성화된 컨트롤의 발견은 비활성화 후 최대 24시간 동안 규정 준수 상태 값을 유지할 수 있습니다.

보안 점수 결정

Security Hub 콘솔의 요약 페이지 및 제어 페이지에는 활성화된 모든 표준에 대한 요약 보안 점수가 표시됩니다. 또한 보안 표준 페이지에서 Security Hub는 활성화된 각 표준에 대해 0~ 100%의 보안 점수를 표시합니다.

Security Hub를 처음 활성화하면 Security Hub는 사용자가 Security Hub 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 요약 보안 점수와 표준 보안 점수를 계산합니다. 점수는 해당 페이지를 방문할 때 활성화된 표준에 대해서만 생성됩니다. 현재 활성화된 표준 목록을 보려면 `GetEnabledStandards` API 작업을 호출하십시오. 또한 점수가 표시되도록 AWS Config 리소스 기록을 구성해야 합니다. 요약 보안 점수는 표준 보안 점수의 평균입니다.

Security Hub는 점수를 처음 생성한 후 24시간마다 보안 점수를 업데이트합니다. Security Hub는 보안 점수가 마지막으로 업데이트된 시기를 나타내는 타임스탬프를 표시합니다.

> **Note**
>
> 중국 리전 및 AWS GovCloud (US) Region에서 처음으로 보안 점수를 생성하는 데 최대 24시간이 걸릴 수 있습니다.

통합 제어 조사 결과를 켜면 보안 점수가 업데이트되는 데 최대 24시간이 걸릴 수 있습니다. 또한 새 집계 영역을 활성화하거나 연결된 리전을 업데이트하면 기존 보안 점수가 재설정됩니다. Security Hub가 업데이트된 리전의 데이터를 포함하는 새 보안 점수를 생성하는 데 최대 24시간이 걸릴 수 있습니다.

보안 점수 계산 방법

보안 점수는 활성화된 제어에 대한 통과된 제어의 비율을 나타냅니다. 점수는 가장 가까운 정수로 반올림되거나 반내림된 백분율로 표시됩니다.

Security Hub는 활성화된 모든 표준에 대한 요약 보안 점수를 계산합니다. 또한 Security Hub는 활성화된 각 표준에 대한 보안 점수를 계산합니다. 점수 계산을 위해, 활성화된 제어에는 통과, 실패 및 알 수 없음 상태의 제어가 포함됩니다. 데이터 없음 상태인 제어는 점수 계산에서 제외됩니다.

Security Hub는 제어 상태를 계산할 때 보관된 조사 결과 및 억제된 조사 결과를 무시합니다. 이는 보안 점수에 영향을 미칠 수 있습니다. 예를 들어 제어에 대한 모든 실패 조사 결과를 숨기면 상태가 통과로 바뀌어 보안 점수를 높일 수 있습니다. 제어 상태에 대한 자세한 내용은 규정 준수 상태 및 제어 상태을 참조하십시오.

채점 예제:

표준	통과된 제어	실패한 제어	알 수 없는 제어	표준 점수
AWS 기본 보안 모범 사례 v1.0.0	168	22	0	88%
CIS AWS 재단 벤치마크 v1.4.0	8	29	0	22%
CIS AWS 재단 벤치마크 v1.2.0	6	35	0	15%
NIST 특별 간행물 800-53 개정 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

요약 보안 점수를 계산할 때 Security Hub는 표준 전체에서 각 제어를 한 번만 계산합니다. 예를 들어, 세 가지 활성화된 표준에 적용되는 제어를 활성화한 경우 채점 목적상 하나의 활성화된 제어로만 계산됩니다.

이 예시에서는활성화된 표준 전체에 걸쳐 활성화된 제어의 총 개수가 528개이지만 Security Hub는 채점 목적으로 각 고유 제어를 한 번만 계산합니다. 활성화된 고유한 제어의 수는 528개 미만일 수 있습니다. 활성화된 고유한 제어의 수가 515개이고 통과한 고유 제어의 수가 357개라고 가정할 경우 요약 점수는 69% 입니다. 이 점수는 통과된 고유 제어의 수를 활성화된 고유 제어의 수로 나누어 계산합니다.

현재 리전의 계정에 하나의 표준만 활성화했더라도 요약 점수가 표준 보안 점수와 다를 수 있습니다. 관리자 계정에 로그인하고 구성원 계정에 추가 표준이나 다른 표준이 활성화되어 있는 경우 이런 현상이 발생할 수 있습니다. 집계 영역의 점수를 보는 도중 연결된 리전에 추가 표준이나 다른 표준이 활성화되어 있는 경우에도 이런 현상이 발생할 수 있습니다.

관리자 계정의 보안 점수

관리자 계정에 로그인한 경우 요약 보안 점수 및 표준 점수는 관리자 계정 및 모든 구성원 계정의 제어 상태를 반영합니다.

멤버 계정이 하나라도 제어 상태가 실패인 경우 관리자 계정에서는 해당 제어의 상태가 실패로 표시되며 관리자 계정 점수에 영향을 줍니다.

관리자 계정으로 로그인하고 집계 영역에서 점수를 보는 경우 보안 점수는 모든 구성원 계정 및 모든 연결된 리전의 제어 상태를 반영합니다.

집계 영역을 설정한 경우 보안 점수

집계를 AWS 리전설정한 경우 요약 보안 점수와 표준 점수가 통제 상태를 모두 반영합니다. 연결 지역.

하나의 연결된 리전에서라도 제어 상태가 실패인 경우 집계 영역에서도 해당 제어의 상태가 실패로 표시되며 집계 영역 점수에 영향을 줍니다.

관리자 계정으로 로그인하고 집계 영역에서 점수를 보는 경우 보안 점수는 모든 구성원 계정 및 모든 연결된 리전의 제어 상태를 반영합니다.

Security Hub 표준 참조

AWS Security Hub 현재 이 섹션에 설명된 보안 표준을 지원합니다.

표준을 선택하면 표준 및 해당 표준에 적용되는 제어에 대한 자세한 내용을 볼 수 있습니다.

Security Hub 표준 및 제어는 규제 프레임워크 또는 감사 준수를 보장하지 않습니다. 대신 제어는 AWS 계정 및 리소스의 현재 상태를 모니터링하는 방법을 제공합니다.

지원되는 표준

- AWS 기본 보안 모범 사례 (FSBP) 표준
- CIS AWS 기반 벤치마크
- NIST(국립 표준 기술 연구소) SP 800-53 개정 5
- Payment Card Industry Data Security Standard(PCI DSS)
- AWS 리소스 태깅 표준
- 서비스 관리형 표준

AWS 기본 보안 모범 사례 (FSBP) 표준

AWS 기본 보안 모범 사례 표준은 사용자 AWS 계정 및 리소스가 보안 모범 사례에서 벗어나는 경우 이를 탐지하는 제어 집합입니다.

이 표준을 사용하면 모든 AWS 계정 및 워크로드를 지속적으로 평가하여 모범 사례에서 벗어나는 영역을 신속하게 식별할 수 있습니다. 이 표준은 조직의 보안 태세를 개선하고 유지하는 방법에 대한 실행 가능한 규범적 지침을 제공합니다.

제어에는 여러 AWS 서비스로부터의 리소스에 대한 보안 모범 사례가 포함됩니다. 각 제어에는 또한 적용되는 보안 기능을 반영하는 범주가 할당됩니다. 자세한 내용은 the section called “제어 범주”을 참조하십시오.

FSBP 표준에 적용되는 제어

[계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정

[ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.

[ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.

[API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.

[APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.

[ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.

[APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.

[APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.

[APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.

[APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.

[AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.

[AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.

[AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.

[AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포함해야 합니다.

[AutoScaling.3] Auto Scaling 그룹 시작 구성에서는 인스턴스 메타데이터 서비스 버전 2 (IMDSv2) 를 요구하도록 EC2 인스턴스를 구성해야 합니다.

[Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.

[AutoScaling.6] Auto Scaling 그룹은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.

[AutoScaling.9] Amazon EC2 Auto Scaling 그룹은 Amazon EC2 시작 템플릿을 사용해야 합니다.

[백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.

[CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.

[CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.

[CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.

[CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

[CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.

[CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.

[CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.

[CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.

[CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.

[CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.

[CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.

[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.

[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.

[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch

[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.

[CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.

[CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.

[CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.

[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.

[DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.

[DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.

[DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

[DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

[DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.

[DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.

[DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.

[DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.

[DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.

[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.

[DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.

[DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch

[DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.

[DynamoDB.2] DynamoDB 테이블에는 복구가 활성화되어 있어야 합니다. point-in-time

[DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.

[DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.

[EC2.1] Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.

[EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

[EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.

[EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.

[EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.

[EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.

[EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.

[EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.

[EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.

[EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

[EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.

[EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.

[EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.

[EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.

[ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.

[ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.

[ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.

[ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.

[ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.

[ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.

[ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.

[ECS.5] ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다.

[ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.

[ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.

[ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.

[ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.

[EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS

[EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.

[EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.

[EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.

[EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.

[EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.

[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.

[EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.

[EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

[ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

[ElastiCache.2] Redis 캐시 ElastiCache 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.

[ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.

[ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.

[ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.

[ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.

[ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.

[ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.

[ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch

[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.

[ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager

[ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.

[ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.

[ELB.5] 애플리케이션 및 Classic Load Balancer 로깅이 활성화되어야 합니다.

[ELB.6] 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다.

[ELB.7] Classic Load Balancer connection draining닝이 활성화되어 있어야 합니다.

[ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config

[ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.

[ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.

[ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.

[ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.

[ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.

[EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

[EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

[ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

[ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .

[ES.5] Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

[ES.6] Elasticsearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.

[ES.7] Elasticsearch 도메인은 최소 3개의 전용 프라이머리 노드로 구성해야 합니다.

[ES.8] Elasticsearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다.

[EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.

[FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.

[FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.

[GuardDuty.1] 을 GuardDuty 활성화해야 합니다.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

[IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.

[Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.

[KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.

[KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.

[KMS.3] 을 (를) 실수로 AWS KMS keys 삭제해서는 안 됩니다.

[Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.

[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.

[Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.

[Macie.1] Amazon Macie를 활성화해야 합니다

[Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.

[MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch

[MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.

[MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.

[Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.

[Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch

[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.

[Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

[Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.

[Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.

[Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.

[NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.

[NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.

[NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.

[NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.

[NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.

[NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.

[Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

[Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .

[Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

[Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.

[Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.

[Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .

[Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.

[PCA.1] AWS Private CA 루트 인증 기관을 비활성화해야 합니다.

[Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.

[RDS.1] RDS 스냅샷은 비공개여야 합니다.

[RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

[RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.

[RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.

[RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.

[RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch

[RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.

[RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.

[RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.

[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

[RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.

[RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.

[RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.

[RDS.17] RDS DB 인스턴스는 태그를 스냅샷에 복사하도록 구성되어야 합니다.

[RDS.18] RDS 인스턴스는 VPC에 배포되어야 합니다.

[RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.21] 중요한 데이터베이스 파라미터 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.22] 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.23] RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용하지 않아야 합니다.

[RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

[RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

[RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.

[RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch

[RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.

[Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.

[Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.

[Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

[Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.

[Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다

[Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.

[Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.

[Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다

[Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.

[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.

[S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.

[S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다.

[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.

[S3.6] S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

[S3.9] S3 범용 버킷은 서버 액세스 로깅을 활성화해야 합니다.

[S3.12] ACL은 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 됩니다.

[S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.

[S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.

[SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

[SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.

[SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.

[SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.

[SecretsManager.1] Secrets Manager 비밀번호에는 자동 로테이션이 활성화되어 있어야 합니다.

[SecretsManager.2] 자동 순환으로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.

[SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제

[SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.

[ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS

[SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.

[SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager

[SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.

[SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

[SSM.4] SSM 문서는 공개해서는 안 됩니다.

[StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.

[Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.

[WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

[WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.

[WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.

[WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

[WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.

[WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.

[WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

[WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

[WAF.12] AWS WAF 규칙에는 메트릭이 활성화되어 있어야 합니다. CloudWatch

CIS AWS 기반 벤치마크

CIS (인터넷 보안 센터) AWS 기반 벤치마크는 보안 구성 모범 사례의 집합으로 사용됩니다. AWS업계에서 인정받은 이러한 모범 사례는 명확한 step-by-step 구현 및 평가 절차를 제공합니다. 운영 체제에서 클라우드 서비스 및 네트워크 장치에 이르기까지 이 벤치마크의 제어 기능은 조직에서 사용하는 특정 시스템을 보호하는 데 도움이 됩니다.

AWS Security Hub CIS AWS 재단 벤치마크 v3.0.0, 1.4.0 및 v1.2.0을 지원합니다.

이 페이지는 각 버전에서 지원하는 보안 제어를 나열하고 버전을 비교합니다.

CIS AWS 재단 벤치마크 v3.0.0

Security Hub는 CIS AWS 재단 벤치마크 버전 3.0.0을 지원합니다.

Security Hub는 CIS 보안 소프트웨어 인증 요구 사항을 충족했으며 다음 CIS 벤치마크에 대해 CIS 보안 소프트웨어 인증을 받았습니다.

- CIS AWS 재단 벤치마크용 CIS 벤치마크, v3.0.0, 레벨 1
- CIS 재단 벤치마크용 AWS CIS 벤치마크, v3.0.0, 레벨 2

CIS 재단 벤치마크 v3.0.0에 적용되는 규제 AWS

[계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정

[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.

[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.

[CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail

[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

[EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.

[EC2.54] EC2 보안 그룹은: :/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.

[EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

[IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support

[IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.

[IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.

[IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess

[IAM.28] IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.

[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS

[RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.

[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.

[S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.

[S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.

CIS 재단 벤치마크 v1.4.0 AWS

Security Hub는 CIS AWS 재단 벤치마크 v1.4.0을 지원합니다.

CIS 재단 벤치마크 v1.4.0에 적용되는 규제 항목 AWS

[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.

[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.

[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch

[CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.

[CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail

[CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.

[CloudWatch.4] IAM 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.5] 기간 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오 CloudTrail AWS Config.

[CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제를 위한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.8] S3 버킷 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.9] AWS Config 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.10] 보안 그룹 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.11] 네트워크 액세스 제어 목록 (NACL) 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.12] 네트워크 게이트웨이 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.13] 라우팅 테이블 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.14] VPC 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인

[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

[IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support

[IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.

[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.

[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.

인터넷 보안 센터(CIS) AWS 파운데이션 벤치마크 v1.2.0

Security Hub는 CIS AWS 재단 벤치마크 버전 1.2.0을 지원합니다.

Security Hub는 CIS 보안 소프트웨어 인증 요구 사항을 충족했으며 다음 CIS 벤치마크에 대해 CIS 보안 소프트웨어 인증을 받았습니다.

- CIS AWS 재단 벤치마크용 CIS 벤치마크, v1.2.0, 레벨 1
- CIS AWS 재단 벤치마크용 CIS 벤치마크, v1.2.0, 레벨 2

CIS 재단 벤치마크 v1.2.0에 적용되는 규제 AWS

[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.

[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.

[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch

[CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.

[CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail

[CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.

[CloudWatch.2] 승인되지 않은 API 호출에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.3] MFA를 사용하지 않는 관리 콘솔 로그인에 대한 로그 메트릭 필터 및 경보가 있는지 확인

[CloudWatch.4] IAM 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.5] 기간 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오 CloudTrail AWS Config.

[CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제를 위한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.8] S3 버킷 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.9] AWS Config 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.10] 보안 그룹 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.11] 네트워크 액세스 제어 목록 (NACL) 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.12] 네트워크 게이트웨이 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.13] 라우팅 테이블 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

[CloudWatch.14] VPC 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인

[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.

[EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.

[IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.

[IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.

[IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.

[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

[IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.

[IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support

[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS

CIS 재단 벤치마크 버전 비교 AWS

이 섹션에서는 CIS (인터넷 보안 센터) AWS 재단 벤치마크 v3.0.0, v1.4.0 및 v1.2.0 간의 차이점을 요약합니다.

Security Hub는 이러한 CIS AWS 기반 벤치마크 버전을 각각 지원하지만 보안 모범 사례를 최신 상태로 유지하려면 v3.0.0을 사용하는 것이 좋습니다. 동시에 여러 버전의 표준을 사용할 수 있습니다. 자세한 정보는 보안 표준 활성화 및 비활성화을 참조하세요. v3.0.0으로 업그레이드하려면 이전 버전을 비활성화하기 전에 먼저 활성화하는 것이 가장 좋습니다. Security Hub 통합을 사용하여 여러 AWS 계정 계정을 중앙에서 관리하고 모든 계정에서 v3.0.0을 일괄 사용하도록 설정하려는 경우 중앙 구성을 사용할 수 있습니다. AWS Organizations

각 버전의 CIS 요구 사항에 컨트롤 매핑

CIS AWS 재단 벤치마크의 각 버전이 지원하는 제어 항목을 파악하십시오.

제어 ID 및 제목	CIS v3.0.0 요구 사항	CIS v1.4.0 요구 사항	CIS v1.2.0 요구 사항
[계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정	1.2	1.2	1.18
[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.	3.1	3.1	2.1
[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.	3.1	3.1	2.1
[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.	3.5	3.7	2.7
[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.	3.2	3.2	2.2
[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	3.4	2.4
[CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	3.3	2.3
[CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail	3.4	3.6	2.6

제어 ID 및 제목	CIS v3.0.0 요구 사항	CIS v1.4.0 요구 사항	CIS v1.2.0 요구 사항
[CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.	지원되지 않음 — 수동 확인	4.3	3.3
[CloudWatch.2] 승인되지 않은 API 호출에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	지원되지 않음 — 수동 확인	3.1
[CloudWatch.3] MFA를 사용하지 않는 관리 콘솔 로그인에 대한 로그 메트릭 필터 및 경보가 있는지 확인	지원되지 않음 — 수동 확인	지원되지 않음 — 수동 확인	3.2
[CloudWatch.4] IAM 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	4.4	3.4
[CloudWatch.5] 기간 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오 CloudTrail AWS Config.	지원되지 않음 — 수동 확인	4.5	3.5
[CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	4.6	3.6
[CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제를 위한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	4.7	3.7
[CloudWatch.8] S3 버킷 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	4.8	3.8

제어 ID 및 제목	CIS v3.0.0 요구 사항	CIS v1.4.0 요구 사항	CIS v1.2.0 요구 사항
[CloudWatch.9] AWS Config 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	4.9	3.9
[CloudWatch.10] 보안 그룹 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	4.10	3.10
[CloudWatch.11] 네트워크 액세스 제어 목록 (NACL) 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	4.11	3.11
[CloudWatch.12] 네트워크 게이트웨이 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	4.12	3.12
[CloudWatch.13] 라우팅 테이블 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	지원되지 않음 — 수동 확인	4.13	3.13
[CloudWatch.14] VPC 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인	지원되지 않음 — 수동 확인	4.14	3.14
[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.	3.3	3.5	2.5
[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.	5.4	5.3	4.3
[EC2.6] VPC 플로 로깅은 모든 VPC 에서 활성화되어야 합니다.	3.7	3.9	2.9

제어 ID 및 제목	CIS v3.0.0 요구 사항	CIS v1.4.0 요구 사항	CIS v1.2.0 요구 사항
[EC2.7] EBS 기본 암호화를 활성화해야 합니다.	2.2.1	2.2.1	지원되지 않음
[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.	5.6	지원되지 않음	지원되지 않음
[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.	지원되지 않음 — 요구 사항 5.2 및 5.3으로 대체	지원되지 않음 — 요구 사항 5.2 및 5.3으로 대체	4.1
[EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.	지원되지 않음 — 요구 사항 5.2 및 5.3으로 대체	지원되지 않음 — 요구 사항 5.2 및 5.3으로 대체	4.2
[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.	5.1	5.1	지원되지 않음
[EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.	5.2	지원되지 않음	지원되지 않음
[EC2.54] EC2 보안 그룹은: :/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.	5.3	지원되지 않음	지원되지 않음
[EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS	2.4.1	지원되지 않음	지원되지 않음
[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.	지원되지 않음	1.16	1.22
[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.	1.15	지원되지 않음	1.16

제어 ID 및 제목	CIS v3.0.0 요구 사항	CIS v1.4.0 요구 사항	CIS v1.2.0 요구 사항
[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.	1.14	1.14	1.4
[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.	1.4	1.4	1.12
[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.	1.10	1.10	1.2
[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.	1.6	1.6	1.14
[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.	지원되지 않음 — 대신 참조 [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.	지원되지 않음 - [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다. 대신 참조	1.3
[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.	1.5	1.5	1.13
[IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	1.5
[IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	1.6

제어 ID 및 제목	CIS v3.0.0 요구 사항	CIS v1.4.0 요구 사항	CIS v1.2.0 요구 사항
[IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	1.7
[IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	1.8
[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.	1.8	1.8	1.9
[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.	1.9	1.9	1.10
[IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	1.11
[IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support	1.17	1.17	1.2
[IAM.20] 루트 사용자의 사용을 피합니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	지원되지 않음 — CIS는 이 요구 사항을 제거했습니다.	1.1
[IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.	1.12	1.12	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.

제어 ID 및 제목	CIS v3.0.0 요구 사항	CIS v1.4.0 요구 사항	CIS v1.2.0 요구 사항
[IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.	1.19	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.
[IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess	1.22	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.
[IAM.28] IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.	1.20	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.
[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS	3.6	3.8	2.8
[Macie.1] Amazon Macie를 활성화해야 합니다	지원되지 않음 — 수동 확인	지원되지 않음 — 수동 확인	지원되지 않음 — 수동 확인
[RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config	2.3.3	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.
[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.	2.3.1	2.3.1	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.
[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.	2.3.2	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.

제어 ID 및 제목	CIS v3.0.0 요구 사항	CIS v1.4.0 요구 사항	CIS v1.2.0 요구 사항
[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.	2.1.4	2.1.5	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.
[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.	2.1.1	2.1.2	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.
[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.	2.1.4	2.1.5	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.
[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.	2.1.2	2.1.3	지원되지 않음 — CIS는 이 요구 사항을 이후 버전에서 추가했습니다.

CIS AWS 재단 벤치마크용 ARN

CIS AWS 재단 벤치마크 버전을 하나 이상 활성화하면 AWS 보안 조사 결과 형식 (ASFF) 으로 결과를 받기 시작합니다. ASFF에서 각 버전은 다음과 같은 Amazon 리소스 이름 (ARN) 을 사용합니다.

CIS AWS 재단 벤치마크 v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

CIS AWS 재단 벤치마크 v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/1.4.0
```

CIS 재단 벤치마크 v1.2.0 AWS

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Security Hub API의 GetEnabledStandards작업을 사용하여 활성화된 표준의 ARN을 확인할 수 있습니다.

위 값은 for입니다. `StandardsArn` 그러나 `StandardsSubscriptionArn` 는 사용자가 BatchEnableStandards지역에서 전화를 걸어 표준을 구독할 때 Security Hub가 생성하는 표준 구독 리소스를 나타냅니다.

> **Note**
>
> CIS AWS Foundation Benchmark 버전을 활성화하면 Security Hub가 다른 사용 표준에서 활성화된 컨트롤과 동일한 AWS Config 서비스 연결 규칙을 사용하는 컨트롤에 대한 검색 결과를 생성하는 데 최대 18시간이 걸릴 수 있습니다. 자세한 정보는 보안 검사 실행 예약을 참조하세요.

통합 제어 결과를 켜면 검색 필드가 달라집니다. 해당 차이점에 대한 자세한 내용은 ASFF 필드 및 값에 대한 통합의 영향을 참조하십시오. 샘플 제어 결과에 대한 내용은 을 참조하십시오샘플 제어 조사 결과.

Security Hub에서 지원되지 않는 CIS 요구 사항

위 표에서 설명한 것처럼 Security Hub는 CIS AWS 기반 벤치마크의 모든 버전에서 모든 CIS 요구 사항을 지원하지는 않습니다. 지원되지 않는 요구 사항의 대부분은 리소스 상태를 검토하여 수동으로만 평가할 수 있습니다. AWS

NIST(국립 표준 기술 연구소) SP 800-53 개정 5

NIST SP 800-53 개정 5는 미국 상무부 산하 기관인 국립 표준 기술 연구소(NIST)에서 개발한 사이버 보안 및 규정 준수 프레임워크입니다. 이 규정 준수 프레임워크는 정보 시스템 및 중요 자원의 가용성, 기밀성 및 무결성을 보호하는 데 도움이 됩니다. 미국 연방 정부 기관 및 계약업체는 시스템을 보호하기 위해 NIST SP 800-53을 준수해야 하지만 민간 기업은 자발적으로 이를 사이버 보안 위험을 줄이기 위한 지침 프레임워크로 사용할 수 있습니다.

Security Hub는 일부 NIST SP 800-53 요구 사항을 지원하는 제어 기능을 제공합니다. 이러한 제어는 자동 보안 검사를 통해 평가됩니다. Security Hub 제어는 수동 검사가 필요한 NIST SP 800-53 요구 사

항을 지원하지 않습니다. 또한 Security Hub 제어는 각 제어의 세부 정보에 관련 요구 사항으로 나열된 자동화된 NIST SP 800-53 요구 사항만 지원합니다. 다음 목록에서 제어를 선택하여 세부 정보를 확인하십시오. 제어 세부 정보에 언급되지 않은 관련 요구 사항은 현재 Security Hub에서 지원되지 않습니다.

다른 프레임워크와 달리 NIST SP 800-53은 요구 사항 평가 방법에 대한 규범이 아닙니다. 대신 프레임워크는 지침을 제공하며 Security Hub NIST SP 800-53 제어는 해당 지침의 서비스 이해를 나타냅니다.

Security Hub 통합을 사용하여 여러 계정을 중앙에서 관리하고 모든 계정에서 NIST SP 800-53을 일괄 사용하도록 설정하려는 경우 관리자 계정에서 Security Hub 다중 계정 스크립트를 실행할 수 있습니다. AWS Organizations

NIST SP 800-53 개정 5에 대한 자세한 내용은 NIST 컴퓨터 보안 리소스 센터를 참조하십시오.

NIST SP 800-53 개정 5에 적용되는 제어

[계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정

[Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations

[ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.

[API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.

[APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.

[ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.

[APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.

[APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.

[APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.

[APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.

[AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.

[AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.

[AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포함해야 합니다.

[AutoScaling.3] Auto Scaling 그룹 시작 구성에서는 인스턴스 메타데이터 서비스 버전 2 (IMDSv2) 를 요구하도록 EC2 인스턴스를 구성해야 합니다.

[Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.

[AutoScaling.6] Auto Scaling 그룹은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.

[AutoScaling.9] Amazon EC2 Auto Scaling 그룹은 Amazon EC2 시작 템플릿을 사용해야 합니다.

[백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.

[CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.

[CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.

[CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.

[CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

[CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.

[CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.

[CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.

[CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.

[CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.

[CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.

[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.

[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.

[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch

[CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.

[CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.

[CloudWatch.17] CloudWatch 알람 조치를 활성화해야 합니다.

[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.

[CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.

[CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.

[CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.

[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.

[DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.

[DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.

[DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

[DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

[DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.

[DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.

[DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.

[DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.

[DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.

[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.

[DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.

[DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch

[DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.

[DynamoDB.2] DynamoDB 테이블에는 복구가 활성화되어 있어야 합니다. point-in-time

[DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.

[DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.

[DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.

[EC2.1] Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.

[EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

[EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.

[EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.

[EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.

[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.

[EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.

[EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.

[EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.

[EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.

[EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.

[EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

[EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.

[EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.

[EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.

[EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.

[EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.

[ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.

[ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.

[ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.

[ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.

[ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.

[ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.

[ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.

[ECS.5] ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다.

[ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.

[ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.

[ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.

[ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.

[EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS

[EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.

[EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.

[EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.

[EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.

[EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.

[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.

[EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.

[EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

[ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

[ElastiCache.2] Redis 캐시 ElastiCache 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.

[ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.

[ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.

[ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.

[ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.

[ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.

[ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.

[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.

[ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager

[ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.

[ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.

[ELB.5] 애플리케이션 및 Classic Load Balancer 로깅이 활성화되어야 합니다.

[ELB.6] 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다.

[ELB.7] Classic Load Balancer connection draining닝이 활성화되어 있어야 합니다.

[ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config

[ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.

[ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.

[ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.

[ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.

[ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.

[ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF

[EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

[EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

[ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

[ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .

[ES.5] Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

[ES.6] Elasticsearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.

[ES.7] Elasticsearch 도메인은 최소 3개의 전용 프라이머리 노드로 구성해야 합니다.

[ES.8] Elasticsearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다.

[EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.

[EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.

[FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.

[FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.

[GuardDuty.1] 을 GuardDuty 활성화해야 합니다.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.

[Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.

[KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.

[KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.

[KMS.3] 을 (를) 실수로 AWS KMS keys 삭제해서는 안 됩니다.

[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS

[Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.

[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.

[Lambda.3] Lambda 함수는 VPC에 있어야 합니다.

[Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.

[Macie.1] Amazon Macie를 활성화해야 합니다

[Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.

[MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.

[MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.

[MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch

[MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.

[MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.

[MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다

[Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.

[Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch

[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.

[Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

[Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.

[Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.

[Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.

[Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.

[NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.

[NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.

[NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.

[NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.

[NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.

[NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.

[NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.

[Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

[Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .

[Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

[Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.

[Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.

[Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .

[Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.

[Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.

[PCA.1] AWS Private CA 루트 인증 기관을 비활성화해야 합니다.

[RDS.1] RDS 스냅샷은 비공개여야 합니다.

[RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

[RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.

[RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.

[RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.

[RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch

[RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.

[RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.

[RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.

[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

[RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.

[RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.

[RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.

[RDS.17] RDS DB 인스턴스는 태그를 스냅샷에 복사하도록 구성되어야 합니다.

[RDS.18] RDS 인스턴스는 VPC에 배포되어야 합니다.

[RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.21] 중요한 데이터베이스 파라미터 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.22] 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.23] RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용하지 않아야 합니다.

[RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

[RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

[RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.

[RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.

[RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch

[RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.

[Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.

[Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.

[Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

[Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.

[Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다

[Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.

[Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.

[Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다

[Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.

[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.

[S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.

[S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다.

[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.

[S3.6] S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정

[S3.7] S3 범용 버킷은 지역 간 복제를 사용해야 합니다.

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

[S3.9] S3 범용 버킷은 서버 액세스 로깅을 활성화해야 합니다.

[S3.10] 버전 관리가 활성화된 S3 범용 버킷은 수명 주기 구성을 가져야 합니다.

[S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.

[S3.12] ACL은 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 됩니다.

[S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.

[S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.

[S3.15] S3 범용 버킷에는 객체 잠금이 활성화되어 있어야 합니다.

[S3.17] S3 범용 버킷은 저장 시 다음을 사용하여 암호화해야 합니다. AWS KMS keys

[S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.

[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.

[SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

[SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.

[SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.

[SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.

[SecretsManager.1] Secrets Manager 비밀번호에는 자동 로테이션이 활성화되어 있어야 합니다.

[SecretsManager.2] 자동 순환으로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.

[SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제

[SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.

[ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS

[SNS.1] SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS

[SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.

[SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager

[SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.

[SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

[SSM.4] SSM 문서는 공개해서는 안 됩니다.

[Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.

[WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

[WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.

[WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.

[WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

[WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.

[WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.

[WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

[WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

[WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

[WAF.12] AWS WAF 규칙에는 메트릭이 활성화되어 있어야 합니다. CloudWatch

Payment Card Industry Data Security Standard(PCI DSS)

Security Hub의 PCI DSS(지불 카드 산업 데이터 AWS 보안 표준)는 카드 소지자 데이터 처리에 대한 일련의 보안 모법 사례를 제공합니다. 이 표준을 사용하여 카드 소지자 데이터를 처리하는 리소스의 보안 취약성을 발견할 수 있습니다. Security Hub는 현재 계정 수준에서 제어의 범위를 지정합니다. 카드 소유자 데이터를 저장, 처리 또는 전송하는 리소스가 있는 모든 계정에서 이러한 제어를 활성화하는 것이 좋습니다.

이 표준은 PCI AWS DSS 지침을 제공하는 인증을 받은 공인 AWS 보안 평가자 (QSA) 팀인 보안 보증 서비스 LLC (SAS) 의 검증과 PCI DSS 보안 표준 위원회 (PCI SSC) 의 평가를 받았습니다. AWS SAS는 자동 검사가 고객이 PCI DSS 평가를 준비하는 데 도움이 될 수 있음을 확인했습니다.

이 페이지에는 보안 제어 ID와 제목이 나열되어 있습니다. AWS GovCloud (US) Region 및 중국 지역에서는 표준별 제어 ID와 제목이 사용됩니다. 보안 제어 ID 및 제목을 표준별 제어 ID 및 제목에 매핑하는 방법은 통합이 제어 ID 및 제목에 미치는 영향을 참조하십시오.

PCI DSS에 적용되는 제어

[AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.

[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.

[CloudTrail.3] 하나 이상의 트레일을 활성화해야 합니다. CloudTrail

[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.

[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch

[CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.

[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.

[CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.

[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.

[DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.

[EC2.1] Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.

[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.

[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.

[ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[GuardDuty.1] 을 GuardDuty 활성화해야 합니다.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.10] IAM 사용자를 위한 암호 정책은 엄격한 기준을 적용해야 합니다. AWS Config

[IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS

[Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.

[Lambda.3] Lambda 함수는 VPC에 있어야 합니다.

[Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.

[Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[RDS.1] RDS 스냅샷은 비공개여야 합니다.

[RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config

[PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.

[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.

[S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.

[S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다.

[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.

[S3.7] S3 범용 버킷은 지역 간 복제를 사용해야 합니다.

[SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

[SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager

[SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.

[SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

AWS 리소스 태깅 표준

이 섹션에서는 AWS 리소스 태깅 표준에 대한 정보를 제공합니다.

> **Note**
>
> AWS 리소스 태깅 표준은 캐나다 서부 (캘거리), 중국 및 지역에서는 사용할 수 없습니다. AWS GovCloud (US)

AWS 리소스 태깅 표준이란 무엇입니까?

태그는 AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키와 값 쌍입니다. 대부분의 AWS 리소스에서는 리소스를 생성할 때 또는 리소스를 만든 후에 태그를 추가할 수 있습니다. 리소스의 예로는 아마존 CloudFront 배포판, 아마존 Elastic Compute Cloud (Amazon EC2) 인스턴스, 시크릿 인 등이 있습니다. AWS Secrets Manager

태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색 및 필터링할 수 있습니다.

각 태그에는 다음 두 가지 부분이 있습니다.

- 태그 키(예: `CostCenter`, `Environment` 또는 `Project`). 태그 키는 대/소문자를 구별합니다.
- 태그 값 (예: `111122223333` 또는`Production`) 태그 키처럼 태그 값은 대/소문자를 구별합니다.

태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다.

AWS 리소스에 태그를 추가하는 방법에 대한 지침은AWS Security Hub 사용 설명서에서 AWS 리소스에 태그를 추가하는 방법을 참조하십시오.

AWS Security Hub에서 개발한 AWS 리소스 태깅 표준을 사용하면 AWS 리소스에 태그 키가 누락되었는지 신속하게 식별할 수 있습니다. `requiredTagKeys`매개 변수를 사용자 지정하여 컨트롤이 확인하는 특정 태그 키를 지정할 수 있습니다. 특정 태그가 제공되지 않은 경우 컨트롤은 하나 이상의 태그 키가 있는지만 확인합니다.

AWS 리소스 태깅 표준을 활성화하면 AWS 보안 검색 결과 형식 (ASFF) 으로 검색 결과를 받기 시작합니다.

> **Note**
>
> AWS 리소스 태깅 표준을 사용하도록 설정하면 Security Hub에서 지원되는 다른 표준에서 사용하도록 설정된 컨트롤과 동일한 AWS Config 서비스 연결 규칙을 사용하는 컨트롤에 대한 검색 결과를 생성하는 데 최대 18시간이 걸릴 수 있습니다. 자세한 정보는 보안 검사 실행 예약을 참조하세요.

이 표준에는 다음과 같은 Amazon 리소스 이름 (ARN) 이 있습니다.
`arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`

Security Hub API의 GetEnabledStandards작업을 사용하여 활성화된 표준의 ARN을 확인할 수도 있습니다.

AWS 리소스 태깅 표준의 제어

AWS 리소스 태깅 표준에는 다음과 같은 컨트롤이 포함됩니다. 컨트롤을 선택하면 해당 컨트롤에 대한 자세한 설명을 볼 수 있습니다.

- [ACM.3] ACM 인증서에는 태그를 지정해야 합니다.

- [AppSync.4] AWS AppSync GraphQL API는 태그가 지정되어야 합니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다
- [AutoScaling.10] EC2 Auto Scaling 그룹에는 태그를 지정해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudTrail.9] CloudTrail 트레일에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DynamoDB.5] DynamoDB 테이블에는 태그를 지정해야 합니다.
- [EC2.33] EC2 트랜짓 게이트웨이 첨부 파일에는 태그를 지정해야 합니다.
- [EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.35] EC2 네트워크 인터페이스에는 태그를 지정해야 합니다.
- [EC2.36] EC2 고객 게이트웨이에는 태그를 지정해야 합니다.
- [EC2.37] EC2 엘라스틱 IP 주소에는 태그를 지정해야 합니다.
- [EC2.38] EC2 인스턴스에는 태그를 지정해야 합니다.
- [EC2.39] EC2 인터넷 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.41] EC2 네트워크 ACL에는 태그를 지정해야 합니다.
- [EC2.42] EC2 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.43] EC2 보안 그룹에는 태그를 지정해야 합니다.

- [EC2.44] EC2 서브넷에는 태그가 지정되어야 합니다.
- [EC2.45] EC2 볼륨에는 태그가 지정되어야 합니다.
- [EC2.46] 아마존 VPC는 태그가 지정되어야 합니다
- [EC2.47] Amazon VPC 엔드포인트 서비스는 태그가 지정되어야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.
- [EC2.49] Amazon VPC 피어링 연결에는 태그를 지정해야 합니다.
- [EC2.50] EC2 VPN 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.52] EC2 트랜짓 게이트웨이에는 태그가 지정되어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.13] ECS 서비스에는 태그를 지정해야 합니다.
- [ECS.14] ECS 클러스터에는 태그를 지정해야 합니다.
- [ECS.15] ECS 작업 정의에는 태그를 지정해야 합니다.
- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EKS.6] EKS 클러스터에는 태그를 지정해야 합니다.
- [EKS.7] EKS ID 공급자 구성에는 태그를 지정해야 합니다.
- [ES.9] Elasticsearch 도메인에는 태그를 지정해야 합니다.
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.23] IAM 액세스 분석기 분석기는 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다

- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.2] Kinesis 스트림에는 태그가 지정되어야 합니다.
- [Lambda.6] Lambda 함수는 태그가 지정되어야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [NetworkFirewall.7] Network Firewall 방화벽에는 태그를 지정해야 합니다.
- [NetworkFirewall.8] Network Firewall 방화벽 정책에 태그를 지정해야 합니다.
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.
- [RDS.29] RDS DB 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [RDS.30] RDS DB 인스턴스에는 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.32] RDS DB 스냅샷에는 태그가 지정되어야 합니다.
- [RDS.33] RDS DB 서브넷 그룹에는 태그가 지정되어야 합니다.
- [Redshift.11] Redshift 클러스터에는 태그를 지정해야 합니다.
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [Redshift.14] Redshift 클러스터 서브넷 그룹은 태그가 지정되어야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [SecretsManager.5] Secrets Manager 비밀에는 태그를 지정해야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.

서비스 관리형 표준

서비스 관리형 표준은 다른 사람이 관리하는 보안 표준입니다. AWS 서비스 예를 들어, 서비스 관리형 AWS Control Tower표준:은 관리하는 서비스 관리형 표준입니다. AWS Control Tower 서비스 관리형 표준은 다음과 같은 측면에서 AWS Security Hub가 관리하는 보안 표준과 다릅니다.

- 표준 생성 및 삭제 - 관리 서비스의 콘솔이나 API 또는 AWS CLI를 사용하여 서비스 관리형 표준을 생성하고 삭제합니다. 이러한 방법 중 하나로 관리 서비스에서 표준을 작성하기 전까지는 표준이 Security Hub 콘솔에 나타나지 않으며 Security Hub API 또는 AWS CLI에 의해 액세스할 수 없습니다.
- 제어 자동 활성화 없음 - 서비스 관리형 표준을 만들 때 Security Hub 및 관리 서비스는 표준에 적용되는 제어를 자동으로 활성화하지 않습니다. 또한 Security Hub에서 표준에 대한 새 제어를 릴리스하더라도 자동으로 활성화되지는 않습니다. 이는 Security Hub가 관리하는 표준과는 다릅니다. Security Hub에서 제어를 구성하는 일반적인 방법에 대한 자세한 내용은 보안 제어 보기 및 관리을 참조하십시오.
- 제어 활성화 및 비활성화 - 드리프트를 방지하려면 관리 서비스에서 제어를 활성화 및 비활성화하는 것이 좋습니다.
- 제어 가용성 – 관리 서비스는 서비스 관리형 표준의 일부로 사용할 수 있는 제어를 선택합니다. 사용 가능한 제어에는 기존 Security Hub 제어의 전부 또는 일부가 포함될 수 있습니다.

관리 서비스가 서비스 관리형 표준을 만들고 이에 대한 제어를 사용할 수 있게 만든 후에는 Security Hub 콘솔, Security Hub API 또는 AWS CLI에서 제어 조사 결과, 제어 상태 및 표준 보안 점수에 액세스할 수 있습니다. 이 정보의 일부 또는 전부는 관리 서비스에서도 확인할 수 있습니다.

다음 목록에서 서비스 관리형 표준을 선택하면 해당 표준에 대한 자세한 내용을 볼 수 있습니다.

서비스 관리형 표준

- 서비스 관리형 표준: AWS Control Tower

서비스 관리형 표준: AWS Control Tower

이 섹션에서는 서비스 관리 표준에 대한 정보를 제공합니다. AWS Control Tower

서비스 관리형 표준이란 무엇입니까? AWS Control Tower

이 표준은 AWS Security Hub 및 사용자를 위해 설계되었습니다 AWS Control Tower. 이를 통해 서비스에서 Security Hub의 탐지 AWS Control Tower 제어와 함께 사전 예방적 제어를 구성할 수 있습니다. AWS Control Tower

사전 예방적 제어는 정책 위반이나 잘못된 구성으로 이어질 수 있는 작업에 플래그를 지정하므로 규정 준수를 AWS 계정 유지하는 데 도움이 됩니다. 탐지 제어 기능은 AWS 계정내의 리소스 비준수(예: 잘못된 구성)를 감지합니다. AWS 환경에 대한 사전 예방적 탐지 제어를 지원함으로써 다양한 개발 단계에서 보안 태세를 강화할 수 있습니다.

> **Tip**
>
> 서비스 관리 표준은 AWS Security Hub에서 관리하는 표준과 다릅니다. 예를 들어, 관리 서비스에서 서비스 관리형 표준을 만들고 삭제해야 합니다. 자세한 정보는 서비스 관리형 표준을 참조하세요.

Security Hub 콘솔 및 API에서 다른 Security Hub AWS Control Tower 표준과 함께 서비스 관리형 표준을 볼 수 있습니다.

표준 생성

이 표준은 에서 표준을 생성한 경우에만 사용할 수 있습니다. AWS Control Tower AWS Control Tower 다음 방법 중 하나를 사용하여 해당 컨트롤을 처음 활성화할 때 표준을 만듭니다.

- AWS Control Tower 콘솔
- AWS Control Tower API (API를 `EnableControl`호출하세요)
- AWS CLI (`enable-control`명령 실행)

Security Hub 컨트롤은 AWS Control Tower 콘솔에서 SH로 식별됩니다. ***## ID*** (예: SH) CodeBuild.1).

표준을 생성할 때 Security Hub를 아직 활성화하지 않았다면 Security AWS Control Tower Hub도 자동으로 활성화됩니다.

설정하지 않은 경우 Security Hub 콘솔 AWS Control Tower, Security Hub API 또는 에서 이 표준을 보거나 액세스할 수 없습니다 AWS CLI. AWS Control Tower설정했더라도 위의 방법 중 하나를 AWS Control Tower 사용하여 표준을 먼저 만들지 않으면 Security Hub에서 이 표준을 보거나 액세스할 수 없습니다.

이 표준은 다음을 포함하여 AWS GovCloud (US)사용 가능한 AWS 리전AWS Control Tower 지역에서만 사용할 수 있습니다.

표준의 제어 활성화 및 비활성화

AWS Control Tower 콘솔에서 표준을 만든 후 두 서비스에서 표준 및 사용 가능한 컨트롤을 볼 수 있습니다.

표준을 처음 만든 후에는 자동으로 활성화되는 제어가 없습니다. 또한 Security Hub에서 새 컨트롤을 추가할 때 서비스 관리형 표준:에 대해 해당 컨트롤이 자동으로 활성화되지 않습니다. AWS Control

Tower다음 방법 중 하나를 사용하여 AWS Control Tower 표준에 대한 제어를 활성화하거나 비활성화해야 합니다.

- AWS Control Tower 콘솔
- AWS Control Tower API (EnableControl 및 DisableControlAPI를 호출하세요)
- AWS CLI (enable-control 및 disable-control명령 실행)

에서 AWS Control Tower컨트롤의 활성화 상태를 변경하면 Security Hub에도 변경 내용이 반영됩니다.

하지만 Security Hub에서 활성화된 컨트롤을 사용하지 않도록 설정하면 제어 드리프트가 AWS Control Tower 발생합니다. 의 제어 상태는 다음과 같이 AWS Control Tower 표시됩니다. `Drifted` AWS Control Tower 콘솔에서 OU 재등록을 선택하거나 위 방법 중 하나를 AWS Control Tower 사용하여 컨트롤을 비활성화했다가 다시 활성화하여 이 드리프트를 해결할 수 있습니다.

에서 활성화 및 비활성화 작업을 완료하면 컨트롤 드리프트를 방지하는 데 도움이 됩니다. AWS Control Tower

에서 제어를 활성화하거나 비활성화하면 해당 작업이 계정 AWS Control Tower및 지역에 적용됩니다. Security Hub에서 제어를 사용하거나 사용하지 않도록 설정하는 경우(이 표준에서는 권장되지 않음) 작업은 현재 계정 및 리전에만 적용됩니다.

> **Note**
>
> 중앙 구성은 서비스 관리 표준:을 관리하는 데 사용할 수 없습니다. AWS Control Tower중앙 구성을 사용하는 경우 중앙에서 관리되는 계정에 대해 이 표준에서 제어를 활성화 및 비활성화하는 데는 AWS Control Tower 서비스만 사용할 수 있습니다.

활성화 상태 및 제어 상태 보기

다음 방법 중 하나를 사용하여 제어의 활성화 상태를 볼 수 있습니다.

- 보안 허브 콘솔, 보안 허브 API 또는 AWS CLI
- AWS Control Tower 콘솔
- AWS Control Tower 활성화된 컨트롤 목록을 볼 수 있는 API (ListEnabledControlsAPI 호출)
- AWS CLI 활성화된 컨트롤 목록을 보려면 (list-enabled-controls명령 실행)

Security Hub에서 해당 컨트롤을 명시적으로 활성화하지 않는 한 Security `Disabled` Hub에서 사용하지 않도록 설정한 AWS Control Tower 컨트롤은 Security Hub의 활성화 상태가 됩니다.

Security Hub는 제어 조사 결과의 워크플로 상태 및 규정 준수 상태를 기반으로 제어 상태를 계산합니다. 활성화 상태 및 제어 상태에 대한 자세한 내용은 제어에 대한 세부 정보 보기을 참조하십시오.

Security Hub는 제어 상태를 기반으로 서비스 관리형 표준:의 보안 점수를 계산합니다. AWS Control Tower이 점수는 Security Hub에서만 사용할 수 있습니다. 또한 Security Hub에서는 제어 조사 결과만 볼 수 있습니다. 표준 보안 점수 및 제어 결과는 에서 사용할 수 없습니다. AWS Control Tower

> **Note**
>
> 서비스 관리 AWS Control Tower표준:에 대한 제어를 사용하도록 설정하면 Security Hub에서 기존 AWS Config 서비스 연결 규칙을 사용하는 컨트롤에 대한 검색 결과를 생성하는 데 최대 18시간이 걸릴 수 있습니다. Security Hub에서 다른 표준 및 제어를 활성화한 경우 기존 서비스 연결 규칙이 있을 수 있습니다. 자세한 내용은 보안 검사 실행 예약을 참조하십시오.

표준 삭제

다음 방법 중 하나를 사용하여 해당하는 모든 제어를 AWS Control Tower 비활성화하여 에서 이 표준을 삭제할 수 있습니다.

- AWS Control Tower 콘솔
- AWS Control Tower API (API를 `DisableControl`호출하세요)
- AWS CLI (`disable-control`명령 실행)

모든 제어를 비활성화하면 AWS Control Tower의 모든 관리 계정 및 관리되는 리전의 표준이 삭제됩니다. 에서 표준을 삭제하면 Security Hub 콘솔의 표준 페이지에서 해당 표준이 AWS Control Tower 제거되며 더 이상 Security Hub API 또는 를 사용하여 액세스할 수 없습니다 AWS CLI.

> **Note**
>
> Security Hub의 표준에서 모든 제어를 비활성화해도 표준이 비활성화되거나 삭제되지는 않습니다.

Security Hub 서비스를 사용하지 않도록 설정하면 서비스 관리 표준 AWS Control Tower 및 활성화한 기타 모든 표준이 제거됩니다.

서비스 관리형 표준의 필드 형식 찾기: AWS Control Tower

서비스 관리형 AWS Control Tower 표준:을 만들고 이에 대한 제어를 활성화하면 Security Hub에서 제어 결과를 받기 시작합니다. Security Hub는 제어 조사 결과를 AWS 보안 검색 형식 (ASFF)로 보고합니다. 다음은 이 표준의 Amazon 리소스 이름(ARN) 및 `GeneratorId`에 대한 ASFF 값입니다.

- 표준 ARN – *`arn:aws:us-east-1`*`:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/`*`CodeBuild.1`*

서비스 관리형 표준에 대한 샘플 검색 결과는 을 참조하십시오. AWS Control Tower샘플 제어 조사 결과

서비스 관리형 표준에 적용되는 규제 항목: AWS Control Tower

서비스 관리 표준: FSBP (기본 보안 모범 사례) 표준의 AWS 일부인 일부 컨트롤을 AWS Control Tower 지원합니다. 실패한 조사 결과에 대한 수정 단계를 포함하여 이에 대한 정보를 보려면 다음 테이블에서 제어를 선택하십시오.

다음 목록은 서비스 관리형 표준에 사용할 수 있는 컨트롤을 보여줍니다. AWS Control Tower제어에 대한 리전별 제한은 FSBP 표준의 상관 제어에 대한 리전별 제한과 일치합니다. 이 목록은 표준에 구애받지 않는 보안 제어 ID를 보여줍니다. AWS Control Tower 콘솔에서 컨트롤 ID는 SH로 포맷됩니다. ***`## ID`*** (예: SH) CodeBuild.1). Security Hub에서 계정에서 통합 제어 조사 결과가 꺼져 있는 경우 `ProductFields.ControlId` 필드는 표준 기반 제어 ID를 사용합니다. 표준 기반 제어 ID는 CT로 포맷됩니다. ***`ControlId`***(예: CT. CodeBuild.1).

- [계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정
- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.

- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포함해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성에서는 인스턴스 메타데이터 서비스 버전 2 (IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [AutoScaling.6] Auto Scaling 그룹은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [AutoScaling.9] Amazon EC2 Auto Scaling 그룹은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.
- [CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.
- [CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.
- [CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.
- [DynamoDB.2] DynamoDB 테이블에는 복구가 활성화되어 있어야 합니다. point-in-time

- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [EC2.1] Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.
- [EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.
- [EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.
- [EC2.7] EBS 기본 암호화를 활성화해야 합니다.
- [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.
- [EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.
- [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.
- [EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.
- [EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다.

- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.
- [ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.
- [ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.
- [ELB.5] 애플리케이션 및 Classic Load Balancer 로깅이 활성화되어야 합니다.
- [ELB.6] 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다.
- [ELB.7] Classic Load Balancer connection draining닝이 활성화되어 있어야 합니다.
- [ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config
- [ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.

- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .
- [ES.5] Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [ES.6] Elasticsearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.
- [ES.7] Elasticsearch 도메인은 최소 3개의 전용 프라이머리 노드로 구성해야 합니다.
- [ES.8] Elasticsearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.

- [KMS.3] 을 (를) 실수로 AWS KMS keys 삭제해서는 안 됩니다.
- [KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS
- [Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.
- [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.
- [Lambda.3] Lambda 함수는 VPC에 있어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.

- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config
- [RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.
- [RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.
- [RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.
- [RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.
- [RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.
- [RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.17] RDS DB 인스턴스는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.18] RDS 인스턴스는 VPC에 배포되어야 합니다.
- [RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.21] 중요한 데이터베이스 파라미터 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.22] 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.23] RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용하지 않아야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
- [Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.

- [Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.
- [S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다.
- [S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.
- [S3.6] S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정
- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
- [S3.9] S3 범용 버킷은 서버 액세스 로깅을 활성화해야 합니다.
- [S3.12] ACL은 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 됩니다.
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.
- [S3.17] S3 범용 버킷은 저장 시 다음을 사용하여 암호화해야 합니다. AWS KMS keys
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SecretsManager.1] Secrets Manager 비밀번호에는 자동 로테이션이 활성화되어 있어야 합니다.
- [SecretsManager.2] 자동 순환으로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제
- [SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

이 표준에 대한 자세한 내용은 AWS Control Tower 사용 설명서의 Security Hub 제어를 참조하십시오.

보안 표준 보기 및 관리

보안 표준에는 규제 프레임워크, 업계 모범 사례 또는 회사 정책의 준수 여부를 결정하기 위한 일련의 요구 사항이 포함됩니다. AWS Security Hub 이러한 요구 사항을 제어 항목에 매핑하고 제어 항목에 대한 보안 검사를 실행하여 표준 요구 사항이 충족되고 있는지 평가합니다. 제어는 하나 이상의 표준에서 활성화될 수 있습니다. 통합 제어 조사 결과를 설정하면 Security Hub는 제어가 여러 활성화된 표준에 포함된 경우에도 보안 검사당 단일 조사 결과를 생성합니다. 자세한 내용은 통합 제어 조사 결과을 참조하십시오.

사용 가능한 표준 및 해당 표준에 적용되는 제어 목록은 표준 참조을 참조하십시오. Security Hub 콘솔의 보안 표준 페이지에는 Security Hub에서 지원되는 모든 보안 표준과 해당 보안 표준의 활성화 상태가 표시됩니다. 계정에서 활성화된 각 보안 표준 (또는 조직의 하나 이상의 계정과 AWS Organizations 통합을 사용하는 경우) 에 대해 다음 정보를 확인할 수 있습니다.

- 중앙 구성을 사용하는 경우 다양한 Security Hub 구성 정책의 표준 활성화 상태
- 비활성화된 표준에 대한 설명
- 표준에서 현재 활성화된 제어 목록과 결과의 규정 준수 상태에 기반한 해당 제어의 전체 상태
- 표준에 적용되지만 현재 비활성화된 제어 목록
- 표준의 보안 점수

Security Hub는 각 표준에 대한 보안 점수를 생성합니다. 관리자 계정은 구성원 계정 전반에 걸쳐 집계된 보안 점수와 제어 상태를 확인합니다. 집계 영역을 설정한 경우 보안 점수는 연결된 모든 리전의 규정 준수 상태를 반영합니다. 자세한 내용은 보안 점수 계산 방법을 참조하십시오.

주제

- 보안 표준 활성화 및 비활성화

- 표준에 대한 세부 정보 보기
- 특정 표준에서의 제어 활성화 및 비활성화

보안 표준 활성화 및 비활성화

Security Hub에서 사용할 수 있는 각 보안 표준을 활성화하거나 비활성화할 수 있습니다.

보안 표준을 활성화하기 전에 리소스 기록을 AWS Config 활성화하고 구성했는지 확인하십시오. 그렇지 않으면 Security Hub가 표준에 적용되는 제어 항목에 대한 결과를 생성하지 못할 수 있습니다. 자세한 정보는 구성 AWS Config을 참조하세요.

> **Note**
>
> 표준 활성화 및 비활성화 지침은 중앙 구성 사용 여부에 따라 달라집니다. 이 섹션에서는 차이점을 설명합니다. Security Hub 및 를 통합하는 사용자는 중앙 구성을 사용할 수 AWS Organizations있습니다. 다중 계정, 다중 리전 환경에서 표준을 활성화 또는 비활성화하는 프로세스를 단순화하려면 중앙 구성을 사용하는 것이 좋습니다.

보안 표준 활성화

보안 표준을 활성화하면 해당 표준에 대한 모든 제어가 자동으로 활성화됩니다. 또한 Security Hub는 표준에 적용되는 제어 기능에 대한 결과를 생성하기 시작합니다.

각 표준에서 비활성화 및 비활성화할 제어를 선택할 수 있습니다. 제어를 비활성화하면 해당 제어에 대한 조사 결과가 생성되지 않고 보안 점수를 계산할 때 제어가 무시됩니다.

Security Hub를 활성화하면 Security Hub는 사용자가 Security Hub 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 표준에 대한 초기 보안 점수를 계산합니다. 중국 리전 및 AWS GovCloud (US) Region에 처음으로 보안 점수를 생성하는 데 최대 24시간이 걸릴 수 있습니다. 점수는 해당 페이지를 방문할 때 활성화된 표준에 대해서만 생성됩니다. 또한 점수가 표시되도록 AWS Config 리소스 기록을 구성해야 합니다. 처음으로 점수를 생성한 후 Security Hub는 24시간마다 보안 점수를 업데이트합니다. Security Hub는 보안 점수가 마지막으로 업데이트된 시기를 나타내는 타임스탬프를 표시합니다. 현재 활성화된 표준 목록을 보려면 GetEnabledStandards API를 호출하세요.

다중 계정 및 리전에 표준 활성화

여러 계정에서 보안 표준을 적용하려면 중앙 구성을 사용해야 합니다. AWS 리전

중앙 구성을 사용하는 경우 위임된 관리자는 하나 이상의 표준을 활성화하는 Security Hub 구성 정책을 만들 수 있습니다. 그런 다음 구성 정책을 특정 계정 및 OU(조직 단위) 또는 루트와 연결할 수 있습니다. 구성 정책은 홈 리전(집계 영역이라고도 함) 및 연결된 모든 리전에 적용됩니다.

구성 정책은 사용자 지정을 제공합니다. 예를 들어 한 OU에서는 FSBP (기본 보안 모범 사례) 만 사용하도록 선택하고 다른 OU에서는 FSBP 및 CIS (인터넷 보안 센터) AWS 재단 벤치마크 v1.4.0을 사용하도록 선택할 수 있습니다. AWS 지정된 표준을 활성화하는 구성 정책을 만드는 방법에 대한 지침은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요.

중앙 구성을 사용하는 경우 Security Hub는 새 계정이나 기존 계정의 표준을 자동으로 활성화하지 않습니다. 대신 구성 정책을 만들 때 위임된 관리자는 여러 계정에서 사용할 표준을 정의합니다. Security Hub는 FSBP만 활성화하는 권장 구성 정책을 제공합니다. 자세한 정보는 구성 정책 유형을 참조하세요.

> **Note**
>
> 위임된 관리자는 구성 정책을 생성하여 서비스 관리 표준을 제외한 모든 표준을 활성화할 수 있습니다. AWS Control Tower 이 표준은 서비스에서만 활성화할 수 있습니다. AWS Control Tower 중앙 구성을 사용하는 경우 AWS Control Tower에서만 중앙에서 관리되는 계정에 대해 이 표준의 제어를 활성화 및 비활성화할 수 있습니다.

일부 계정에서 위임된 관리자가 아닌 자체 표준을 구성하도록 하려면 위임된 관리자가 해당 계정을 자체 관리형 계정으로 지정할 수 있습니다. 자체 관리형 계정은 각 리전에서 개별적으로 표준을 구성해야 합니다.

단일 계정 및 리전에서 표준 활성화

중앙 구성을 사용하지 않거나 자체 관리형 계정인 경우 구성 정책을 사용하여 다중 계정 및 리전에서 표준을 중앙에서 활성화할 수 없습니다. 하지만 다음 단계를 사용하여 단일 계정 및 리전에서 표준을 활성화할 수 있습니다.

Security Hub console

한 계정과 리전에서 표준을 활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 표준을 활성화하려는 리전에서 Security Hub를 사용하고 있는지 확인합니다.
3. Security Hub 탐색 창에서 보안 표준을 선택합니다.

4. 활성화하려는 표준에 대해 활성화를 선택합니다. 이렇게 하면 해당 표준 내의 모든 제어도 활성화됩니다.
5. 표준을 활성화하려는 각 리전에 대해 이 단계를 반복합니다.

Security Hub API

한 계정과 리전에서 표준을 활성화하려면

1. BatchEnableStandards API를 호출합니다.
2. 활성화하려는 표준의 Amazon 리소스 이름(ARN)을 입력합니다. 표준 ARN을 얻으려면 DescribeStandards API를 호출하세요.
3. 표준을 활성화하려는 각 리전에 대해 이 단계를 반복합니다.

AWS CLI

한 계정과 리전에서 표준을 활성화하려면

1. batch-enable-standards 명령을 실행합니다.
2. 활성화하려는 표준의 Amazon 리소스 이름(ARN)을 입력합니다. 표준 ARN을 얻으려면 describe-standards 명령을 실행하세요.

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn": "standard ARN"}'
```

예

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"}'
```

3. 표준을 활성화하려는 각 리전에 대해 이 단계를 반복합니다.

기본 보안 표준 자동 활성화

중앙 구성을 사용하지 않는 경우 Security Hub는 새 계정이 조직에 가입할 때 기본 보안 표준을 자동으로 활성화합니다. 기본 표준의 일부인 모든 제어도 자동으로 활성화됩니다. 현재 자동으로 활성화되는 기본 보안 표준은 기본 보안 모범 사례 (FSBP) 및 CIS (인터넷 보안 센터) AWS 재단 벤치마크 v1.2.0

입니다. AWS 새 계정에서 표준을 수동으로 활성화하려는 경우 자동으로 활성화된 표준을 끌 수 있습니다.

중앙 구성을 사용하는 경우 기본 표준을 활성화하는 구성 정책을 만들고 이 정책을 루트에 연결할 수 있습니다. 다른 정책과 연결하거나 자체 관리하지 않는 한 모든 조직 계정 및 OU는 이 구성 정책을 상속합니다.

자동 활성화된 표준 끄기

다음 단계는 중앙 구성과 통합하지만 중앙 구성을 사용하지 않는 경우에만 적용됩니다. AWS Organizations Organizations를 사용하지 않는 경우 Security Hub를 처음 활성화할 때 기본 표준을 끄거나 표준을 비활성화하는 단계를 따를 수 있습니다.

Security Hub console

자동 활성화된 표준을 끄려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   관리자 계정의 보안 인증을 사용하여 로그인합니다.
2. Security Hub 탐색 창의 설정에서 구성를 선택합니다.
3. 계정 탭에서 기본 표준 자동 활성화를 끕니다.

Security Hub API

자동 활성화된 표준을 끄려면

1. Security Hub 관리자 계정에서 UpdateOrganizationConfiguration API를 호출합니다.
2. 새 구성원 계정에서 자동 활성화 표준을 끄려면 `AutoEnableStandards`를 `NONE`과 같도록 설정합니다.

AWS CLI

자동 활성화된 표준을 끄려면

1. update-organization-configuration 명령을 실행합니다.
2. 새 구성원 계정에서 자동 활성화된 표준을 끄기 위한 `auto-enable-standards` 파라미터를 포함시킵니다.

```
aws securityhub update-organization-configuration --auto-enable-standards
```

보안 표준 비활성화

Security Hub에서 보안 표준을 비활성화하면 다음과 같은 상황이 발생합니다.

- 표준에 적용되는 모든 제어도 다른 표준과 연관되지 않는 한 비활성화됩니다.
- 비활성화된 제어에 대한 확인은 더 이상 수행되지 않으며 비활성화된 제어에 대한 추가 조사 결과는 생성되지 않습니다.
- 비활성화된 제어에 대한 기존 결과는 약 3~5일 후에 자동으로 보관됩니다.
- Security Hub에서 비활성화된 컨트롤에 대해 만든 AWS Config 규칙이 제거됩니다.

  이 문제는 일반적으로 표준을 비활성화한 후 몇 분 내에 발생하지만 시간이 더 걸릴 수 있습니다. AWS Config 규칙을 삭제하기 위한 첫 번째 요청이 실패하면 Security Hub는 12시간마다 재시도합니다. 하지만 Security Hub를 비활성화했거나 다른 표준을 활성화하지 않은 경우 Security Hub는 요청을 재시도할 수 없습니다. 즉, AWS Config 규칙을 삭제할 수 없습니다. 이 문제가 발생하여 AWS Config 규칙을 삭제해야 하는 경우 문의하세요 AWS Support.

다중 계정 및 리전에서 표준 비활성화

다중 계정 및 리전에서 보안 표준을 비활성화하려면 중앙 구성을 사용해야 합니다.

중앙 구성을 사용하는 경우 위임된 관리자는 하나 이상의 표준을 비활성화하는 구성 정책을 만들 수 있습니다. 구성 정책을 특정 계정 및 OU 또는 루트와 연결할 수 있습니다. 구성 정책은 홈 리전(집계 영역이라고도 함) 및 연결된 모든 리전에 적용됩니다.

구성 정책은 사용자 지정을 제공합니다. 예를 들어 한 OU에서는 PCI DSS(지불 카드 산업 데이터 보안 표준)를 비활성화하는 것을 선택하고 다른 OU에서는 PCI DSS와 NIST(국립 표준 기술 연구소) SP 800-53 개정 5를 모두 비활성화하는 것을 선택할 수 있습니다. 지정된 표준을 비활성화하는 구성 정책을 만드는 방법에 대한 지침은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요.

> **Note**
>
> 위임된 관리자는 구성 정책을 생성하여 서비스 관리 표준:을 제외한 모든 표준을 사용하지 않도록 설정할 수 있습니다. AWS Control Tower서비스에서만 이 표준을 사용하지 않도록 설정

할 수 있습니다. AWS Control Tower 중앙 구성을 사용하는 경우 AWS Control Tower에서만 중앙에서 관리되는 계정에 대해 이 표준의 제어를 활성화 및 비활성화할 수 있습니다.

일부 계정에서 위임된 관리자가 아닌 자체 표준을 구성하도록 하려면 위임된 관리자가 해당 계정을 자체 관리형 계정으로 지정할 수 있습니다. 자체 관리형 계정은 각 리전에서 개별적으로 표준을 구성해야 합니다.

단일 계정 및 리전에서 표준 비활성화

중앙 구성을 사용하지 않거나 자체 관리형 계정인 경우 구성 정책을 사용하여 다중 계정 및 리전에서 표준을 중앙에서 비활성화할 수 없습니다. 하지만 다음 단계를 사용하여 단일 계정 및 리전에서 표준을 비활성화할 수 있습니다.

Security Hub console

한 계정 및 리전에서 표준을 비활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 표준을 비활성화하려는 리전에서 Security Hub를 사용하고 있는지 확인합니다.
3. Security Hub 탐색 창에서 보안 표준을 선택합니다.
4. 비활성화하려는 표준에 대해 비활성화를 선택합니다.
5. 표준을 비활성화하려는 각 리전에 대해 이 단계를 반복합니다.

Security Hub API

한 계정 및 리전에서 표준을 비활성화하려면

1. BatchDisableStandards API를 호출합니다.
2. 비활성화하려는 각 표준에 대해 표준 구독 ARN을 입력합니다. 활성화된 표준에 맞는 구독 ARN을 가져오려면 GetEnabledStandards API를 호출하세요.
3. 표준을 비활성화하려는 각 리전에 대해 이 단계를 반복합니다.

AWS CLI

한 계정 및 리전에서 표준을 비활성화하려면

1. batch-disable-standards 명령을 실행합니다.

2. 비활성화하려는 각 표준에 대해 표준 구독 ARN을 입력합니다. 활성화된 표준에 맞는 구독 ARN을 가져오려면 get-enabled-standards 명령을 실행하세요.

```
aws securityhub batch-disable-standards --standards-subscription-arns "standard subscription ARN"
```

예

```
aws securityhub batch-disable-standards --standards-subscription-arns "arn:aws:securityhub:us-west-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0"
```

3. 표준을 비활성화하려는 각 리전에 대해 이 단계를 반복합니다.

표준에 대한 세부 정보 보기

AWS Security Hub 콘솔의 표준 세부 정보 페이지에는 다음 정보가 포함됩니다.

- 표준에서 활성화된 제어에 대한 표준 보안 점수 및 보안 검사의 시각적 요약. 와 AWS Organizations 통합하는 경우 하나 이상의 조직 계정에서 활성화된 컨트롤은 활성화된 것으로 간주됩니다.
- 표준에 적용되는 제어를 활성화하거나 비활성화하기 위한 설정.
- 표준에 적용되는 제어 목록입니다. 제어는 활성화 상태에 따라 여러 탭으로 구분됩니다. 모두 사용 가능 열의 제어 수는 실패, 알 수 없음, 데이터 없음, 통과 열에 있는 제어의 합계입니다.

Security Hub API를 사용하여 표준에 대한 세부 정보를 검색할 수도 있습니다. AWS CLI 다음 섹션에서는 표준에 대한 세부 정보를 얻는 방법을 설명합니다.

활성화된 표준에 대한 세부 정보 표시(콘솔)

보안 표준 페이지에서 활성화된 표준의 세부 정보 페이지를 표시할 수 있습니다.

관리자 계정으로 로그인한 경우 하나 이상의 구성원 계정에서 활성화된 모든 표준에 대한 세부 정보를 볼 수 있습니다.

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. Security Hub 탐색 창에서 보안 표준을 선택합니다.
3. 세부 정보를 표시하려는 표준에 대해 결과 보기를 선택합니다.

표준 보안 점수 및 보안 검사 요약

표준 세부 정보 페이지 상단에는 표준에 대한 보안 점수가 있습니다. 점수는 표준에 대해 활성화된 제어(데이터가 있는)의 수에 대한 통과된 제어의 백분율입니다.

Security Hub는 일반적으로 Security Hub 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 초기 보안 점수를 계산합니다. 점수는 해당 페이지를 방문할 때 활성화된 표준에 대해서만 생성됩니다. 현재 활성화된 표준 목록을 보려면 `GetEnabledStandards` API 작업을 사용하십시오. 또한 점수가 표시되도록 AWS Config 리소스 기록을 구성해야 합니다. 처음으로 점수를 생성한 후 Security Hub는 24시간마다 보안 점수를 업데이트합니다. Security Hub는 보안 점수가 마지막으로 업데이트된 시기를 나타내는 타임스탬프를 표시합니다. 자세한 정보는 the section called “보안 점수 결정”을 참조하세요.

> **Note**
>
> 중국 리전 및 AWS GovCloud (US) Region에 처음으로 보안 점수를 생성하는 데 최대 24시간이 걸릴 수 있습니다.

점수 옆에는 표준에 맞게 활성화된 제어에 대한 보안 검사를 요약한 차트가 있습니다. 차트는 실패한 보안 검사와 통과한 보안 검사의 비율을 보여줍니다. 차트에서 일시 중지하면 팝업에 다음이 표시됩니다.

- 각 심각도의 제어에 대한 보안 검사 실패 수
- 알 수 없음 상태인 제어에 대한 보안 검사 수
- 통과한 보안 검사 수

관리자 계정의 경우 표준 점수와 차트는 관리자 계정 및 모든 구성원 계정에서 집계됩니다.

보안 표준 세부 정보 페이지의 모든 데이터는 집계 영역을 설정하지 않은 한 현재 리전에만 적용됩니다. 집계 영역을 설정한 경우 보안 점수는 여러 리전에 적용되며 연결된 모든 리전의 조사 결과를 포함합니다. 표준 세부 정보 페이지에 있는 제어의 규정 준수 상태에는 연결된 리전의 조사 결과도 반영되며, 보안 검사 횟수에는 연결된 리전의 조사 결과도 포함됩니다.

활성화된 표준에서 제어 보기

표준의 세부 정보 페이지를 방문하면 표준에 적용되는 보안 제어 목록을 볼 수 있습니다. 이 목록은 제어의 규정 준수 상태와 각 제어에 할당된 심각도를 기준으로 정렬됩니다. Security Hub는 24시간마다

제어 상태와 보안 검사 수를 업데이트합니다. 각 탭의 타임스탬프는 제어 상태와 보안 검사 수가 가장 최근에 업데이트된 시기를 나타냅니다. 자세한 내용은 the section called “규정 준수 상태 및 제어 상태”을 참조하십시오.

관리자 계정의 경우 관리자 계정 및 모든 구성원 계정의 제어 규정 준수 상태 및 보안 검사 횟수가 집계됩니다.

모두 활성화 탭에는 표준에서 현재 활성화된 모든 제어가 나열됩니다. 관리자 계정의 경우 모두 활성화 탭에는 해당 계정 또는 하나 이상의 멤버 계정에서 표준으로 활성화된 제어가 포함됩니다.

실패, 알 수 없음, 데이터 없음 및 통과 탭에서 모두 활성화 탭의 제어는 특정 상태의 활성화된 제어만 포함하도록 필터링됩니다.

비활성화 탭에는 표준에서 비활성화된 제어 목록이 포함되어 있습니다. 관리자 계정의 경우 비활성화 탭에는 표준에서 비활성화된 제어가 해당 계정 및 모든 구성원 계정에서 포함됩니다.

각 제어에 대해 탭에는 다음 정보가 표시됩니다.

- 제어 상태 (the section called “규정 준수 상태 및 제어 상태” 참조)
- 제어에 할당된 심각도
- 제어 ID 및 제목
- 총 활성 조사 결과 수 중 실패한 활성 조사 결과 수입니다. 해당하는 경우 실패 검사 열에는 알 수 없음 상태인 조사 결과 수도 나열됩니다.

각 탭의 검색 필터 외에도 다음 필드를 기준으로 목록을 정렬할 수 있습니다.

- 규정 준수 상태
- 심각도
- ID
- 제목
- 실패한 검사

열 중 하나를 사용하여 각 목록을 정렬할 수 있습니다. 기본적으로 모두 활성화 탭은 실패한 제어가 목록의 맨 위에 표시되도록 정렬됩니다. 이렇게 하면 수정이 필요한 문제에 즉시 집중할 수 있습니다.

나머지 탭에서는 제어가 기본적으로 심각도에 따라 내림차순으로 정렬됩니다. 즉, 중요 제어가 먼저 적용되고 그 다음으로 높음, 중간, 낮은 심각도 제어가 적용됩니다.

원하는 액세스 방법을 선택한 다음 단계에 따라 활성화된 표준에 사용 가능한 제어를 표시합니다. 이 지침 대신 DescribeStandardsControlAPI 작업을 사용할 수도 있습니다.

Security Hub console

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 보안 표준을 선택합니다.
3. 표준에 대한 결과 보기를 선택합니다. 페이지 하단에는 표준에 적용되는 제어(탭으로 구분)가 나열됩니다.

Security Hub API

1. ListSecurityControlDefinitions를 실행하고 표준 Amazon 리소스 이름(ARN)을 입력하여 해당 표준에 대한 제어 ID 목록을 가져옵니다. 표준 ARN을 가져오려면 DescribeStandards를 실행하십시오. 표준 ARN을 입력하지 않는 경우 이 API는 모든 Security Hub 제어 ID를 반환합니다. 이 API는 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

   요청 예:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. ListStandardsControlAssociations를 실행하여 계정에서 활성화한 각 표준에서 제어가 활성화되어 있는지 확인하십시오.
3. SecurityControlId또는 SecurityControlArn를 입력하여 제어를 식별하십시오. 페이지 매김 파라미터는 선택 사항입니다.

   요청 예:

   ```
   {
       SecurityControlId: Config.1
       NextToken: lkeyusdlk-sdlflsnd-ladfterb
       MaxResults: 5
   }
   ```

AWS CLI

1. list-security-control-definitions 명령을 실행하고 하나 이상의 표준 ARN을 입력하여 제어 ID 목록을 가져옵니다. 표준 ARN을 얻으려면 describe-standards 명령을 실행합니다. 표준 ARN을 입력하지 않는 경우 이 명령은 모든 Security Hub 제어 ID를 반환합니다. 이 명령은 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

   ```
   aws securityhub --region us-east-1 list-security-control-definitions --
   standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
   security-best-practices/v/1.0.0"
   ```

2. list-standards-control-associations 명령을 실행하여 계정에서 활성화한 각 표준에서 제어가 활성화되어 있는지 확인하십시오.

3. security-control-id 또는 security-control-arn를 입력하여 제어를 식별하십시오.

   명령 예:

   ```
   aws securityhub --region us-east-1 list-standards-control-associations --
   security-control-id Config.1
   ```

제어 목록 다운로드

제어 목록의 현재 페이지를 .csv 파일로 다운로드할 수 있습니다.

제어 목록을 필터링한 경우 다운로드한 파일에는 필터 설정과 일치하는 제어만 포함됩니다.

목록에서 특정 제어를 선택한 경우 다운로드한 파일에는 해당 제어만 포함됩니다.

제어 목록의 현재 페이지 또는 현재 선택한 제어를 다운로드하려면 다운로드를 선택합니다.

특정 표준에서의 제어 활성화 및 비활성화

에서 표준을 활성화하면 해당 표준에 적용되는 모든 컨트롤이 해당 표준에서 자동으로 활성화됩니다(단 AWS Security Hub, 서비스 관리 표준은 예외). 그런 다음 표준 내에서 특정 제어를 비활성화하고 다시 활성화할 수 있습니다. 하지만 제어의 활성화 상태를 활성화된 모든 표준에 맞게 조정하는 것이 좋습니다.

> **Note**
>
> Security Hub 중앙 구성을 사용하는 경우 위임된 관리자는 활성화된 모든 표준에서 조직 계정에 대한 제어를 활성화 및 비활성화할 수 있습니다. 제어의 활성화 상태를 표준 전반에 걸쳐 조정하려면 이 방법을 사용하는 것이 좋습니다. 하지만 위임된 관리자는 계정을 자체 관리형으로 지정하여 특정 표준에 따라 제어를 활성화 및 비활성화할 수 있습니다. 자세한 정보는 중앙 구성 작동 방식을 참조하세요.

표준의 세부 정보 페이지에는 표준에 적용할 수 있는 제어 목록과 해당 표준에서 현재 활성화되고 비활성화된 제어에 대한 정보가 포함되어 있습니다.

표준 세부 정보 페이지에서 특정 표준의 제어를 활성화하고 비활성화할 수도 있습니다. 각 AWS 계정 AND에서 컨트롤을 개별적으로 활성화하고 비활성화해야 합니다. AWS 리전제어를 활성화 또는 비활성화하면 현재 계정 및 리전에만 영향을 미칩니다.

Security Hub 콘솔, Security Hub API 또는 를 사용하여 각 지역에서 제어를 활성화하거나 비활성화할 수 AWS CLI있습니다. 집계 영역을 설정한 경우 연결된 모든 리전의 제어가 표시됩니다. 연결된 리전에서는 제어를 사용할 수 있지만 집계 영역에서는 사용할 수 없는 경우, 집계 영역에서 해당 제어를 활성화하거나 비활성화할 수 없습니다. 다중 계정 및 다중 리전 제어 비활성화 스크립트의 경우 다중 계정 환경에서 Security Hub 제어 비활성화를 참조하세요.

특정 표준에서 제어 활성화하기

표준에서 제어를 활성화하려면 먼저 제어가 적용되는 표준을 하나 이상 활성화해야 합니다. 표준 활성화에 대한 자세한 내용은 보안 표준 활성화 및 비활성화을 참조하십시오. 표준에서 컨트롤을 활성화하면 해당 컨트롤에 대한 검색 결과가 AWS Security Hub 생성되기 시작합니다. Security Hub는 전체 보안 점수 및 표준 보안 점수 계산에 제어 상태를 포함합니다. 여러 표준에서 제어를 활성화하더라도 통합 제어 조사 결과를 켜면 표준 전반에 걸쳐 보안 검사당 단일 조사 결과를 받게 됩니다. 자세한 내용은 Consolidated control findings를 참조하세요.

표준에서 제어를 활성화하려면 현재 리전에서 제어를 사용할 수 있어야 합니다. 자세한 내용은 리전별 제어 가용성 섹션을 참조하세요.

다음 단계에 따라 특정 표준에서 Security Hub 제어를 활성화하세요. 다음 단계 대신 `UpdateStandardsControl` API 작업을 사용하여 특정 표준에서 제어를 활성화할 수도 있습니다. 모든 표준에서 제어를 활성화하는 방법에 대한 지침은 단일 계정 및 리전에서 모든 표준의 제어 활성화 섹션을 참조하세요.

Security Hub console

특정 표준에서 제어를 활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 보안 표준을 선택합니다.
3. 관련 표준의 결과 보기를 선택합니다.
4. 제어를 선택합니다.
5. 제어 활성화를 선택합니다(이 옵션은 이미 활성화된 제어에는 표시되지 않습니다). 활성화를 선택하여 확인합니다.

Security Hub API

특정 표준에서 제어를 활성화하려면

1. ListSecurityControlDefinitions를 실행하고 표준 ARN을 입력하여 특정 표준에 사용할 수 있는 제어 목록을 가져옵니다. 표준 ARN을 얻으려면 DescribeStandards를 실행하십시오. 이 API는 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

   요청 예:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. ListStandardsControlAssociations를 실행하고 특정 제어 ID를 입력하여 각 표준에서 제어의 현재 활성화 상태를 반환하십시오.

   요청 예:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. BatchUpdateStandardsControlAssociations를 실행합니다. 제어를 활성화하려는 표준의 ARN을 입력합니다.
4. AssociationStatus 파라미터를 ENABLED와 동일하게 설정합니다.

요청 예:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

특정 표준에서 제어를 활성화하려면

1. list-security-control-definitions 명령을 실행하고 표준 ARN을 입력하여 특정 표준에 사용할 수 있는 제어 목록을 가져옵니다. 표준 ARN을 얻으려면 describe-standards를 실행하십시오. 이 명령은 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. list-standards-control-associations 명령을 실행하고 특정 제어 ID를 제공하여 각 표준에서 제어의 현재 활성화 상태를 반환합니다.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. batch-update-standards-control-associations 명령을 실행합니다. 제어를 활성화하려는 표준의 ARN을 입력합니다.
4. AssociationStatus 파라미터를 ENABLED와 동일하게 설정합니다.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

특정 표준의 제어 비활성화

표준에서 제어를 사용하지 않도록 설정하면 Security Hub는 제어에 대한 조사 결과 생성을 중지합니다. 제어 상태는 표준의 보안 점수를 계산하는 데 더 이상 사용되지 않습니다.

제어를 비활성화하는 한 가지 방법은 제어가 적용되는 모든 표준을 비활성화하는 것입니다. 표준을 비활성화하면 표준에 적용되는 모든 제어가 비활성화됩니다. 그러나 다른 표준에서는 해당 제어가 계속 활성화되어 있을 수 있습니다. 표준 비활성화에 대한 자세한 내용은 the section called “표준 활성화 및 비활성화”을 참조하십시오.

적용되는 표준을 비활성화하여 제어를 비활성화하면 다음과 같은 상황이 발생합니다.

- 해당 표준에 대해서는 제어에 대한 보안 검사가 더 이상 수행되지 않습니다. 즉, 제어 상태는 표준 보안 점수에 영향을 주지 않습니다(Security Hub는 다른 표준에서 활성화된 경우 해당 제어에 대한 보안 검사를 계속 실행합니다).
- 해당 제어에 대해 추가 조사 결과가 생성되지 않습니다.
- 기존 조사 결과는 3-5일 후에 자동으로 보관됩니다(이는 최선의 노력이며 보장되지는 않음).
- Security Hub에서 생성한 관련 AWS Config 규칙이 제거됩니다.

표준을 비활성화하면 Security Hub는 어떤 제어가 비활성화되었는지 추적하지 않습니다. 이후에 표준을 다시 활성화하면 해당 표준에 적용되는 모든 제어가 자동으로 활성화됩니다. 또한 제어 비활성화는 일회성 작업입니다. 제어를 비활성화한 다음 이전에 비활성화했던 표준을 활성화한다고 가정해 보겠습니다. 표준에 해당 제어가 포함되어 있는 경우 해당 표준에서도 해당 제어가 활성화됩니다. Security Hub에서 표준을 활성화하면 해당 표준에 적용되는 모든 제어가 자동으로 활성화됩니다.

적용되는 표준을 비활성화하여 제어를 비활성화하는 대신 하나 이상의 특정 표준에서 제어를 비활성화할 수 있습니다.

결과 노이즈를 줄이려면 환경과 관련이 없는 제어를 비활성화하는 것이 유용할 수 있습니다. 비활성화할 제어에 대한 자세한 내용은 비활성화하면 좋을 Security Hub 제어를 참조하세요.

다음 단계에 따라 특정 표준에서 제어를 비활성화하세요. 다음 단계 대신 `UpdateStandardsControl`API 작업을 사용하여 특정 표준의 제어를 비활성화할 수도 있습니다. 모든 표준에서 제어를 비활성화하는 방법에 대한 지침은 모든 표준에서 제어 활성화 및 비활성화 섹션을 참조하세요.

Security Hub console

특정 표준에서 제어를 비활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 보안 표준을 선택합니다. 관련 표준의 결과 보기를 선택합니다.
3. 제어를 선택합니다.
4. 제어 비활성화를 선택합니다. 이 옵션은 이미 비활성화된 제어에는 나타나지 않습니다.
5. 제어를 비활성화하는 이유를 제공하고 비활성화를 선택하여 확인합니다.

Security Hub API

특정 표준에서 제어를 비활성화하려면

1. ListSecurityControlDefinitions를 실행하고 표준 ARN을 입력하여 특정 표준에 사용할 수 있는 제어 목록을 가져옵니다. 표준 ARN을 얻으려면 DescribeStandards를 실행하십시오. 이 API는 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

   요청 예:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. ListStandardsControlAssociations를 실행하고 특정 제어 ID를 입력하여 각 표준에서 제어의 현재 활성화 상태를 반환하십시오.

   요청 예:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. BatchUpdateStandardsControlAssociations를 실행합니다. 제어를 비활성화하려는 표준의 ARN을 제공합니다.
4. AssociationStatus 파라미터를 DISABLED와 동일하게 설정합니다. 이미 비활성화된 제어에 대해 다음 단계를 수행하면 API가 HTTP 상태 코드 200 응답을 반환합니다.

요청 예:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to
 environment"}]
}
```

AWS CLI

특정 표준에서 제어를 비활성화하려면

1. list-security-control-definitions 명령을 실행하고 표준 ARN을 입력하여 특정 표준에 사용할 수 있는 제어 목록을 가져옵니다. 표준 ARN을 얻으려면 describe-standards를 실행하십시오. 이 명령은 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. list-standards-control-associations 명령을 실행하고 특정 제어 ID를 제공하여 각 표준에서 제어의 현재 활성화 상태를 반환합니다.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. batch-update-standards-control-associations 명령을 실행합니다. 제어를 비활성화하려는 표준의 ARN을 제공합니다.
4. AssociationStatus 파라미터를 DISABLED와 동일하게 설정합니다. 이미 활성화된 제어에 대해 다음 단계를 수행하면 명령은 HTTP 상태 코드 200 응답을 반환합니다.

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Security Hub 제어 참조

이 컨트롤 참조는 사용 가능한 AWS Security Hub 컨트롤 목록과 각 컨트롤에 대한 자세한 정보로 연결되는 링크를 제공합니다. 개요 테이블에는 제어 ID별로 알파벳 순서로 제어가 표시됩니다. Security Hub에서 현재 사용 중인 컨트롤만 여기에 포함됩니다. 사용 중지된 컨트롤은 이 목록에서 제외됩니다. 이 테이블은 각 제어에 대해 다음 정보가 표시됩니다.

- 보안 제어 ID — 이 ID는 여러 표준에 적용되며 제어와 관련된 AWS 서비스 및 리소스를 나타냅니다. Security Hub 콘솔은 계정에서 통합 제어 조사 결과가 켜져 있는지 또는 사용 중지되었는지에 관계없이 보안 제어 ID를 표시합니다. 하지만 Security Hub 조사 결과는 계정에 통합 제어 조사 결과가 설정된 경우에만 보안 제어 ID를 참조합니다. 계정에서 통합 제어 결과가 해제된 경우 일부 제어 ID는 제어 결과의 표준에 따라 다릅니다. 표준별 제어 ID를 보안 제어 ID에 매핑하는 방법은 통합이 제어 ID 및 제목에 미치는 영향 섹션을 참조하세요.

  보안 제어를 위한 자동화를 설정하려는 경우 제목이나 설명보다는 제어 ID를 기준으로 필터링하는 것이 좋습니다. Security Hub는 때때로 제어 기능의 제목이나 설명을 업데이트할 수 있지만 제어 ID는 동일하게 유지됩니다.

  제어 ID는 숫자를 건너뛸 수 있습니다. 이는 향후 제어를 위한 자리표시자입니다.
- 적용 가능한 표준 - 제어가 적용되는 표준을 나타냅니다. 제어를 선택하면 타사 규정 준수 프레임워크의 특정 요구 사항을 확인할 수 있습니다.
- 보안 제어 제목 - 이 제목은 여러 표준에 적용됩니다. Security Hub 콘솔에는 계정에서 통합 제어 조사 결과가 켜져 있는지 또는 사용 중지되었는지에 관계없이 보안 제어 제목이 표시됩니다. 그러나 Security Hub 조사 결과는 계정에 통합 제어 조사 결과가 설정된 경우에만 보안 제어 제목을 참조합니다. 계정에서 통합 제어 결과가 해제된 경우 일부 제어 목록은 제어 결과의 표준에 따라 다릅니다. 표준별 제어 ID를 보안 제어 ID에 매핑하는 방법은 통합이 제어 ID 및 제목에 미치는 영향 섹션을 참조하세요.
- 심각도 - 제어의 심각도는 보안 관점에서 그 중요성을 식별합니다. Security Hub에서 제어 심각도를 결정하는 방법에 대한 자세한 내용은 제어 조사 결과에 심각도 할당을 참조하십시오.
- 일정 유형 - 제어가 평가되는 시기를 나타냅니다. 자세한 정보는 보안 검사 실행 예약을 참조하세요.
- 사용자 지정 파라미터 지원 - 제어가 하나 이상의 파라미터에 대한 사용자 지정 값을 지원하는지 여부를 나타냅니다. 제어를 선택하면 파라미터 세부 정보를 볼 수 있습니다. 자세한 정보는 사용자 지정 제어 파라미터을 참조하세요.

제어를 선택하면 추가 세부 정보를 볼 수 있습니다. 제어는 서비스 이름의 알파벳순으로 나열됩니다.

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
Account.1	다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	주기적
Account.2	AWS 계정 조직의 AWS Organizations 일원이어야 합니다.	NIST SP 800-53 개정 5	높음	 아니요	주기적
ACM.1	가져온 인증서 및 ACM 발행 인증서는 지정된 기간 후 갱신해야 합니다	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 예	변경이 트리거되고 주기적입니다.
ACM.2	ACM에서 관리하는 RSA 인증서는 2,048비트 이상의 키 길이를 사용해야 합니다	AWS 기본 보안 모범 사례 v1.0.0	높음	 아니요	변경이 트리거됨
ACM.3	ACM 인증서에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
APIGateway.1	API Gateway WebSocket REST 및 API 실행 로깅을 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
APIGateway.2	API Gateway REST API 단계는 백엔드 인증에 SSL 인증서를 사용하도록 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
APIGateway.3	API Gateway REST API 스테이지에는 AWS X-Ray 추적 기능이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
APIGateway.4	API Gateway는 WAF 웹 ACL과 연결되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
APIGateway.5	API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
APIGateway.8	API Gateway 경로에는 권한 부여 유형을 지정해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 예	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
APIGateway.9	API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
AppSync.2	AWS AppSync 필드 수준 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0	중간	 너	변경이 트리거됨
AppSync4.	AWS AppSync GraphQL API는 태그가 지정되어야 합니다	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
AppSync5.	AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 아니요	변경이 트리거됨
아테나.2	Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
아테나.3	Athena 워크그룹에 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
AutoScaling1.	로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 수정 버전 5	낮음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
AutoScaling2. 2.	Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포함해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 여	변경이 트리거됨
AutoScaling3.	Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
Autoscaling.5	Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
AutoScaling6.6.	Auto Scaling 그룹은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
AutoScaling9.9.	EC2 Auto Scaling 그룹은 EC2 시작 템플릿을 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
AutoScaling1.0	EC2 Auto Scaling 그룹에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
Backup.1	AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
백업.2	AWS Backup 복구 지점에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
백업.3	AWS Backup 저장소에 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
백업.4	AWS Backup 보고서 계획에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
백업.5	AWS Backup 백업 계획에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
CloudFormation2.	CloudFormation 스택에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	 예	변경이 트리거됨
CloudFront.1.	CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
CloudFront.3.	CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
CloudFront.4.	CloudFront 배포판에는 오리진 페일오버가 구성되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	낮음	 아니요	변경이 트리거됨
CloudFront.5.	CloudFront 배포판에는 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
CloudFront.6.	CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
CloudFront.7	CloudFront 배포판에서는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
CloudFront.8.	CloudFront 배포판은 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	낮음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
CloudFront.9	CloudFront 배포판은 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
CloudFront.10	CloudFront 배포판은 엣지 로케이션과 커스텀 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
CloudFront.2	CloudFront 배포판은 존재하지 않는 S3 오리진을 가리키면 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 아니요	주기적
CloudFront.13	CloudFront 배포판은 원본 액세스 제어를 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0	중간	 아니요	변경이 트리거됨
CloudFront.4	CloudFront 배포판에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
CloudTrail.1.	CloudTrail 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 멀티 리전 트레일로 활성화하고 구성해야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, CIS AWS 재단 벤치마크 v1.4.0, 기본 보안 모범 사례 v1.0.0, 서비스 AWS 관리형 표준:, NIST SP 800-53 개정 5 AWS Control Tower	높음	 아니요	주기적
CloudTrail.2.	CloudTrail 저장 중 암호화가 활성화되어 있어야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, PCI DSS v3.2.1, CIS AWS 재단 벤치마크 v1.4.0, NIST SP AWS Control Tower 800-53 개정판 5 AWS	중간	 아니요	주기적
CloudTrail.3.	하나 이상의 CloudTrail 트레일을 활성화해야 합니다.	PCI DSS v3.2.1	높음	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
CloudTrail.4.	CloudTrail 로그 파일 검증이 활성화되어야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, PCI DSS v3.2.1, CIS AWS 재단 벤치마크 v1.4.0, NIST AWS Control Tower SP 800-53 개정판 5 AWS	낮음	 아니요	주기적
CloudTrail.5.	CloudTrail 트레일은 Amazon CloudWatch Logs와 통합되어야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, 기본 보안 모범 사례 v1.0.0, 서비스 AWS 관리형 표준:, PCI DSS v3.2.1, CIS 재단 벤치마크 v1.4.0, NIST SP AWS Control Tower 800-53 개정 5 AWS	낮음	 아니요	주기적
CloudTrail.6	CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하십시오.	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	심각	 아니요	변경이 트리거되고 주기적입니다.
CloudTrail.7.	S3 버킷에서 S3 버킷 액세스 로깅이 활성화되었는지 확인합니다. CloudTrail	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
CloudTrail.9.	CloudTrail 트레일에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
CloudWatch1.	루트 사용자 사용을 위한 로그 지표 필터 및 경보가 있는지 확인합니다.	CIS AWS 재단 벤치마크 v1.2.0, PCI DSS v3.2.1, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.2.	무단 API 직접 호출에 대해 로그 지표 필터와 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0	낮음	 아니요	주기적
CloudWatch3.	MFA 없는 Management Console 로그인에 대해 로그 지표 필터 및 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0	낮음	 아니요	주기적
CloudWatch4.	IAM 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.5.	CloudTrail 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
CloudWatch.6.	AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.7.	고객이 생성한 CMK의 비활성화 또는 예약된 삭제에 대해 로그 지표 필터 및 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.8	S3 버킷 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.9.	AWS Config 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.10	보안 그룹 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.11	네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
CloudWatch.12	네트워크 게이트웨이 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.13	라우팅 테이블 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.14	VPC 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적
CloudWatch.15	CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.	NIST SP 800-53 개정 5	높음	 예	변경이 트리거됨
CloudWatch.16	CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.	NIST SP 800-53 개정 5	중간	 예	주기적
CloudWatch.17	CloudWatch 알람 동작을 활성화해야 합니다.	NIST SP 800-53 개정 5	높음	 아니요	변경이 트리거됨
CodeArtifact1.	CodeArtifact 리포지토리에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	 예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
CodeBuild.1.	CodeBuild 비트버킷 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 개정판 AWS Control Tower 5	심각	 아니요	변경이 트리거됨
CodeBuild.2.	CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 개정판 5	심각	 아니요	변경이 트리거됨
CodeBuild.3.	CodeBuild S3 로그는 암호화되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
CodeBuild.4.	CodeBuild 프로젝트 환경에는 로깅 구성이 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
Config.1	AWS Config 서비스 연결 역할을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.	CIS AWS 재단 벤치마크 v1.4.0, CIS AWS 재단 벤치마크 v1.2.0, 기본 보안 모범 사례, NIST SP 800-53 개정판 5, AWS PCI DSS v3.2.1	중간	 아니요	주기적
DataFirehose.1.	Firehose 전송 스트림은 저장 시 암호화해야 합니다.	AWS 기본 보안 모범 사례 NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
형사.1	Detective 행동 그래프에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
DMS.1	Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 AWS Control Tower개정판 5	심각	 아니요	주기적
DMS.2	DMS 인증서에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
DMS.3	DMS 이벤트 구독에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
DMS.4	DMS 복제 인스턴스에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
DMS.5	DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
DMS.6	DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
DMS.7	대상 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
DMS.8	소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
DMS.9	DMS 엔드포인트는 SSL을 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
DMS.10	Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
DMS.11	MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
DMS.12	Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
DocumentDB.1	Amazon DocumentDB 클러스터는 저장 시 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	중간	 아니요	변경이 트리거됨
DocumentDB.2	Amazon DocumentDB 클러스터는 적절한 백업 보존 기간을 가져야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	중간	 예	변경이 트리거됨
DocumentDB.3	Amazon DocumentDB 수동 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	심각	 아니요	변경이 트리거됨
DocumentDB.4	Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
DocumentDB.5	Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
DynamoDB.1	DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 예	주기적
DynamoDB.2	DynamoDB 테이블에는 복구가 활성화되어 있어야 합니다. point-in-time	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
DynamoDB.3	DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
DynamoDB.4	DynamoDB 테이블은 백업 계획에 있어야 합니다.	NIST SP 800-53 개정 5	중간	 네	주기적
다이나모드 B.5	DynamoDB 테이블에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
DynamoDB 6	DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
다이나모드 B.7	DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
EC2.1	EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 개정 5 AWS Control Tower	심각	 아니요	주기적
EC2.2	VPC 기본 보안 그룹은 인바운드 또는 아웃바운드 트래픽을 허용하지 않아야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, 기본 보안 모범 사례 v1.0.0, 서비스 AWS 관리형 표준:, PCI DSS v3.2.1, CIS 재단 벤치마크 v1.4.0, NIST SP 800-53 개정판 5 AWS Control Tower AWS	높음	 아니요	변경이 트리거됨
EC2.3	연결된 EBS 볼륨은 저장 시 암호화되어야 되어야 합니다.	AWS 기본 보안 모범 사례 AWS Control Tower v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EC2.4	중지된 EC2 인스턴스는 지정된 기간 후에 제거해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 예	주기적
EC2.6	VPC 흐름 로깅은 모든 VPC에서 활성화되어야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, PCI DSS v3.2.1, CIS AWS 재단 벤치마크 v1.4.0, NIST AWS Control Tower SP 800-53 개정판 5 AWS	중간	 아니요	주기적
EC2.7	EBS 기본 암호화를 활성화해야 합니다.	AWS 기본 보안 모범 사례 AWS Control Tower v1.0.0, AWS 서비스 관리형 표준:, CIS 재단 벤치마크 v1.4.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
EC2.8	EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EC2.9	EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
EC2.10	Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	주기적
EC2.12	사용하지 않는 EC2 EIP를 제거해야 합니다.	PCI DSS v3.2.1, NIST SP 800-53 개정 5	낮음	 아니요	변경이 트리거됨
EC2.13	보안 그룹은 0.0.0.0/0 또는: :/0에서 포트 22로의 수신을 허용해서는 안 됩니다.	CIS AWS 파운데이션 벤치마크 v1.2.0, PCI DSS v3.2.1, NIST SP 800-53 개정판 5	높음	 아니요	변경이 트리거됨
EC2.14	보안 그룹은 0.0.0.0/0 또는: :/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.	AWS CIS 재단 벤치마크 v1.2.0	높음	 아니요	변경이 트리거됨
EC2.15	EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EC2.16	사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
EC2.17	EC2 인스턴스는 ENI를 여러 개 사용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
EC2.18	보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 여	변경이 트리거됨
EC2.19	보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	심각	 아니요	변경이 트리거됨
EC2.20	AWS 사이트-사이트 간 VPN 연결을 위한 두 VPN 터널이 모두 작동 상태여야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EC2.21	네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, CIS 재단 벤치마크 v1.4.0, NIST SP 800-53 수정 버전 5 AWS Control Tower AWS	중간	 아니요	변경이 트리거됨
EC2.22	사용되지 않는 EC2 보안 그룹은 제거해야 합니다.	서비스 관리형 표준: AWS Control Tower	중간	 아니요	주기적
EC2.23	EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 아니요	변경이 트리거됨
EC2.24	EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
EC2.25	EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
EC2.28	EBS 볼륨은 백업 계획에 포함되어야 합니다.	NIST SP 800-53 개정 5	낮음	 예	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EC2.33	EC2 트랜짓 게이트웨이 첨부 파일에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.34	EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.35	EC2 네트워크 인터페이스는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.36	EC2 고객 게이트웨이는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.37	EC2 엘라스틱 IP 주소는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.38	EC2 인스턴스는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.39	EC2 인터넷 게이트웨이는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.40	EC2 NAT 게이트웨이는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EC2.41	EC2 네트워크 ACL에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.42	EC2 라우팅 테이블에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.43	EC2 보안 그룹에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.44	EC2 서브넷은 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.45	EC2 볼륨에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.46	Amazon VPC에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.47	Amazon VPC 엔드포인트 서비스는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.48	Amazon VPC 흐름 로그에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.49	Amazon VPC 피어링 연결에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EC2.50	EC2 VPN 게이트웨이는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.51	EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	낮음	 아니요	변경이 트리거됨
EC2.52	EC2 트랜짓 게이트웨이는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EC2.53	EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.	AWS CIS 재단 벤치마크 v3.0.0	높음	 아니요	주기적
EC2.54	EC2 보안 그룹은: :/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.	CIS 재단 벤치마크 v3.0.0 AWS	높음	 아니요	주기적
ECR.1	ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	높음	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
ECR.2	ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ECR.3	ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ECR.4	ECR 퍼블릭 리포지토리에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
ECS.1	Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
ECS.2	ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
ECS.3	ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
ECS.4	ECS 컨테이너는 권한이 없는 상태로 실행되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
ECS.5	ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
EC.8	암호는은 컨테이너 환경 변수로 전달되어서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
ECS.9	ECS 작업 정의에는 로깅 구성이 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 아니요	변경이 트리거됨
ECS.10	ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
ECS.12	ECS 클러스터는 Container Insights를 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ECS.13	ECS 서비스는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
ECS.14	ECS 클러스터에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
ECS.15	ECS 작업 정의에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EFS.1	다음을 사용하여 저장 중인 파일 데이터를 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	주기적
EFS.2	Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	주기적
EFS.3	EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EFS.4	EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
EFS.5	EFS 액세스 포인트는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	 0	변경이 트리거됨
EFS.6	EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.	AWS 기본 보안 모범 사례	중간	 아니요	주기적
EKS.1	EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 아니요	주기적
EKS.2	EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
EKS.3	EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EKS.6	EKS 클러스터에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EKS.7	EKS ID 공급자 구성에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EKS.8	EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
ElastiCache1.	ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 너	주기적
ElastiCache2.	ElastiCache Redis 캐시 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 아니요	주기적
ElastiCache.3.	ElastiCache 복제 그룹에는 자동 페일오버가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
ElastiCache4.	ElastiCache 복제 그룹이 활성화되어 있어야 encryption-at-rest 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
ElastiCache.5.	ElastiCache 복제 그룹이 활성화되어 있어야 encryption-in-transit 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
ElastiCache.6.	ElastiCache 이전 Redis 버전의 복제 그룹에는 Redis 인증이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
ElastiCache7.7	ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 아니요	주기적
ElasticBeanstalk1.	Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
ElasticBeanstalk.2.	Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	높음	 예	변경이 트리거됨
ElasticBeanstalk3.	Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch	AWS 기본 보안 모범 사례 v1.0.0	높음	 네	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
ELB.1	Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 개정판 5.	중간	 아니요	주기적
ELB.2	SSL/HTTPS 리스너가 있는 Classic Load Balancer는 AWS Certificate Manager에서 제공하는 인증서를 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ELB.3	Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ELB.4	http 헤더를 삭제하도록 Application Load Balancer를 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ELB.5	Application 및 Classic Load Balancer 로깅이 활성화되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
ELB.6	애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준: AWS Control Tower, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
ELB.7	Classic Load Balancer connection draining 레이닝이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ELB.8	SSL 리스너가 있는 Classic Load Balancer는 강력한 구성이 있는 사전 정의된 보안 정책을 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ELB.9	Classic Load Balancer에서 교차 영역 로드 밸런싱을 사용 설정해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ELB.10	Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
ELB.12	Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기 완화 모드로 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ELB.13	애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 예	변경이 트리거됨
ELB.14	Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ELB.16	애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF	NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
EMR.1	Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EMR.2	Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	심각	 아니요	주기적
ES.1	Elasticsearch 도메인에서 저장 시 암호화를 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	주기적
ES.2	Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 수정 버전 5 AWS Control Tower	심각	 아니요	주기적
ES.3	Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ES.4	로그에 대한 CloudWatch Elasticsearch 도메인 오류 로깅을 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
ES.5	Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ES.6	ElasticSearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ES.7	Elasticsearch 도메인은 최소 세 개의 전용 마스터 노드로 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ES.8	Elasticsearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
ES.9	엘라스틱서치 도메인은 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
EventBridge2.	EventBridge 이벤트 버스는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
EventBridge3.	EventBridge 커스텀 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	낮음	 아니요	변경이 트리거됨
EventBridge4.	EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.	NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
FSx.1	FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	낮음	 아니요	변경이 트리거됨
FSx.2	FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 수정 버전 5	낮음	 아니요	변경이 트리거됨
접착제.1	AWS Glue 작업에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
GlobalAccelerator1.	글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
GuardDuty 1.	GuardDuty 활성화되어야 합니다	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 수정 버전 5	높음	 아니요	주기적
GuardDuty .2.	GuardDuty 필터에 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
GuardDuty 3.	GuardDuty IPset에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
GuardDuty 4.	GuardDuty 감지기에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
IAM.1	IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.	CIS AWS 재단 벤치마크 v1.2.0, 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, PCI DSS v3.2.1, CIS AWS 재단 벤치마크 v1.4.0, NIST SP AWS Control Tower 800-53 개정 5 AWS	높음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
IAM.2	IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.	CIS AWS 재단 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준: AWS Control Tower, PCI DSS v3.2.1, NIST SP 800-53 개정판 5	낮음	 아니요	변경이 트리거됨
IAM.3	IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, CIS 재단 벤치마크 v1.4.0, NIST SP 800-53 개정 5 AWS AWS Control Tower AWS	중간	 아니요	주기적
IAM.4	IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준: AWS Control Tower, PCI DSS v3.2.1, CIS AWS 재단 벤치마크 v1.4.0, NIST SP 800-53 개정판 5	심각	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
IAM.5	콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준: AWS Control Tower, CIS AWS 재단 벤치마크 v1.4.0, NIST SP 800-53 개정판 5	중간	 아니요	주기적
IAM.6	루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준: AWS Control Tower, PCI DSS v3.2.1, CIS AWS 재단 벤치마크 v1.4.0, NIST SP 800-53 개정판 5	심각	 아니요	주기적
IAM.7	IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.	AWS 기본 보안 모범 사례 AWS Control Tower v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5	중간	 예	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
IAM.8	사용하지 않은 IAM 사용자 보안 인증은 제거해야 합니다.	CIS AWS 재단 벤치마크 v1.2.0, 기본 보안 모범 사례 v1.0.0, AWS 서비스 관리 표준:, PCI DSS v3.2.1, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	주기적
IAM.9	루트 사용자에 대해 MFA를 활성화해야 합니다.	CIS 재단 벤치마크 v1.2.0, PCI DSS v3.2.1, CIS 재단 벤치마크 v1.4.0, NIST SP 800-53 개정판 5 AWS AWS	심각	 아니요	주기적
IAM.10	IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.	PCI DSS v3.2.1	중간	 아니요	주기적
IAM.11	IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.	CIS AWS 파운데이션 벤치마크 v1.2.0	중간	 아니요	주기적
IAM.12	IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.	CIS 재단 벤치마크 v1.2.0 AWS	중간	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
IAM.13	IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.	CIS 재단 벤치마크 v1.2.0 AWS	중간	 아니요	주기적
IAM.14	IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.	CIS 재단 벤치마크 v1.2.0 AWS	중간	 아니요	주기적
IAM.15	IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	중간	 아니요	주기적
IAM.16	IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.	CIS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS AWS	낮음	 아니요	주기적
IAM.17	IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.	CIS AWS 재단 벤치마크 v1.2.0	낮음	 아니요	주기적
IAM.18	다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support	CIS AWS 재단 벤치마크 v1.2.0, CIS 재단 벤치마크 v1.4.0 AWS	낮음	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
IAM.19	모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.	PCI DSS v3.2.1, NIST SP 800-53 개정 5	중간	 아니요	주기적
IAM.21	생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
IAM.22	45일 동안 사용하지 않은 IAM 사용자 보안 인증은 제거해야 합니다.	AWS CIS 재단 벤치마크 v1.4.0	중간	 아니요	주기적
IAM.23	IAM 액세스 분석기 분석기는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	 예	변경이 트리거됨
IAM.24	IAM 역할에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	 예	변경이 트리거됨
IAM.25	IAM 사용자는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	 예	변경이 트리거됨
IAM.26	IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.	AWS CIS 재단 벤치마크 v3.0.0	중간	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
IAM.27	IAM ID에는 정책이 첨부되어 있지 않아야 합니다. AWSCloudShellFullAccess	CIS AWS 재단 벤치마크 v3.0.0	중간	 아니요	변경이 트리거됨
IAM.28	IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.	CIS 재단 벤치마크 v3.0.0 AWS	높음	 아니요	주기적
IoT.1	AWS IoT Core 보안 프로필에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
IoT.2	AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
IoT.3	AWS IoT Core 치수에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
IoT.4	AWS IoT Core 승인자는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
IoT.5	AWS IoT Core 역할 별칭에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
IoT.6	AWS IoT Core 정책에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
Kinesis.1	Kinesis 스트림은 저장 시 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
중국어.2	Kinesis 스트림에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
KMS.1	IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
KMS.2	IAM 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
KMS.3	AWS KMS keys 실수로 삭제해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	심각	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
KMS.4	AWS KMS key 순환이 활성화되어야 합니다.	CIS AWS 파운데이션 벤치마크 v1.2.0, PCI DSS v3.2.1, CIS 파운데이션 벤치마크 v1.4.0, NIST SP 800-53 AWS 개정판 5	중간	 아니요	주기적
Lambda.1	Lambda 함수는 퍼블릭 액세스를 금지해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 개정판 5 AWS Control Tower	심각	 아니요	변경이 트리거됨
Lambda.2	Lambda 함수는 최신 런타임을 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Lambda.3	Lambda 함수는 VPC에 있어야 합니다.	PCI DSS v3.2.1, NIST SP 800-53 개정 5	낮음	 아니요	변경이 트리거됨
Lambda.5	VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
람다.6	Lambda 함수는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
Macie.1	Amazon Macie를 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
메이시.2	Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	높음	 아니요	주기적
MSK.1	MSK 클러스터는 브로커 노드 간에 전송되는 동안 암호화되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
MSK.2	MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.	NIST SP 800-53 개정 5	낮음	 아니요	변경이 트리거됨
MQ.2	ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch	AWS 기본 보안 모범 사례, NIST SP 800-53 개정판 5	중간	 아니요	변경이 트리거됨
MQ.3	Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5	낮음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
MQ.4	Amazon MQ 브로커에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
MQ.5	ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.	NIST SP 800-53 개정판 5, 서비스 관리형 표준: AWS Control Tower	낮음	 아니요	변경이 트리거됨
MQ.6	RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다.	NIST SP 800-53 개정판 5, 서비스 관리형 표준: AWS Control Tower	낮음	 아니요	변경이 트리거됨
Neptune.1	Neptune DB 클러스터는 저장 시 암호화되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	중간	 아니요	변경이 트리거됨
Neptune.2	Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	중간	 아니요	변경이 트리거됨
Neptune.3	Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	심각	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
Neptune.4	Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	낮음	 아니요	변경이 트리거됨
Neptune.5	Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	중간	 예	변경이 트리거됨
Neptune.6	Neptune DB 클러스터 스냅샷은 저장 시 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	중간	 아니요	변경이 트리거됨
Neptune.7	Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	중간	 아니요	변경이 트리거됨
Neptune.8	태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	낮음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
Neptune.9	Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.	NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
NetworkFirewall1..	Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.	NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
NetworkFirewall2.	Network Firewall 로깅을 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
NetworkFirewall.3.	Network Firewall 정책에는 적어도 하나의 규칙 그룹이 연결되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
NetworkFirewall4.	네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
NetworkFirewall.5.	네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
NetworkFirewall6.6.	상태 비저장 네트워크 방화벽 규칙 그룹은 비워둘 수 없습니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
NetworkFirewall7.7.	Network Firewall 방화벽에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
NetworkFirewall.8.	Network Firewall 방화벽 정책에 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
NetworkFirewall9.	Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
Opensearch.1	OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
Opensearch.2	OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 수정 버전 5	심각	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
Opensearch.3	OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Opensearch.4	OpenSearch 로그에 대한 CloudWatch 도메인 오류 로깅을 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Opensearch.5	OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Opensearch.6	OpenSearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Opensearch.7	OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
Opensearch.8	도메인 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다. OpenSearch	AWS 기본 보안 모범 사례, 서비스 관리 표준: AWS Control Tower, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
오픈서치.9	OpenSearch 도메인은 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
Opensearch.10	OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	낮음	 아니요	변경이 트리거됨
오픈서치.11	OpenSearch 도메인에는 최소 3개의 전용 기본 노드가 있어야 합니다.	NIST SP 800-53 개정 5	중간	 아니요	주기적
PCA.1	AWS Private CA 루트 인증 기관을 비활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	낮음	 아니요	주기적
RDS.1	RDS 스냅샷은 비공개 상태여야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 개정판 5 AWS Control Tower	심각	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
RDS.2	RDS DB 인스턴스는 구성에 따라 퍼블릭 PubliclyAccessible 액세스를 금지해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 수정 버전 AWS Control Tower 5	심각	 아니요	변경이 트리거됨
RDS.3	RDS DB 인스턴스에서 저장 시 암호화를 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, CIS 재단 벤치마크 v1.4.0, NIST SP 800-53 수정 버전 5 AWS Control Tower AWS	중간	 아니요	변경이 트리거됨
RDS.4	RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
RDS.5	RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
RDS.6	RDS DB 인스턴스에 대해 향상된 모니터링을 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 0	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
RDS.7	RDS 클러스터에는 삭제 보호 기능이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	낮음	 아니요	변경이 트리거됨
RDS.8	RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
RDS.9	RDS DB 인스턴스는 로그를 CloudWatch 로그에 게시해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
RDS.10	RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
RDS.11	RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
RDS.12	RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
RDS.13	RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
RDS.14	Amazon Aurora 클러스터에는 백트래킹이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 너	변경이 트리거됨
RDS.15	RDS DB 클러스터는 여러 가용 영역에 맞게 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
RDS.16	태그를 스냅샷에 복사하도록 RDS DB 클러스터를 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5	낮음	 아니요	변경이 트리거됨
RDS.17	태그를 스냅샷에 복사하도록 RDS DB 인스턴스를 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
RDS.18	RDS 인스턴스는 VPC에 배포해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
RDS.19	기존 RDS 이벤트 알림 구독은 중요 클러스터 이벤트에 맞게 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
RDS.20	기존 RDS 이벤트 알림 구독은 중요한 데이터베이스 인스턴스 이벤트에 맞게 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
RDS.21	중요한 데이터베이스 파라미터 그룹 이벤트에 대해서는 RDS 이벤트 알림 구독을 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
RDS.22	중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
RDS.23	RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
RDS.24	RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
RDS.25	RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
RDS.26	RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.	NIST SP 800-53 개정 5	중간	 예	주기적
RDS.27	RDS DB 클러스터는 저장 시 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5, 서비스 관리형 표준: AWS Control Tower	중간	 아니요	변경이 트리거됨
RDS.28	RDS DB 클러스터에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
RDS.29	RDS DB 클러스터 스냅샷에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
RDS.30	RDS DB 인스턴스에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
RDS.31	RDS DB 보안 그룹에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
RDS.32	RDS DB 스냅샷에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
RDS.33	RDS DB 서브넷 그룹에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
RDS.34	Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
RDS.35	RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
Redshift.1	Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 개정판 5 AWS Control Tower	심각	 아니요	변경이 트리거됨
Redshift.2	Amazon Redshift 클러스터에 대한 연결은 전송 중에 암호화되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Redshift.3	Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 너	변경이 트리거됨
Redshift.4	Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Redshift.6	Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
Redshift.7	Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Redshift.8	Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Redshift.9	Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
Redshift.10	Redshift 클러스터는 저장 시 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
레드시프트.11	Redshift 클러스터에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
레드시프트.12	Redshift 이벤트 구독 알림은 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
레드시프트.13	Redshift 클러스터 스냅샷에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
레드시프트.14	Redshift 클러스터 서브넷 그룹에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
레드시프트.15	Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.	AWS 기본 보안 모범 사례	높음	 아니요	주기적
루트 53.1	Route 53 상태 확인에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
Route53.2	Route 53 퍼블릭 호스팅 영역은 DNS 쿼리를 기록해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
S3.1	S3 범용 버킷에는 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준:, PCI DSS v3.2.1 AWS Control Tower, AWS CIS 파운데이션 벤치마크 v1.4.0, NIST SP 800-53 개정판 5	중간	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
S3.2	S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 수정 버전 5	심각	 아니요	변경이 트리거되고 주기적입니다.
S3.3	S3 범용 버킷은 퍼블릭 쓰기 액세스를 차단해야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 수정 버전 5	심각	 아니요	변경이 트리거되고 주기적입니다.
S3.5	S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준:, PCI DSS v3.2.1 AWS Control Tower, AWS CIS 파운데이션 벤치마크 v1.4.0, NIST SP 800-53 개정판 5	중간	 아니요	변경이 트리거됨
S3.6	S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정	AWS 기본 보안 모범 사례, 서비스 관리형 표준: AWS Control Tower, NIST SP 800-53 수정 버전 5	높음	 아니요	변경이 트리거됨
S3.7	S3 범용 버킷은 지역 간 복제를 사용해야 합니다.	PCI DSS v3.2.1, NIST SP 800-53 개정 5	낮음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
S3.8	S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리 표준:, CIS AWS 재단 벤치마크 v1.4.0 AWS Control Tower, NIST SP 800-53 수정 버전 5	높음	 아니요	변경이 트리거됨
S3.9	S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준: AWS Control Tower, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
S3.10	버전 관리가 활성화된 S3 범용 버킷은 수명 주기 구성을 가져야 합니다.	NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
S3.11	S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.	NIST SP 800-53 개정 5	중간	 예	변경이 트리거됨
S3.12	ACL은 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 됩니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
S3.13	S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.	AWS 기본 보안 모범 사례, 서비스 관리형 표준: AWS Control Tower, NIST SP 800-53 수정 버전 5	낮음	 예	변경이 트리거됨
S3.14	S3 범용 버킷에는 버전 관리가 활성화되어 있어야 합니다.	NIST SP 800-53 개정 5	낮음	 아니요	변경이 트리거됨
S3.15	S3 범용 버킷에는 오브젝트 잠금이 활성화되어 있어야 합니다.	NIST SP 800-53 개정 5	중간	 예	변경이 트리거됨
S3.17	S3 범용 버킷은 저장 시 다음과 같이 암호화해야 합니다. AWS KMS keys	서비스 매니지드 표준: AWS Control Tower, NIST SP 800-53 개정판 5	중간	 아니요	변경이 트리거됨
S3.19	S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 수정 버전 5	심각	 아니요	변경이 트리거됨
S3.20	S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.	CIS AWS 재단 벤치마크 v1.4.0, NIST SP 800-53 개정판 5	낮음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
S3.22	S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.	CIS 파운데이션 벤치마크 v3.0.0 AWS	중간	 아니요	주기적
S3.23	S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.	CIS 파운데이션 벤치마크 v3.0.0 AWS	중간	 아니요	주기적
SageMaker.1.	Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 수정 버전 5	높음	 아니요	주기적
SageMaker.2.	SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
SageMaker.3.	사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
SageMaker 4.	SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
SecretsManager1.	Secrets Manager 비밀 번호에는 자동 로테이션이 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 예	변경이 트리거됨
SecretsManager2.	자동 교체로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
SecretsManager.3.	사용하지 않는 Secrets Manager 암호를 제거합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 예	주기적
SecretsManager4.	Secrets Manager 암호는 지정된 일수 내에 교체되어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 예	주기적
SecretsManager5.	Secrets Manager 비밀에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
ServiceCatalog1.	Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS	AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5	높음	 아니요	주기적
SES.1	SES 연락처 목록에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
SES.2	SES 구성 세트는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
SNS.1	SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS	NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
SNS.3	SNS 주제에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
SQS.1	Amazon SQS 대기열은 저장 시 암호화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
SQS.2	SQS 대기열에는 태그가 지정되어야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
SSM.1	EC2 인스턴스는 다음으로 관리해야 합니다. AWS Systems Manager	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 AWS Control Tower수정 버전 5	중간	 아니요	변경이 트리거됨
SSM.2	Systems Manager가 관리하는 EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 수정 버전 5 AWS Control Tower	높음	 아니요	변경이 트리거됨
SSM.3	Systems Manager에서 관리하는 EC2 인스턴스의 연결 규정 준수 상태는 COMPLIANT여야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, PCI DSS v3.2.1, NIST SP 800-53 수정 버전 5 AWS Control Tower	낮음	 아니요	변경이 트리거됨
SSM.4	SSM 문서는 공개해서는 안 됩니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5 AWS Control Tower	심각	 아니요	주기적
StepFunctions1..	Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.	AWS 기본 보안 모범 사례	중간	 0	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
StepFunctions2.	Step Functions 활동에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
전송.1	Transfer Family 워크플로에는 태그를 지정해야 합니다.	AWS 리소스 태깅 표준	낮음	예	변경이 트리거됨
전송.2	Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.	AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5	중간	 아니요	주기적
WAF.1	AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	주기적
WAF.2	AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
WAF.3	AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정판 5 AWS Control Tower	중간	 아니요	변경이 트리거됨

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
WAF.4	AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 개정 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
WAF.6	AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5	중간	 아니요	변경이 트리거됨
WAF.7	AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
WAF.8	AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨
WAF.10	AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, 서비스 관리형 표준:, NIST SP 800-53 수정 버전 5 AWS Control Tower	중간	 아니요	변경이 트리거됨
WAF.11	AWS WAF 웹 ACL 로깅을 활성화해야 합니다.	NIST SP 800-53 개정 5	낮음	 아니요	주기적

보안 제어 ID	보안 제어 제목	적용 가능한 표준	심각도	사용자 지정 파라미터를 지원합니다.	일정 유형
WAF.12	AWS WAF 규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.	AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 수정 버전 5	중간	 아니요	변경이 트리거됨

주제

- AWS 계정 제어:
- AWS Certificate Manager 컨트롤
- Amazon API Gateway 제어
- AWS AppSync 컨트롤
- Amazon Athena 제어
- AWS Backup 제어:
- AWS CloudFormation 컨트롤
- 아마존 CloudFront 컨트롤
- AWS CloudTrail 컨트롤:
- 아마존 CloudWatch 컨트롤
- AWS CodeArtifact 제어:
- AWS CodeBuild 컨트롤
- AWS Config 컨트롤
- Amazon Data Firehose 컨트롤
- 아마존 디텍티브 컨트롤
- AWS Database Migration Service 컨트롤:
- Amazon DocumentDB 제어
- Amazon DynamoDB 제어
- Amazon Elastic Container Registry 제어
- Amazon ECS 제어

- Amazon Elastic Compute Cloud 제어
- Amazon EC2 Auto Scaling 제어
- Amazon EC2 Systems Manager 제어
- Amazon Elastic File System 제어
- Amazon Elastic Kubernetes 서비스 제어
- 아마존 ElastiCache 컨트롤
- AWS Elastic Beanstalk 제어:
- Elastic Load Balancing 제어
- Amazon EMR 제어
- Elasticsearch 제어
- 아마존 EventBridge 컨트롤
- Amazon FSx 제어
- AWS Global Accelerator 컨트롤:
- AWS Glue 컨트롤
- 아마존 GuardDuty 컨트롤
- AWS Identity and Access Management 컨트롤
- AWS IoT 제어:
- Amazon Kinesis 제어
- AWS Key Management Service 컨트롤:
- AWS Lambda 제어:
- Amazon Macie 제어
- Amazon MSK 제어
- Amazon MQ 제어
- Amazon Neptune 제어
- AWS Network Firewall 제어:
- 아마존 OpenSearch 서비스 컨트롤
- AWS Private Certificate Authority 규제:
- Amazon Relational Database Service 제어
- Amazon Redshift 제어

- Amazon Route 53 제어
- Amazon Simple Storage Service 제어
- 아마존 SageMaker 컨트롤
- AWS Secrets Manager 제어:
- AWS Service Catalog 컨트롤
- Amazon 심플 이메일 서비스 컨트롤
- Amazon Simple Notification Service 제어
- Amazon Simple Queue Service 제어
- AWS Step Functions 제어 항목:
- AWS Transfer Family 컨트롤
- AWS WAF 컨트롤

AWS 계정 제어:

이러한 컨트롤은 다음과 관련이 AWS 계정있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정

관련 요구 사항: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `security-account-information-provided`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Web Services(AWS) 계정에 보안 연락처 정보가 있는지 확인합니다. 계정에 대한 보안 연락처 정보가 제공되지 않으면 제어가 실패합니다.

다른 보안 AWS 연락처로 연락이 불가능할 경우 계정 관련 문제에 대해 다른 사람에게 연락할 수 있습니다. 사용자 사용과 관련된 보안 관련 주제에 대해 또는 다른 AWS 서비스 팀에서 알림을 받을 수 있습니다. AWS Support AWS 계정

이제 Security Hub가 와 통합되었습니다

대체 연락처를 AWS 계정보안 연락처로 추가하려면 AWS Billing and Cost Management 사용 설명서의 대체 연락처 추가, 변경 또는 제거를 참조하십시오.

[Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations

범주: 보호 > 보안 액세스 관리 > 액세스 제어

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `account-part-of-organizations`

스케줄 유형: 주기적

파라미터: 없음

이 AWS 계정 컨트롤은 가 관리를 통해 관리되는 조직의 일부인지 확인합니다. AWS Organizations계정이 조직의 일부가 아닌 경우 제어가 실패합니다.

Organizations를 사용하면 워크로드를 확장할 때 환경을 중앙에서 관리할 수 있습니다. AWS특정 보안 요구 사항이 있는 워크로드를 격리하거나 HIPAA 또는 PCI와 같은 프레임워크를 준수하기 위해 여러 개의 AWS 계정 을 사용할 수 있습니다. 조직을 만들면 여러 계정을 단일 단위로 관리하고 계정 액세스, 리소스 AWS 서비스, 지역을 중앙에서 관리할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

새 조직을 만들고 자동으로 조직에 AWS 계정 추가하려면 AWS Organizations 사용 설명서의 조직 만들기를 참조하십시오. 기존 조직에 계정을 추가하려면 AWS Organizations 사용 설명서의 조직에 AWS 계정 가입하도록 초대하기를 참조하십시오.

AWS Certificate Manager 컨트롤

이러한 제어는 ACM 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.

관련 요구 사항: NIST.800-53.r5 SC-28(3), NIST.800-53.r5 SC-7(16)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::ACM::Certificate`

AWS Config 규칙: `acm-certificate-expiration-check`

스케줄 유형: 트리거형 및 주기적 변경

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`daysToExpiration`	ACM 인증서를 갱신해야 하는 기간(일수)	Integer	`14~365`	`30`

이 컨트롤은 AWS Certificate Manager (ACM) 인증서가 지정된 기간 내에 갱신되는지 여부를 확인합니다. 가져온 인증서와 ACM에서 제공하는 인증서를 모두 확인합니다. 인증서가 지정된 기간 내에 갱신되지 않으면 제어가 실패합니다. 갱신 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 30일을 사용합니다.

ACM은 DNS 검증을 사용하는 인증서를 자동으로 갱신할 수 있습니다. 이메일 검증을 사용하는 인증서의 경우 도메인 검증 이메일에 응답해야 합니다. ACM은 사용자가 가져오는 인증서를 자동으로 갱신하지 않습니다. 사용자는 가져온 인증서를 수동으로 갱신해야 합니다.

이제 Security Hub가 와 통합되었습니다

ACM은 Amazon에서 발급한 SSL/TLS 인증서에 대한 관리형 갱신을 제공합니다. 즉, ACM은 인증서를 자동으로 갱신하거나(DNS 검증을 사용하는 경우) 인증서 만료가 가까워지면 이메일 알림을 보냅니다. 이러한 서비스는 퍼블릭 및 프라이빗 ACM 인증서 모두에 대해 제공됩니다.

이메일로 검증된 도메인의 경우

인증서 만료 후 45일이 지나면 ACM은 도메인 소유자에게 각 도메인 이름에 대한 이메일을 보냅니다. 도메인을 검증하고 갱신을 완료하려면 이메일 알림에 응답해야 합니다.

자세한 내용은 AWS Certificate Manager 사용 설명서의 이메일로 검증된 도메인의 갱신을 참조하십시오.

DNS로 검증된 도메인의 경우

ACM은 DNS 검증을 사용하는 인증서를 자동으로 갱신합니다. 만료 60일 전에 ACM은 인증서를 갱신할 수 있는지 확인합니다.

도메인 이름을 검증할 수 없는 경우 ACM은 수동 검증이 필요하다는 알림을 보냅니다. 만료일 45일, 30일, 7일 및 1일 전에 이러한 알림을 보냅니다.

자세한 내용은 AWS Certificate Manager 사용 설명서의 DNS로 검증된 도메일의 갱신을 참조하십시오.

[ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.

범주: 식별 > 인벤토리 > 인벤토리 서비스

심각도: 높음

리소스 유형: `AWS::ACM::Certificate`

AWS Config 규칙: `acm-certificate-rsa-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 사용자가 관리하는 RSA 인증서가 최소 2,048비트의 키 길이를 AWS Certificate Manager 사용하는지 여부를 확인합니다. 키 길이가 2,048비트보다 작으면 제어가 실패합니다.

암호화의 강도는 키 크기와 직접적인 상관관계가 있습니다. 컴퓨팅 성능은 점점 저렴해지고 서버는 점점 더 고급화됨에 따라 AWS 리소스를 보호하려면 최소 2,048비트의 키 길이를 사용하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

ACM에서 발급한 RSA 인증서의 최소 키 길이는 이미 2,048비트입니다. ACM으로 새 RSA 인증서를 발급하는 방법에 대한 지침은 AWS Certificate Manager 사용 설명서의 인증서 발급 및 관리를 참조하십시오.

ACM을 사용하면 키 길이가 더 짧은 인증서를 가져올 수 있지만 이 제어를 통과하려면 최소 2,048비트의 키를 사용해야 합니다. 인증서를 가져온 후에는 키 길이를 변경할 수 없습니다. 대신 키 길이가 2,048비트보다 작은 인증서를 삭제해야 합니다. 인증서를 ACM으로 가져오는 방법에 대한 자세한 내용은 AWS Certificate Manager 사용 설명서의 인증서 가져오기 사전 조건을 참조하십시오.

[ACM.3] ACM 인증서에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::ACM::Certificate`

AWS Config 규칙: `tagged-acm-certificate` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 AWS Certificate Manager (ACM) 인증서에 파라미터에 `requiredTagKeys` 정의된 특정 키가 있는 태그가 있는지 확인합니다. 인증서에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 인증서에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

ACM 인증서에 태그를 추가하려면 사용 설명서의 인증서 태그 지정을 AWS Certificate Manager 참조하십시오.AWS Certificate Manager

Amazon API Gateway 제어

이러한 제어는 API Gateway 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

AWS Config 규칙: `api-gw-execution-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`loggingLevel`	로깅 수준	Enum	`ERROR`, `INFO`	`No default value`

이 컨트롤은 Amazon API Gateway REST 또는 WebSocket API의 모든 단계에서 로깅이 활성화되었는지 여부를 확인합니다. API의 모든 단계에 대해 `loggingLevel`이 `ERROR` 또는 `INFO`가 아니면 제어가 실패합니다. 특정 로그 유형을 활성화해야 함을 나타내는 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 로깅 수준이 `ERROR` 또는 `INFO`인 경우 경과 통과를 생성합니다.

API Gateway WebSocket REST 또는 API 스테이지에는 관련 로그가 활성화되어 있어야 합니다. API Gateway WebSocket REST 및 API 실행 로깅은 API Gateway REST 및 WebSocket API 단계에 대한 요청의 세부 기록을 제공합니다. 단계에는 API 통합 백엔드 응답, Lambda 권한 부여자 응답 및 통합 엔드포인트가 포함됩니다. `requestId` AWS

이제 Security Hub가 와 통합되었습니다

WebSocket REST 및 API 작업에 대한 로깅을 활성화하려면 CloudWatch API Gateway 개발자 안내서의 API Gateway 콘솔을 사용하여 API 로깅 설정을 참조하십시오.

[APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::ApiGateway::Stage`

AWS Config 규칙: `api-gw-ssl-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon API Gateway REST API 단계에 SSL 인증서가 구성되어 있는지 여부를 확인합니다. 백엔드 시스템은 이러한 인증서를 사용하여 들어오는 요청이 API 게이트웨이에서 온 것임을 인증합니다.

API 게이트웨이 REST API 단계는 백엔드 시스템이 API 게이트웨이에서 발생한 요청을 인증할 수 있도록 SSL 인증서로 구성되어야 합니다.

이제 Security Hub가 와 통합되었습니다

API Gateway REST API SSL 인증서를 생성하고 구성하는 방법에 대한 자세한 지침은 API Gateway 개발자 안내서의 백엔드 인증을 위한 SSL 인증서 생성 및 구성을 참조하십시오.

[ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::ApiGateway::Stage`

AWS Config 규칙: `api-gw-xray-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon API Gateway REST API 단계에서 AWS X-Ray 활성 추적이 활성화되었는지 여부를 확인합니다.

X-Ray 활성 추적을 통해 기본 인프라의 성능 변화에 보다 신속하게 대응할 수 있습니다. 성능 변화로 인해 API의 가용성이 떨어질 수 있습니다. X-Ray 활성 추적은 API Gateway REST API 작업 및 연결된 서비스를 통해 전달되는 사용자 요청의 실시간 지표를 제공합니다.

이제 Security Hub가 와 통합되었습니다

API Gateway REST API 작업에 대해 X-Ray 활성 추적을 활성화하는 방법에 대한 자세한 지침은 AWS X-Ray 개발자 안내서의 AWS X-Ray에 대한 Amazon API Gateway 활성 추적 지원을 참조하십시오.

[APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21)

범주: 보호 > 보호 서비스

심각도: 중간

리소스 유형: `AWS::ApiGateway::Stage`

AWS Config 규칙: `api-gw-associated-with-waf`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 API Gateway 단계가 AWS WAF 웹 액세스 제어 목록 (ACL) 을 사용하는지 여부를 확인합니다. AWS WAF 웹 ACL이 REST API Gateway 단계에 연결되지 않은 경우 이 제어가 실패합니다.

AWS WAF 웹 애플리케이션 및 API를 공격으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 이를 통해 사용자 정의 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 집합인 ACL을 구성할 수 있습니다. API Gateway 단계가 AWS WAF 웹 ACL과 연결되어 있는지 확인하여 악의적인 공격으로부터 보호하십시오.

이제 Security Hub가 와 통합되었습니다

API Gateway 콘솔을 사용하여 AWS WAF 리전 웹 ACL을 기존 API Gateway API 단계와 연결하는 방법에 대한 자세한 내용은 API Gateway 개발자 안내서의 API 보호를 위한 사용을 AWS WAF 참조하십시오.

[APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ApiGateway::Stage`

AWS Config 규칙: `api-gw-cache-encrypted` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 캐시가 활성화된 API Gateway REST API 단계의 모든 메서드가 암호화되었는지 여부를 확인합니다. API Gateway REST API 단계의 메서드가 캐시되도록 구성되어 있고 캐시가 암호화되지 않은 경우 제어가 실패합니다. Security Hub는 특정 방법에 대해 캐싱이 활성화된 경우에만 해당 방법의 암호화를 평가합니다.

저장된 데이터를 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. AWS승인되지 않은 사용자의 데이터 액세스를 제한하기 위해 또 다른 액세스 제어 세트를 추가합니다. 예를 들어 데이터를 읽기 전에 해독하려면 API 권한이 필요합니다.

API 게이트웨이 REST API 캐시는 추가 보안 계층을 위해 저장 시 암호화되어야 합니다.

이제 Security Hub가 와 통합되었습니다

단계에 대한 API 캐싱을 구성하려면 API Gateway 개발자 안내서의 Amazon API Gateway 캐싱 활성화를 참조하십시오. 캐시 설정에서 캐시 데이터 암호화를 선택합니다.

[APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::ApiGatewayV2::Route`

AWS Config 규칙: `api-gwv2-authorization-type-configured`

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`authorizationType`	API 경로의 권한 부여 유형	Enum	`AWS_IAM`, `CUSTOM`, `JWT`	기본값 없음

이 제어는 Amazon API Gateway 경로에 인증 유형이 있는지 확인합니다. 인증 유형이 API 게이트웨이 경로에 없으면 제어가 실패합니다. 필요에 따라, 경로가 파라미터에 지정된 인증 유형을 사용하는 경우에만 제어가 전달되도록 하려면 사용자 지정 `authorizationType` 파라미터 값을 제공할 수 있습니다.

API Gateway는 API 액세스 제어 및 관리에 다중 메커니즘을 지원합니다. 인증 유형을 지정하면 API에 대한 액세스를 인증된 사용자 또는 프로세스로만 제한할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

HTTP API에 대한 인증 유형을 설정하려면 API Gateway 개발자 안내서의 API Gateway에서 HTTP API에 대한 액세스 제어 및 관리를 참조하십시오. WebSocket API에 대한 권한 부여 유형을 설정하려면 API Gateway 개발자 안내서의 WebSocket API Gateway에서 API에 대한 액세스 제어 및 관리를 참조하십시오.

[APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::ApiGatewayV2::Stage`

AWS Config 규칙: `api-gwv2-access-logs-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon API Gateway V2 단계에 액세스 로깅이 구성되어 있는지 확인합니다. 액세스 로그 설정이 정의되지 않은 경우 이 제어가 실패합니다.

API Gateway 액세스 로그는 누가 API에 액세스했고 호출자가 API에 어떻게 액세스했는지에 대한 자세한 정보를 제공합니다. 이러한 로그는 보안 및 액세스 감사 및 포렌식 조사와 같은 애플리케이션에 유용합니다. 이러한 액세스 로그를 사용하여 트래픽 패턴을 분석하고 문제를 해결할 수 있습니다.

추가 모범 사례는 API Gateway 개발자 안내서의 REST API 모니터링을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

액세스 로깅을 설정하려면 CloudWatch API Gateway 개발자 안내서의 API Gateway 콘솔을 사용하여 API 로깅 설정을 참조하십시오.

AWS AppSync 컨트롤

이러한 컨트롤은 AWS AppSync 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::AppSync::GraphQLApi`

AWS Config 규칙: `appsync-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
`fieldLoggingLevel`	필드 로깅 수준	Enum	`ERROR`, `ALL`	`No default value`	

이 컨트롤은 AWS AppSync API에 필드 수준 로깅이 켜져 있는지 확인합니다. 필드 리졸버 로그 수준이 없음으로 설정되면 제어가 실패합니다. 특정 로그 유형을 활성화해야 함을 나타내는 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 필드 리졸버 로그 수준이 `ERROR` 또는 `ALL`인 경우 결과 통과를 생성합니다.

로깅 및 지표를 사용해 GraphQL 쿼리를 식별 및 최적화하고, 문제를 해결할 수 있습니다. AWS AppSync GraphQL에 대한 로깅을 켜면 API 요청 및 응답에 대한 자세한 정보를 얻고, 문제를 식별하여 대응하고, 규제 요구 사항을 준수하는 데 도움이 됩니다.

이제 Security Hub가 와 통합되었습니다

에 대한 로깅을 AWS AppSync켜려면 AWS AppSync 개발자 안내서의 설정 및 구성을 참조하십시오.

[AppSync.4] AWS AppSync GraphQL API는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AppSync::GraphQLApi`

AWS Config 규칙: `tagged-appsync-graphqlapi` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 AWS AppSync GraphQL API에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다. `requiredTagKeys` GraphQL API에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 GraphQL API에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

AWS AppSync GraphQL API에 태그를 추가하려면 API 레퍼런스를 TagResource참조하십시오.AWS AppSync

[AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리 > 암호 없는 인증

심각도: 높음

리소스 유형: `AWS::AppSync::GraphQLApi`

AWS Config 규칙: `appsync-authorization-check`

스케줄 유형: 변경이 트리거됨

파라미터:

- `AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS`(사용자 지정할 수 없음)

이 컨트롤은 애플리케이션이 API 키를 사용하여 AWS AppSync GraphQL API와 상호작용하는지 여부를 확인합니다. AWS AppSync GraphQL API가 API 키로 인증되면 제어가 실패합니다.

API 키는 인증되지 않은 GraphQL 엔드포인트를 생성할 때 AWS AppSync 서비스에서 생성되는 애플리케이션의 하드 코딩된 값입니다. 이 API 키가 손상되면 엔드포인트는 의도하지 않은 액세스에 취약합니다. 공개적으로 액세스할 수 있는 애플리케이션 또는 웹사이트를 지원하는 경우가 아니라면 인증에 API 키를 사용하지 않는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

AWS AppSync GraphQL API의 권한 부여 옵션을 설정하려면 개발자 안내서의 권한 부여 및 인증을 참조하십시오.AWS AppSync

Amazon Athena 제어

이러한 제어는 Athena 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Athena.1] Athena 워크그룹은 저장 시 암호화되어야 합니다

> **Important**
>
> Security Hub는 2024년 4월에 이 제어를 폐기했습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

심각도: 중간

리소스 유형: `AWS::Athena::WorkGroup`

AWS Config 규칙: `athena-workgroup-encrypted-at-rest`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Athena 작업 그룹이 저장 시 암호화되었는지 확인합니다. Athena 워크그룹이 저장 시 암호화되지 않으면 제어가 실패합니다.

Athena에서는 팀, 애플리케이션 또는 다양한 워크로드에 대한 쿼리를 실행하기 위한 작업 그룹을 만들 수 있습니다. 각 워크그룹에는 모든 쿼리를 암호화할 수 있는 설정이 있습니다. Amazon Simple Storage Service (Amazon S3) 관리 키를 사용한 서버 측 암호화, () 키를 사용한 서버 측 암호화 또는 고객 관리 KMS 키를 사용한 AWS Key Management Service 클라이언트 측 암호화를 사용할 수 있습니다.AWS KMS저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 해당 데이터의 기밀성을 보호하여 권한 없는 사용자가 해당 데이터에 액세스할 수 있는 위험을 줄일 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Athena 워크그룹에 대해 저장 시 암호화를 활성화하려면 Amazon Athena 사용 설명서의 워크그룹 편집을 참조하십시오. 쿼리 결과 구성 섹션에서 쿼리 결과 암호화를 선택합니다.

[Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Athena::DataCatalog`

AWS Config 규칙: `tagged-athena-datacatalog` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon Athena 데이터 카탈로그에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 데이터 카탈로그에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 데이터 카탈로그에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Athena 데이터 카탈로그에 태그를 추가하려면 Amazon Athena 사용 설명서의 Athena 리소스 태그 지정을 참조하십시오.

[Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Athena::WorkGroup`

AWS Config 규칙: `tagged-athena-workgroup` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
requiredTagKeys	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	No default value

이 컨트롤은 Amazon Athena 워크그룹에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. requiredTagKeys 워크그룹에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. requiredTagKeys 매개 변수를 requiredTagKeys 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 작업 그룹에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 aws: 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Athena 워크그룹에 태그를 추가하려면 Amazon Athena 사용 설명서의 개별 워크그룹에 태그 추가 및 삭제를 참조하십시오.

AWS Backup 제어:

이러한 컨트롤은 AWS Backup 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-9(8), NIST.800-53.r5 SI-12

범주: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::Backup::RecoveryPoint`

AWS Config 규칙: `backup-recovery-point-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS Backup 복구 지점이 유휴 상태에서 암호화되었는지 확인합니다. 복구 시점이 저장 시 암호화되지 않으면 제어가 실패합니다.

AWS Backup 복구 지점이란 백업 프로세스의 일부로 생성되는 데이터의 특정 복사본 또는 스냅샷을 말합니다. 이는 데이터가 백업된 특정 시점을 나타내며 원본 데이터가 손실되거나 손상되거나 액세스할 수 없는 경우에 대비하여 복원 시점 역할을 합니다. 백업 복구 시점을 암호화하면 무단 액세스에 대한 별도의 보호 계층이 추가됩니다. 암호화는 백업 데이터의 기밀성, 무결성 및 보안을 보호하기 위한 모범 사례입니다.

이제 Security Hub가 와 통합되었습니다

AWS Backup 복구 지점을 암호화하려면 AWS Backup 개발자 안내서의 백업 암호화를 참조하십시오. AWS Backup

[백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Backup::RecoveryPoint`

AWS Config규칙: `tagged-backup-recoverypoint` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 AWS Backup 복구 지점에 매개 변수에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 복구 지점에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 복구 지점에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

복구 지점에 태그 추가하기 AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.

2. 탐색 창에서 백업 계획을 선택합니다.
3. 목록에서 백업 계획을 선택합니다.
4. 백업 계획 태그 섹션에서 태그 관리를 선택합니다.
5. 해당 태그의 키와 값을 입력합니다. 키-값 쌍을 추가하려면 새 태그 추가를 선택합니다.
6. 태그 추가가 완료되면 저장을 선택합니다.

[백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Backup::BackupVault`

AWS Config규칙: `tagged-backup-backupvault` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 AWS Backup Vault에 매개변수에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 복구 지점에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 복구 지점에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성,

검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

저장소에 태그 추가하기 AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택합니다.
3. 목록에서 백업 저장소를 선택합니다.
4. Backup Vault 태그 섹션에서 [태그 관리] 를 선택합니다.
5. 해당 태그의 키와 값을 입력합니다. 키-값 쌍을 추가하려면 새 태그 추가를 선택합니다.
6. 태그 추가가 완료되면 저장을 선택합니다.

[백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Backup::ReportPlan`

AWS Config규칙: `tagged-backup-reportplan` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
requiredTagKeys	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 AWS Backup 보고서 계획에 매개변수에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredTagKeys. 보고서 계획에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 제어가 requiredTagKeys 실패합니다. 매개 변수를 requiredTagKeys 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 보고서 계획에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고로 aws: 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

보고서 계획에 태그 추가하기 AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택합니다.
3. 목록에서 백업 저장소를 선택합니다.

4. Backup Vault 태그 섹션에서 [태그 관리] 를 선택합니다.
5. 새 태그 추가를 선택합니다. 해당 태그의 키와 값을 입력합니다. 추가 키-값 쌍을 보려면 이 단계를 반복하세요.
6. 태그 추가가 완료되면 저장을 선택합니다.

[백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Backup::BackupPlan`

AWS Config규칙: `tagged-backup-backupplan` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 AWS Backup 백업 계획에 매개 변수에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 백업 계획에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 백업 계획에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그

를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

백업 계획에 태그 추가하기 AWS Backup

1. https://console.aws.amazon.com/backup 에서 AWS Backup 콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택합니다.
3. 목록에서 백업 저장소를 선택합니다.
4. Backup Vault 태그 섹션에서 [태그 관리] 를 선택합니다.
5. 새 태그 추가를 선택합니다. 해당 태그의 키와 값을 입력합니다. 추가 키-값 쌍을 보려면 이 단계를 반복하세요.
6. 태그 추가가 완료되면 저장을 선택합니다.

AWS CloudFormation 컨트롤

이러한 컨트롤은 CloudFormation 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[CloudFormation.1] CloudFormation 스택은 Simple Notification Service (SNS) 와 통합되어야 합니다.

> **Important**
>
> Security Hub는 2024년 4월에 이 제어를 폐기했습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 SI-4(12), NIST.800-53.r5 SI-4(5)

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::CloudFormation::Stack`

AWS Config 규칙: `cloudformation-stack-notification-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Simple Notification Service 알림이 AWS CloudFormation 스택과 통합되었는지 여부를 확인합니다. 연결된 SNS 알림이 없는 경우 CloudFormation 스택에 대한 제어가 실패합니다.

스택으로 SNS 알림을 구성하면 CloudFormation 스택에서 발생하는 모든 이벤트 또는 변경 사항을 이해관계자에게 즉시 알릴 수 있습니다.

이제 Security Hub가 와 통합되었습니다

CloudFormation 스택과 SNS 주제를 통합하려면 AWS CloudFormation 사용 설명서의 스택 직접 업데이트를 참조하십시오.

[CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::CloudFormation::Stack`

AWS Config 규칙: `tagged-cloudformation-stack` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태	StringList	요구 사항을 충족하는	기본값 없음

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
	그 키는 대소문자를 구별합니다.		AWS 태그 목록	

이 컨트롤은 AWS CloudFormation 스택에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 스택에 태그 키가 없거나 매개변수에 지정된 모든 키가 없는 경우 컨트롤이 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 스택에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

CloudFormation CreateStack스택에 태그를 추가하려면 AWS CloudFormation API 참조를 참조하십시오.

아마존 CloudFront 컨트롤

이러한 컨트롤은 CloudFront 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16)

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-default-root-object-configured`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon CloudFront 배포가 기본 루트 객체인 특정 객체를 반환하도록 구성되어 있는지 여부를 확인합니다. CloudFront 배포에 기본 루트 객체가 구성되어 있지 않으면 제어가 실패합니다.

사용자가 배포의 객체 대신 배포의 루트 URL을 요청하는 경우가 있습니다. 이 경우 기본 루트 객체를 지정하면 웹 배포 내용이 노출되는 것을 방지하는 데 도움이 될 수 있습니다.

이제 Security Hub가 와 통합되었습니다

CloudFront 배포의 기본 루트 객체를 구성하려면 Amazon CloudFront 개발자 안내서의 기본 루트 객체를 지정하는 방법을 참조하십시오.

[CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-viewer-policy-https`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon CloudFront 배포에서 최종 사용자가 HTTPS를 직접 사용하도록 요구하는지 또는 리디렉션을 사용하는지 여부를 확인합니다. `ViewerProtocolPolicy`가 `defaultCacheBehavior`용 또는 `cacheBehaviors`용으로 `allow-all`로 설정된 경우 제어가 실패합니다.

HTTPS (TLS) 는 잠재적 공격자가 네트워크 트래픽을 도청하거나 조작하기 위한 person-in-the-middle 또는 유사한 공격을 사용하는 것을 방지하는 데 사용할 수 있습니다. 암호화된 HTTPS(TLS) 연결만 허용되어야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 이해해야 합니다.

이제 Security Hub가 와 통합되었습니다

전송 중인 CloudFront 배포를 암호화하려면 Amazon CloudFront 개발자 안내서의 최종 사용자 간 통신을 위한 HTTPS 요구 사항을 참조하십시오. CloudFront

[CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 낮음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-origin-failover-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon CloudFront 배포가 오리진이 두 개 이상 있는 오리진 그룹으로 구성되어 있는지 확인합니다.

CloudFront 오리진 페일오버는 가용성을 높일 수 있습니다. 오리진 장애 조치는 기본 오리진을 사용할 수 없거나 특정 HTTP 응답 상태 코드를 반환하는 경우 트래픽을 보조 오리진으로 자동 리디렉션합니다.

이제 Security Hub가 와 통합되었습니다

CloudFront 배포를 위한 오리진 장애 조치를 구성하려면 Amazon CloudFront 개발자 안내서의 오리진 그룹 생성을 참조하십시오.

[CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-accesslogs-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 배포에 CloudFront 서버 액세스 로깅이 활성화되어 있는지 여부를 확인합니다. 배포에 대한 액세스 로깅이 활성화되지 않은 경우 제어가 실패합니다.

CloudFront 액세스 로그는 CloudFront 수신되는 모든 사용자 요청에 대한 자세한 정보를 제공합니다. 각 로그에는 요청이 수신된 날짜 및 시간, 요청한 뷰어의 IP 주소, 요청 소스, 뷰어의 요청 포트 번호 등의 정보가 포함됩니다.

이러한 로그는 보안 및 액세스 감사, 포렌식 조사와 같은 목적에 유용합니다. 액세스 로그를 분석하는 방법에 대한 추가 지침은 Amazon Athena 사용 설명서의 Amazon CloudFront 로그 쿼리를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

CloudFront 배포에 대한 액세스 로깅을 구성하려면 Amazon CloudFront 개발자 안내서의 표준 로그(액세스 로그) 구성 및 사용을 참조하십시오.

[CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21)

범주: 보호 > 보호 서비스

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-associated-with-waf`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 CloudFront 배포가 AWS WAF 클래식 또는 웹 ACL과 연결되어 있는지 확인합니다. AWS WAF 배포가 웹 ACL과 연결되어 있지 않으면 제어가 실패합니다.

AWS WAF 웹 애플리케이션 및 API를 공격으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 사용자가 정의한 맞춤형 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 집합(웹 액세스 제어 목록 또는 웹 ACL)을 구성할 수 있습니다. CloudFront 배포를 AWS WAF 웹 ACL과 연결해야 악의적인 공격으로부터 보호할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

AWS WAF 웹 ACL을 CloudFront 배포와 AWS WAF 연결하려면 Amazon CloudFront 개발자 안내서의 콘텐츠에 대한 액세스 제어를 위한 사용을 참조하십시오.

[CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-custom-ssl-certificate`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 CloudFront 배포에 기본 SSL/TLS 인증서가 제공하는 것을 사용하는지 여부를 확인합니다. CloudFront CloudFront 배포에서 사용자 지정 SSL/TLS 인증서를 사용하는 경우 이 제어가 전달됩니다. CloudFront 배포에서 기본 SSL/TLS 인증서를 사용하는 경우 이 제어가 실패합니다.

사용자 지정 SSL/TLS를 사용하면 사용자가 대체 도메인 이름을 사용하여 콘텐츠에 액세스할 수 있습니다. 사용자 지정 인증서를 AWS Certificate Manager (권장) 또는 IAM에 저장할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

사용자 지정 SSL/TLS 인증서를 사용하여 CloudFront 배포에 대체 도메인 이름을 추가하려면 Amazon 개발자 안내서의 대체 도메인 이름 추가를 참조하십시오. CloudFront

[CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-sni-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon CloudFront 배포가 사용자 지정 SSL/TLS 인증서를 사용하고 있고 SNI를 사용하여 HTTPS 요청을 처리하도록 구성되어 있는지 확인합니다. 사용자 지정 SSL/TLS 인증서가 연결되어 있지만 SSL/TLS 지원 방법이 전용 IP 주소인 경우 이 제어는 실패합니다.

서버 이름 표시(SNI)는 2010년 이후 출시된 브라우저와 클라이언트에서 지원되는 TLS 프로토콜의 확장 기능입니다. SNI를 사용하여 HTTPS 요청을 CloudFront 처리하도록 구성하는 경우 대체 도메인 이름을 각 엣지 로케이션의 IP 주소와 CloudFront 연결합니다. 최종 사용자가 HTTPS 콘텐츠 요청을 제출하면 DNS는 이 요청을 올바른 엣지 로케이션의 IP 주소로 라우팅합니다. 도메인 이름의 IP 주소는 SSL/TLS 핸드셰이크 협상 중에 결정됩니다(IP 주소는 배포 전용이 아님).

이제 Security Hub가 와 통합되었습니다

SNI를 사용하여 HTTPS 요청을 처리하도록 CloudFront 배포를 구성하려면 개발자 안내서의 SNI를 사용하여 HTTPS 요청 제공 (대부분의 클라이언트에 적합) 을 참조하십시오. CloudFront

[CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-traffic-to-origin-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon CloudFront 배포가 사용자 지정 오리진에 대한 트래픽을 암호화하는지 확인합니다. 오리진 프로토콜 정책이 'http-only'를 CloudFront 허용하는 배포에서는 이 제어가 실패합니다. 배포의 원본 프로토콜 정책이 'match-viewer'이고 뷰어 프로토콜 정책이 'all-all'인 경우에도 이 제어가 실패합니다.

HTTPS(TLS)를 사용하면 네트워크 트래픽의 도청이나 조작을 방지할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다.

이제 Security Hub가 와 통합되었습니다

CloudFront 연결에 암호화를 요구하도록 원본 프로토콜 정책을 업데이트하려면 Amazon CloudFront Developer Guide의 사용자 지정 오리진 간 CloudFront 통신을 위한 HTTPS 요구를 참조하십시오.

[CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-no-deprecated-ssl-protocols`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon CloudFront 배포가 CloudFront 엣지 로케이션과 사용자 지정 오리진 간의 HTTPS 통신에 더 이상 사용되지 않는 SSL 프로토콜을 사용하고 있는지 확인합니다. CloudFront 배포에 where가 포함되어 있는 경우 이 제어는 실패합니다. `CustomOriginConfig` `OriginSslProtocols` `SSLv3`

2015년 IETF(Internet Engineering Task Force)는 SSL 3.0의 보안이 충분하지 않기 때문에 더 이상 사용되지 않아야 한다고 공식적으로 발표했습니다. 사용자 지정 오리진에 대한 HTTPS 통신에는 TLSv1.2 이상을 사용하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

CloudFront 배포를 위한 오리진 SSL 프로토콜을 업데이트하려면 Amazon CloudFront 개발자 안내서의 사용자 지정 CloudFront 오리진과 사용자 지정 오리진 간의 통신을 위한 HTTPS 요구를 참조하십시오.

[CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.

관련 요구 사항: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 리소스 구성

심각도: 높음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-s3-origin-non-existent-bucket`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Amazon CloudFront 배포가 존재하지 않는 Amazon S3 오리진을 가리키는지 여부를 확인합니다. 오리진이 존재하지 않는 버킷을 가리키도록 구성된 경우 CloudFront 배포에 대한 제어가 실패합니다. 이 제어는 정적 웹 사이트 호스팅이 없는 S3 버킷이 S3 오리진인 CloudFront 배포에만 적용됩니다.

계정의 CloudFront 배포가 존재하지 않는 버킷을 가리키도록 구성된 경우 악의적인 제3자가 참조된 버킷을 만들고 배포를 통해 자체 콘텐츠를 제공할 수 있습니다. 라우팅 동작에 관계없이 모든 오리진을 검사하여 배포가 적절한 오리진을 가리키고 있는지 확인하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

새 오리진을 가리키도록 CloudFront 배포를 수정하려면 Amazon CloudFront 개발자 안내서의 배포 업데이트를 참조하십시오.

[CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `cloudfront-s3-origin-access-control-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 오리진이 있는 Amazon CloudFront 배포에 원본 액세스 제어 (OAC) 가 구성되어 있는지 확인합니다. 배포를 위해 OAC가 구성되지 않은 경우 제어가 실패합니다 CloudFront .

S3 버킷을 CloudFront 배포용 오리진으로 사용하는 경우 OAC를 활성화할 수 있습니다. 이렇게 하면 지정된 CloudFront 배포를 통해서만 버킷의 콘텐츠에 액세스할 수 있고, 버킷이나 다른 배포에서 직접 액세스하는 것은 금지됩니다. OAI (원본 액세스 ID) 를 CloudFront 지원하지만 OAC는 추가 기능을 제공하며 OAI를 사용하는 배포는 OAC로 마이그레이션할 수 있습니다. OAI는 S3 오리진에 안전하게 액세스할 수 있는 방법을 제공하지만 세분화된 정책 구성과 서명 버전 4 (SigV4) 가 필요한 POST 방법을 사용하는 HTTP/HTTPS 요청에 대한 지원이 부족한 등 한계가 있습니다. AWS 리전 AWS 또한 OAI는 암호화를 지원하지 않습니다. AWS Key Management Service OAC는 IAM 서비스 보안 주체를 사용하여 S3 오리진으로 인증하는 AWS 모범 사례를 기반으로 합니다.

이제 Security Hub가 와 통합되었습니다

S3 오리진을 사용하는 CloudFront 배포에 대해 OAC를 구성하려면 Amazon 개발자 안내서의 Amazon S3 오리진에 대한 액세스 제한을 참조하십시오. CloudFront

[CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: `tagged-cloudfront-distribution` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon CloudFront 배포에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 배포에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 배포에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

CloudFront 배포에 태그를 추가하려면 Amazon CloudFront 개발자 안내서의 Amazon CloudFront 배포에 태그 지정을 참조하십시오.

AWS CloudTrail 컨트롤:

이러한 컨트롤은 CloudTrail 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/2.1, CIS 재단 벤치마크 v1.4.0/3.1, CIS AWS AWS 재단 벤치마크 v3.0.0/3.1, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, Nist.800-53.R5 CA-7, Nist.800-53.R5 CA-7, Nist.800-53.R5 CA-7, Nist.ST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SA-8 (22) AU-14

범주: 식별 > 로깅

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `multi-region-cloudtrail-enabled`

스케줄 유형: 주기적

파라미터:

- `readWriteType`: `ALL`(사용자 지정할 수 없음)

  `includeManagementEvents`: `true`(사용자 지정할 수 없음)

이 컨트롤은 읽기 및 쓰기 관리 이벤트를 캡처하는 다중 지역 AWS CloudTrail 트레일이 하나 이상 있는지 확인합니다. 사용하지 않도록 설정하거나 읽기 및 쓰기 관리 이벤트를 캡처하는 CloudTrail 트레일이 하나 이상 없는 경우 CloudTrail 제어가 실패합니다.

AWS CloudTrail 계정에 대한 AWS API 호출을 기록하고 로그 파일을 사용자에게 전달합니다. 기록된 정보에는 다음 정보가 포함됩니다.

- API 호출자의 ID
- API 호출 시간
- API 호출자의 소스 IP 주소
- 요청 파라미터
- 에서 반환한 응답 요소 AWS 서비스

CloudTrail , AWS SDK AWS Management Console, 명령줄 도구에서 이루어진 API 호출을 포함하여 계정에 대한 API 호출 기록을 제공합니다. AWS 기록에는 다음과 같은 상위 수준의 AWS 서비스 API 호출도 포함됩니다. AWS CloudFormation

에서 생성한 AWS API 호출 기록을 CloudTrail 통해 보안 분석, 리소스 변경 추적 및 규정 준수 감사를 수행할 수 있습니다. 다중 리전 추적에는 다음과 같은 이점이 있습니다.

- 다중 리전 추적을 통해 사용하지 않는 리전에서 발생하는 예기치 않은 활동을 감지할 수 있습니다.
- 다중 리전 추적으로 인해 기본적으로 추적에 글로벌 서비스 이벤트 로깅이 사용되도록 설정됩니다. 글로벌 서비스 이벤트 로깅은 AWS 글로벌 서비스에서 생성된 이벤트를 기록합니다.
- 다중 지역 트레일의 경우 모든 읽기 및 쓰기 작업에 대한 관리 이벤트를 통해 모든 리소스에 대한 CloudTrail 레코드 관리 작업을 한 AWS 계정번에 수행할 수 있습니다.

기본적으로 를 사용하여 만든 CloudTrail AWS Management Console 트레일은 멀티 리전 트레일입니다.

이제 Security Hub가 와 통합되었습니다

에서 새 다중 지역 트레일을 만들려면 사용 CloudTrail 안내서의 트레일 만들기를 참조하십시오.AWS CloudTrail 다음 값을 사용합니다.

필드	값
추가 설정, 로그 파일 검증	활성화됨
로그 이벤트, 관리 이벤트, API 활동 선택	읽기 및 쓰기. 제외 확인란을 선택 취소합니다.

기존 추적을 업데이트하려면 AWS CloudTrail 사용 안내서의 추적 업데이트를 참조하십시오. 관리 이벤트에서 API 활동의 경우 읽기 및 쓰기를 선택합니다.

[CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/3.4, CIS 재단 벤치마크 v1.2.0/2.7, CIS 재단 벤치마크 v1.4.0/3.7, CIS AWS 재단 벤치마크 v3.0.0/3.5, NIST.800-53.r5 AU-9, NIST.800-53.r5 CM-3 (6), NiST.800-53.r5 CM-3 (6), Nist.800-53.r5 CM-3 (6), Nist.800-53.r5 CM-3 (6), Nist.800-53.r5 CM-3 (6), Nist.800-53.r5 CM-3 (6), Nist.800-53.r5 CM-3 (6), Nist.800-53.r5 CM-3 (6 AWS NIST.800-53.r5 SC-13, NIST.800-53.R5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6) AWS

범주: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::CloudTrail::Trail`

AWS Config 규칙: `cloud-trail-encryption-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 CloudTrail 컨트롤은 서버 측 암호화 (SSE) 암호화를 사용하도록 구성되었는지 여부를 확인합니다. AWS KMS key `KmsKeyId`가 정의되지 않은 경우 제어가 실패합니다.

민감한 CloudTrail 로그 파일의 보안을 강화하려면 저장 중인 로그 파일에 대해 서버 측 암호화 AWS KMS keys (SSE-KMS) 를 사용해야 합니다. CloudTrail 기본적으로 버킷으로 전송되는 로그 파일은

Amazon S3에서 관리하는 암호화 키 (SSE-S3) 를 사용한 Amazon 서버 측 암호화로 암호화됩니다. CloudTrail

이제 Security Hub가 와 통합되었습니다

CloudTrail 로그 파일에 SSE-KMS 암호화를 활성화하려면 사용 설명서의 KMS 키를 사용하도록 트레일 업데이트를 참조하십시오.AWS CloudTrail

[CloudTrail.3] 하나 이상의 트레일을 활성화해야 합니다. CloudTrail

관련 요구 사항: PCI DSS v3.2.1/10.1, PCI DSS v3.2.1/10.2.1, PCI DSS v3.2.1/10.2.2, PCI DSS v3.2.1/10.2.3, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.5, PCI DSS v3.2.1/10.2.6, PCI DSS v3.2.1/10.2.7, PCI DSS v3.2.1/10.3.1, PCI DSS v3.2.1/10.3.2, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6

범주: 식별 > 로깅

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `cloudtrail-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 내 AWS CloudTrail 트레일이 활성화되어 있는지 AWS 계정확인합니다. 계정에 CloudTrail 트레일이 하나 이상 활성화되어 있지 않으면 제어가 실패합니다.

하지만 일부 AWS 서비스에서는 모든 API 및 이벤트의 로깅을 활성화하지 않습니다. 이외의 추가 감사 추적을 구현하고 CloudTrail 지원 서비스 CloudTrail 및 통합의 각 서비스에 대한 설명서를 검토해야 합니다.

이제 Security Hub가 와 통합되었습니다

트레일을 CloudTrail 시작하고 생성하려면 AWS CloudTrail 사용 설명서의 시작하기 AWS CloudTrail 튜토리얼을 참조하십시오.

[CloudTrail.4] CloudTrail 로그 파일 검증을 활성화해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/10.5.5, CIS 재단 벤치마크 v1.2.0/2.2, CIS 재단 벤치마크 v1.4.0/3.2, CIS AWS 재단 벤치마크 v3.0.0/3.2, NIST.800-53.r5 AU-9, NIST.800-53.r5

SI-4, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4, AWS NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4, AWS NIST.800-53.r5 SI-4, NIST.SI-7 (1), NIST.800-53.r5 SI-7 (3), NIST.800-53.r5 SI-7 (7)

범주: 데이터 보호 > 데이터 무결성

심각도: 낮음

리소스 유형: `AWS::CloudTrail::Trail`

AWS Config 규칙: `cloud-trail-log-file-validation-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 CloudTrail 트레일에서 로그 파일 무결성 검증이 활성화되었는지 여부를 확인합니다.

CloudTrail 로그 파일 검증은 CloudTrail Amazon S3에 쓰는 각 로그의 해시를 포함하는 디지털 서명된 다이제스트 파일을 생성합니다. 이러한 다이제스트 파일을 사용하여 로그를 전달한 후 로그 파일이 변경, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. CloudTrail

Security Hub에서는 모든 추적에 대해 파일 검증을 활성화할 것을 권장합니다. 로그 파일 검증은 로그의 추가 무결성 CloudTrail 검사를 제공합니다.

이제 Security Hub가 와 통합되었습니다

CloudTrail 로그 파일 검증을 활성화하려면 사용 AWS CloudTrail 설명서의 로그 파일 무결성 검증 활성화를 참조하십시오. CloudTrail

[CloudTrail.5] CloudTrail 트레일은 Amazon Logs와 통합되어야 합니다. CloudWatch

관련 요구 사항: PCI DSS v3.2.1/10.5.3, CIS 재단 벤치마크 v1.2.0/2.4, CIS AWS AWS 재단 벤치마크 v1.4.0/3.4, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AC-6 (9) AU-10, NIST.800-53.r5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (1), NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-6 (4) -6 (5), NIST.800-53.r5 AU-7 (1), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (20), Nist..800-53.r5 SI-4 (SI-205), NIST.800-53.r5 SI-7 (8)

범주: 식별 > 로깅

심각도: 낮음

리소스 유형: `AWS::CloudTrail::Trail`

AWS Config 규칙: `cloud-trail-cloud-watch-logs-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 로그를 로그로 전송하도록 트레일이 구성되어 있는지 확인합니다. CloudTrail CloudWatch 추적의 `CloudWatchLogsLogGroupArn` 속성이 비어 있으면 제어가 실패합니다.

CloudTrail 지정된 계정에서 이루어진 AWS API 호출을 기록합니다. 기록된 정보에는 다음이 포함됩니다.

- API 호출자의 ID
- API 호출 시간
- API 호출자의 소스 IP 주소
- 요청 파라미터
- 에서 반환한 응답 요소 AWS 서비스

CloudTrail Amazon S3를 로그 파일 저장 및 전송에 사용합니다. 장기 분석을 위해 지정된 S3 버킷에서 CloudTrail 로그를 캡처할 수 있습니다. 실시간 분석을 수행하기 위해 로그를 CloudTrail Logs로 전송하도록 구성할 수 있습니다. CloudWatch

계정의 모든 지역에서 활성화된 트레일의 경우 모든 해당 지역의 로그 파일을 로그 CloudWatch 로그 그룹으로 CloudTrail 보냅니다.

Security Hub는 CloudTrail 로그를 로그로 CloudWatch 전송할 것을 권장합니다. 참고로 이 권장 사항은 계정 활동을 캡처, 모니터링하고, 적절하게 경보를 받을 수 있도록 하기 위한 것입니다. CloudWatch 로그를 사용하여 이를 다음과 같이 설정할 수 있습니다 AWS 서비스. 이 권장 사항은 다른 솔루션의 사용을 배제하지 않습니다.

CloudTrail Logs로 CloudWatch 로그를 전송하면 사용자, API, 리소스 및 IP 주소를 기반으로 실시간 및 과거 활동 로깅이 용이해집니다. 이 접근 방식을 사용하여 비정상적이거나 민감한 계정 활동에 대한 경보 및 알림을 설정할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

CloudTrail CloudWatch Logs와 통합하려면 AWS CloudTrail 사용 설명서의 CloudWatch Logs에 이벤트 전송을 참조하십시오.

[CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/2.3, CIS 재단 벤치마크 v1.4.0/3.3 AWS

범주: 식별 > 로깅

심각도: 심각

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적이며 변경이 트리거됨

파라미터: 없음

CloudTrail 계정에서 이루어진 모든 API 호출을 기록합니다. 이 로그 파일은 S3 버킷에 저장됩니다. CIS는 CloudTrail 로그에 대한 공개 액세스를 방지하기 위해 기록하는 S3 버킷에 S3 버킷 정책 또는 ACL (액세스 제어 목록) 을 적용할 것을 권장합니다. CloudTrail CloudTrail 로그 콘텐츠에 대한 공개 액세스를 허용하면 공격자가 해당 계정의 사용 또는 구성의 취약점을 식별하는 데 도움이 될 수 있습니다.

이 검사를 실행하기 위해 Security Hub는 먼저 사용자 지정 로직을 사용하여 CloudTrail 로그가 저장된 S3 버킷을 찾습니다. 그런 다음 AWS Config 관리형 규칙을 사용하여 버킷에 공개적으로 액세스할 수 있는지 확인합니다.

로그를 단일 중앙 집중식 S3 버킷으로 집계하는 경우 Security Hub는 중앙 집중식 S3 버킷이 있는 계정 및 리전에 대해서만 검사를 실행합니다. 기타 계정 및 리전의 경우 제어 상태는 데이터 없음입니다.

버킷에 공개적으로 액세스할 수 있는 경우 검사는 실패한 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

CloudTrail S3 버킷에 대한 퍼블릭 액세스를 차단하려면 Amazon Simple Storage Service 사용 설명서의 S3 버킷에 대한 퍼블릭 액세스 차단 설정 구성을 참조하십시오. 4가지 Amazon S3 퍼블릭 액세스 차단 설정을 모두 선택합니다.

[CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/2.6, CIS 재단 벤치마크 v1.4.0/3.6, CIS AWS 재단 벤치마크 v3.0.0/3.4 AWS

범주: 식별 > 로깅

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

S3 버킷 액세스 로깅은 S3 버킷에 대한 각 요청에 대한 액세스 기록이 포함된 로그를 생성합니다. 액세스 로그 레코드에는 요청 유형, 요청과 관련된 리소스, 요청 처리 날짜/시간과 같은 요청 세부 정보가 포함됩니다.

CIS는 CloudTrail S3 버킷에서 버킷 액세스 로깅을 활성화할 것을 권장합니다.

대상 S3 버킷에서 S3 버킷 로깅을 활성화하면 대상 버킷의 객체에 영향을 미칠 수 있는 모든 이벤트를 캡처할 수 있습니다. 별도 버킷에 배치할 로그를 구성하면 로그 정보에 대한 액세스가 활성화되어 보안 및 인시던트 대응 워크플로에 유용할 수 있습니다.

이 검사를 실행하기 위해 Security Hub는 먼저 사용자 지정 로직을 사용하여 CloudTrail 로그가 저장된 버킷을 찾은 다음 AWS Config 관리형 규칙을 사용하여 로깅이 활성화되었는지 확인합니다.

여러 개의 로그 파일을 단일 대상 Amazon S3 AWS 계정 버킷으로 전송하는 경우 CloudTrail Security Hub는 해당 버킷이 위치한 지역의 대상 버킷에 대해서만 이 제어를 평가합니다. 이렇게 하면 조사 결과가 간소화됩니다. 하지만 대상 버킷으로 로그를 전송하는 모든 계정을 활성화해야 합니다. CloudTrail 대상 버킷을 보유한 계정을 제외한 모든 계정의 제어 상태는 데이터 없음입니다.

버킷에 공개적으로 액세스할 수 있는 경우 검사는 실패한 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

CloudTrail S3 버킷에 대한 서버 액세스 로깅을 활성화하려면 Amazon 심플 스토리지 서비스 사용 설명서의 Amazon S3 서버 액세스 로깅 활성화를 참조하십시오.

[CloudTrail.9] CloudTrail 트레일에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::CloudTrail::Trail`

AWS Config 규칙: `tagged-cloudtrail-trail` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS CloudTrail 트레일에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 트레일에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 컨트롤이 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 트레일에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

CloudTrail 트레일에 태그를 추가하려면 AWS CloudTrail API AddTags참조를 참조하십시오.

아마존 CloudWatch 컨트롤

이러한 컨트롤은 CloudWatch 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/7.2.1, CIS 재단 벤치마크 v1.2.0/1.1, CIS 재단 벤치마크 v1.2.0/3.3, CIS AWS 재단 벤치마크 v1.4.0/1.7, CIS AWS 재단 벤치마크 v1.4.0/4.3 AWS AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

루트 사용자에게는 AWS 계정의 모든 서비스 및 리소스에 제한 없이 액세스할 수 있습니다. 일상적인 작업에는 루트 사용자를 사용하지 않는 것이 좋습니다. 루트 사용자의 사용을 최소화하고 액세스 관리를 위해 최소 권한 원칙을 채택하면 권한이 높은 보안 인증 정보의 의도하지 않은 변경 및 노출 위험이 줄어듭니다.

계정 및 서비스 관리 작업 수행에 필요한 경우에만 루트 사용자 보안 인증 정보를 사용하는 것이 가장 좋습니다. AWS Identity and Access Management (IAM) 정책을 그룹과 역할에 직접 적용하되 사용자

에게는 적용하지 마십시오. 일상적 사용을 위해 관리자를 설정하는 방법에 대한 자습서는 IAM 사용 설명서의 첫 IAM 관리자 및 그룹 생성을 참조하십시오.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.4.0의 제어 1.7에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

Note

Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

  조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**
기본값	**`0`**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *`your-metric-name`*	크거나 같음
...보다	**`1`**

[CloudWatch.2] 승인되지 않은 API 호출에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.1

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch

CIS에서는 지표 필터를 생성하고 승인되지 않은 API 호출에 경보를 생성할 것을 권장합니다. 무단 API 호출을 모니터링하면 애플리케이션 오류를 표시하는 데 도움이 되고 악의적인 활동을 탐지하는 시간을 단축할 수 있습니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.2의 제어 3.1에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우 NO_DATA의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

  조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 NO_DATA의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 ListSubscriptionsByTopic를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 WARNING 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
지표 네임스페이스	**LogMetrics**
지표 값	**1**
기본값	**0**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *your-metric-name*	크거나 같음
...보다	**1**

[CloudWatch.3] MFA를 사용하지 않는 관리 콘솔 로그인에 대한 로그 메트릭 필터 및 경보가 있는지 확인

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.2

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch

CIS에서는 MFA로 보호되지 않는 지표 필터 및 경보 콘솔 로그인을 생성할 것을 권장합니다. 단일 팩터 콘솔 로그인을 모니터링하면 MFA로 보호되지 않는 계정에 대한 가시성이 높아집니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.2의 제어 3.2에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.
>
>   조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**
기본값	**`0`**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *your-metric-name*	크거나 같음
...보다	**1**

[CloudWatch.4] IAM 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.4, CIS 재단 벤치마크 v1.4.0/4.4 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링하는지 여부를 확인합니다. CloudWatch

CIS에서는 IAM 정책의 변경 사항에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 인증 및 권한 부여 제어가 영향을 받지 않게 하는 데 도움이 됩니다.

> **Note**
>
> Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.

검사 결과 다음과 같은 경우에 FAILED 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우 NO_DATA의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

  조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 NO_DATA의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 ListSubscriptionsByTopic를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 WARNING 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

> **Note**
>
> 이러한 수정 단계에서 권장하는 필터 패턴은 CIS 지침의 필터 패턴과 다릅니다. 권장 필터는 IAM API 호출에서 발생하는 이벤트만 대상으로 합니다.

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) || ($.eventName=DeletePolicyVersion) \|\| ($.eventName=AttachRolePolicy) || ($.eventName=DetachRolePolicy) \|\| ($.eventName=AttachUserPolicy) || ($.eventName=DetachUserPolicy) \|\| ($.eventName=AttachGroupPolicy) || ($.eventName=DetachGroupPolicy))}`
지표 네임스페이스	**`LogMetrics`**

필드	값
지표 값	**1**
기본값	**0**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *your-metric-name*	크거나 같음
...보다	**1**

[CloudWatch.5] 기간 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오 CloudTrail AWS Config.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.5, CIS 재단 벤치마크 v1.4.0/4.5 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch

CIS는 CloudTrail 구성 설정 변경에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 계정 내 활동에 대해 지속적인 가시성을 확보하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.4.0의 제어 4.5에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

Note

Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

  조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**
기본값	**`0`**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *`your-metric-name`*	크거나 같음

필드	값
…보다	**1**

[CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.6, CIS 재단 벤치마크 v1.4.0/4.6 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch

CIS에서는 실패한 콘솔 인증 시도에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 실패한 콘솔 로그인을 모니터링하면 자격 증명에 대한 Brute-Force 공격 시도를 감지하는 데 걸리는 리드 타임이 줄어 다른 이벤트 상관관계에서 사용할 수 있는 지표(예: 소스 IP)를 얻을 수 있습니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.4.0의 제어 4.6에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.

- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우 NO_DATA의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

  조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 NO_DATA의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.

3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**
기본값	**`0`**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *`your-metric-name`*	크거나 같음
...보다	**`1`**

[CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제를 위한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.7, CIS 재단 벤치마크 v1.4.0/4.7 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch

CIS에서는 상태가 비활성화됨 또는 예약된 삭제로 변경된 고객 관리형 키에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 비활성화되거나 삭제된 키로 암호화된 데이터는 더 이상 액세스할 수 없습니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.4.0의 제어 4.7에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다. `ExcludeManagementEventSources`에 `kms.amazonaws.com`이 포함된 경우에도 제어가 실패합니다.

> **Note**
>
> Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.
>
> 조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구

성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**
기본값	**`0`**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *your-metric-name*	크거나 같음
...보다	**1**

[CloudWatch.8] S3 버킷 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.8, CIS 재단 벤치마크 v1.4.0/4.8 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch

CIS에서는 S3 버킷 정책 변경 사항에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 민감한 S3 버킷에 관한 허용적인 정책을 감지하고 교정하는 데 걸리는 시간을 줄일 수 있습니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.4.0의 제어 4.8에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

Note

Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

  조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**
기본값	**`0`**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *your-metric-name*	크거나 같음
...보다	**1**

[CloudWatch.9] AWS Config 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.9, CIS 재단 벤치마크 v1.4.0/4.9 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch

CIS에서는 AWS Config 구성 설정 변경에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 계정 내 구성 항목에 대해 지속적인 가시성을 확보하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.4.0의 제어 4.9에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

Note

Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

  조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**
기본값	**`0`**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *`your-metric-name`*	크거나 같음
...보다	**`1`**

[CloudWatch.10] 보안 그룹 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.10, CIS 재단 벤치마크 v1.4.0/4.10 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch 보안 그룹은 VPC에서 수신 및 발신 트래픽을 제어하는 상태 저장 패킷 필터입니다.

CIS에서는 보안 그룹 변경 사항에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 리소스 및 서비스가 의도치 않게 노출되는 일을 방지하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.4.0의 제어 4.10에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우 NO_DATA의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

  조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 NO_DATA의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 ListSubscriptionsByTopic를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 WARNING 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**
기본값	**`0`**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *`your-metric-name`*	크거나 같음
...보다	**`1`**

[CloudWatch.11] 네트워크 액세스 제어 목록 (NACL) 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.11, CIS 재단 벤치마크 v1.4.0/4.11 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch NACL은 VPC에서 서브넷에 대한 수신 및 발신 트래픽을 제어하기 위한 상태 비저장 패킷 필터로 사용됩니다.

CIS에서는 NACL 변경 사항에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 AWS 리소스와 서비스가 의도치 않게 노출되는 것을 방지할 수 있습니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.4.0의 제어 4.11에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkA`

필드	값
	`clEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**
기본값	**`0`**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *`your-metric-name`*	크거나 같음
...보다	**`1`**

[CloudWatch.12] 네트워크 게이트웨이 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.12, CIS 재단 벤치마크 v1.4.0/4.12 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch 네트워크 게이트웨이는 VPC 밖에 있는 대상에(서) 트래픽을 송수신하는 데 필요합니다.

CIS에서는 네트워크 게이트웨이 변경 사항에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 모든 수신 및 발신 트래픽이 제어된 경로를 통해 VPC 경계를 통과하게 하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.2의 제어 4.12에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.
>
>   조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
지표 네임스페이스	**`LogMetrics`**
지표 값	**`1`**

필드	값
기본값	**0**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *your-metric-name*	크거나 같음
...보다	**1**

[CloudWatch.13] 라우팅 테이블 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.13, CIS 재단 벤치마크 v1.4.0/4.13 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링하는지 여부를 확인합니다. CloudWatch 라우팅 테이블을 통해 네트워크 트래픽이 서브넷 간에, 그리고 네트워크 게이트웨이로 라우팅됩니다.

CIS에서는 라우팅 테이블 변경 사항에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 모든 VPC 트래픽이 예상 경로를 따라 흐르게 하는 데 도움이 됩니다.

Note

Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

  조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

> **Note**
>
> 이러한 수정 단계에서 권장하는 필터 패턴은 CIS 지침의 필터 패턴과 다릅니다. 권장 필터는 Amazon Elastic Compute Cloud(EC2) API 호출에서 발생하는 이벤트만 대상으로 합니다.

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`
지표 네임스페이스	**`LogMetrics`**

필드	값
지표 값	**1**
기본값	**0**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *your-metric-name*	크거나 같음
...보다	**1**

[CloudWatch.14] VPC 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/3.14, CIS 재단 벤치마크 v1.4.0/4.14 AWS

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 로그로 보내고 해당 지표 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. CloudWatch 계정에 VPC가 한 개 이상 있을 수 있으므로 VPC 두 개 사이에 피어 연결을 생성하여 네트워크 트래픽이 VPC 간에 라우팅되게 할 수 있습니다.

CIS에서는 VPC 변경 사항에 대한 지표 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 인증 및 권한 부여 제어가 영향을 받지 않게 하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub는 사용자 지정 로직을 사용하여 CIS AWS 기반 벤치마크 v1.4.0의 제어 4.14에 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 지표 필터를 사용하지 않으면 이 제어가 실패합니다. 지표 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub는 이 컨트롤에 대한 검사를 수행할 때 현재 계정에서 사용하는 CloudTrail 트레일을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 결과 다음과 같은 경우에 `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우 `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.
>
>   조직 내 여러 계정의 이벤트를 기록하려면 조직 추적을 사용하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.
>
> 경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub에서 제어에 대한 `WARNING` 조사 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 지표 필터 및 지표 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하십시오.
2. 모두에게 적용되는 CloudTrail 트레일을 만드세요. AWS 리전이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하십시오.

   CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 지표 필터를 생성합니다.
3. 지표 필터를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹에 대한 지표 필터 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
패턴 정의, 패턴 필터링	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
지표 네임스페이스	**`LogMetrics`**

필드	값
지표 값	**1**
기본값	**0**

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon 사용 CloudWatch 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하십시오. 다음 값을 사용합니다.

필드	값
조건, 임계값 유형	정적
언제라도... *your-metric-name*	크거나 같음
...보다	**1**

[CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.

범주: 감지 > 감지 서비스

관련 요구 사항: NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 IR-4(1), NIST.800-53.r5 IR-4(5), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-4(12), NIST.800-53.r5 SI-4(5)

심각도: 높음

리소스 유형: `AWS::CloudWatch::Alarm`

AWS Config 규칙: **`cloudwatch-alarm-action-check`**

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
alarmActionRequired	파라미터가 true로 설정되어 있고 경보 상태가 ALARM으로 변경될 때 작업이 경보에 포함되어 있는 경우 제어가 PASSED 결과를 생성합니다.	불	사용자 지정할 수 없음	true
insufficientDataActionRequired	파라미터가 true로 설정되어 있고 경보 상태가 INSUFFICIENT_DATA 으로 변경될 때 작업이 경보에 포함되어 있는 경우 제어가 PASSED 결과를 생성합니다.	불	true 또는 false	false
okActionRequired	파라미터가 true로 설정되어 있고 경보 상태가 OK으로 변경될 때 작업이 경보에 포함되어 있는 경우 제어가 PASSED 결과를 생성합니다.	불	true 또는 false	false

이 컨트롤은 Amazon CloudWatch 경보에 해당 ALARM 상태에 대해 구성된 작업이 하나 이상 있는지 확인합니다. ALARM 상태에 대해 활성화된 작업이 경보에 없으면 제어가 실패합니다. 필요에 따라 사용자 지정 파라미터 값을 포함시켜 INSUFFICIENT_DATA 또는 OK 상태에 대한 경보 작업도 요구할 수 있습니다.

> **Note**
>
> Security Hub는 CloudWatch 메트릭 경보를 기반으로 이 제어를 평가합니다. 메트릭 경보는 지정된 동작이 구성된 복합 경보의 일부일 수 있습니다. 컨트롤은 다음과 같은 FAILED 경우에 결과를 생성합니다.
>
> - 지정된 동작은 메트릭 경보용으로 구성되지 않았습니다.
> - 메트릭 경보는 지정된 동작이 구성된 복합 경보의 일부입니다.

이 컨트롤은 CloudWatch 경보에 경보 조치가 구성되어 있는지 여부에 초점을 맞추는 반면, CloudWatch.17은 CloudWatch 경보 조치의 활성화 상태에 중점을 둡니다.

모니터링된 지표가 정의된 임계값을 벗어날 경우 자동으로 경고하도록 CloudWatch 경보 조치를 취하는 것이 좋습니다. 모니터링 경보를 통해 비정상적인 활동을 식별하고 경보가 특정 상태로 전환될 때 보안 및 운영 문제에 신속하게 대응할 수 있습니다. 가장 일반적인 유형의 경보 작업은 Amazon Simple Notification Service(SNS) 주제에 메시지를 전송하여 한 명 이상의 사용자에게 알리는 것입니다.

이제 Security Hub가 와 통합되었습니다

경보가 지원하는 CloudWatch 작업에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 알람 작업을 참조하십시오.

[CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.

범주: 식별 > 로깅

관련 요구 사항: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

심각도: 중간

리소스 유형: `AWS::Logs::LogGroup`

AWS Config 규칙: **`cw-loggroup-retention-period-check`**

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
`minRetentionTime`	CloudWatch 로그 그룹의 최소 보존 기간 (일)	Enum	`365`, `400`, `545`, `731`, `1827`, `3653`	`365`	

이 컨트롤은 Amazon CloudWatch 로그 그룹의 보존 기간이 지정된 일수 이상인지 여부를 확인합니다. 보존 기간이 지정된 수 미만인 경우 제어가 실패합니다. 보존 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 365일을 사용합니다.

CloudWatch 로그는 모든 시스템, 애플리케이션 및 확장성이 뛰어난 단일 서비스에 AWS 서비스 있는 로그를 중앙 집중화합니다. CloudWatch 로그를 사용하여 Amazon Elastic Compute Cloud (EC2) 인스턴스, Amazon Route 53 및 기타 소스에서 로그 파일을 모니터링, AWS CloudTrail저장 및 액세스할 수 있습니다. 로그를 1년 이상 보관하면 로그 보존 표준을 준수하는 데 도움이 될 수 있습니다.

이제 Security Hub가 와 통합되었습니다

로그 보존 설정을 구성하려면 Amazon CloudWatch 사용 설명서의 CloudWatch Logs의 로그 데이터 보존 변경을 참조하십시오.

[CloudWatch.17] CloudWatch 알람 조치를 활성화해야 합니다.

범주: 감지 > 감지 서비스

관련 요구 사항: NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-4(12)

심각도: 높음

리소스 유형: `AWS::CloudWatch::Alarm`

AWS Config 규칙: **`cloudwatch-alarm-action-enabled-check`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 CloudWatch 알람 동작이 활성화되었는지 확인합니다 (true로 `ActionEnabled` 설정해야 함). 알람에 대한 알람 동작이 비활성화되면 제어가 실패합니다. CloudWatch

> **Note**
>
> Security Hub는 CloudWatch 메트릭 경보를 기반으로 이 제어를 평가합니다. 메트릭 경보는 경보 동작이 활성화된 복합 경보의 일부일 수 있습니다. 컨트롤은 다음과 같은 `FAILED` 경우에 결과를 생성합니다.
>
> - 지정된 동작은 메트릭 경보용으로 구성되지 않았습니다.

- 메트릭 경보는 경보 동작이 활성화된 복합 경보의 일부입니다.

이 컨트롤은 CloudWatch 알람 동작의 활성화 상태에 초점을 맞추는 반면, CloudWatch.15는 경보에 ALARM 조치가 구성되어 있는지 여부에 중점을 둡니다. CloudWatch

경보 작업은 모니터링된 지표가 정의된 임계값을 벗어나면 자동으로 경고합니다. 경보 동작이 비활성화되면 경보 상태가 변경될 때 아무 작업도 실행되지 않으며 모니터링되는 지표의 변경에 대한 알림도 받지 않습니다. 보안 및 운영 문제에 신속하게 대응할 수 있도록 CloudWatch 경보 조치를 활성화하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

CloudWatch 알람 동작을 활성화하려면 (콘솔)

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 경보 아래의 모든 경보를 선택합니다.
3. 동작을 활성화할 경보를 선택합니다.
4. 작업에서 경보 작업-신규를 선택한 다음 활성화를 선택합니다.

CloudWatch 알람 작업 활성화에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 알람 작업을 참조하십시오.

AWS CodeArtifact 제어:

이러한 제어는 CodeArtifact 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::CodeArtifact::Repository`

AWS Config 규칙: `tagged-codeartifact-repository` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 AWS CodeArtifact 리포지토리에 매개 변수에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 리포지토리에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 저장소에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고로 `aws:` 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

CodeArtifact 리포지토리에 태그를 추가하려면 AWS CodeArtifact 사용 설명서의 리포지토리 태그 CodeArtifact 지정을 참조하십시오.

AWS CodeBuild 컨트롤

이러한 컨트롤은 CodeBuild 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.

관련 요구 사항: PCI DSS v3.2.1/8.2.1, NIST.800-53.r5 SA-3

범주: 보호 > 보안 개발

심각도: 심각

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-source-repo-url-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS CodeBuild 프로젝트 Bitbucket 소스 리포지토리 URL에 개인 액세스 토큰이나 사용자 이름 및 암호가 포함되어 있는지 확인합니다. Bitbucket 소스 리포지토리 URL에 개인용 액세스 토큰 또는 사용자 이름과 암호가 포함된 경우 제어가 실패합니다.

> **Note**
>
> 이 컨트롤은 CodeBuild 빌드 프로젝트의 기본 소스와 보조 소스를 모두 평가합니다. 프로젝트 소스에 대한 자세한 내용은 사용 AWS CodeBuild 안내서의 다중 입력 소스 및 출력 아티팩트 샘플을 참조하십시오.

로그인 자격 증명은 일반 텍스트로 저장 또는 전송하거나 소스 저장소 URL에 표시해서는 안 됩니다. 개인용 액세스 토큰이나 로그인 자격 증명 대신 에서 CodeBuild 소스 공급자에 액세스하고 Bitbucket 리포지토리 위치의 경로만 포함하도록 소스 저장소 URL을 변경해야 합니다. 개인용 액세스 토큰 또는 로그인 자격 증명을 사용하면 의도하지 않은 데이터 노출이나 무단 액세스가 발생할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

OAuth를 사용하도록 CodeBuild 프로젝트를 업데이트할 수 있습니다.

프로젝트 소스에서 CodeBuild 기본 인증/(GitHub) 개인용 액세스 토큰을 제거하려면

1. https://console.aws.amazon.com/codebuild/ 에서 CodeBuild 콘솔을 엽니다.
2. 개인 액세스 토큰 또는 사용자 이름과 암호가 포함된 빌드 프로젝트를 선택합니다.
3. 편집에서 소스를 선택합니다.
4. GitHub /Bitbucket에서 연결 끊기를 선택합니다.
5. [OAuth를 사용하여 연결] 을 선택한 다음 [GitHub/Bitbucket에 연결] 을 선택합니다.
6. 메시지가 표시되면 적절한 권한 부여를 선택합니다.
7. 필요에 따라 리포지토리 URL 및 추가 구성 설정을 다시 구성합니다.
8. 소스 업데이트를 선택합니다.

자세한 내용은 사용 설명서의 CodeBuild 사용 사례 기반 샘플을 참조하십시오.AWS CodeBuild

[CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.

관련 요구 사항: PCI DSS v3.2.1/8.2.1, NIST.800-53.r5 IA-5(7), NIST.800-53.r5 SA-3

범주: 보호 > 보안 개발

심각도: 심각

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-envvar-awscred-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 프로젝트에 환경 변수 `AWS_ACCESS_KEY_ID` 및 `AWS_SECRET_ACCESS_KEY`가 포함되었는지 확인합니다.

인증 보안 인증 정보 `AWS_ACCESS_KEY_ID` 및 `AWS_SECRET_ACCESS_KEY`를 일반 텍스트로 저장해서는 안 됩니다. 이로 인해 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

CodeBuild 프로젝트에서 환경 변수를 제거하려면 AWS CodeBuild 사용 안내서의 빌드 프로젝트 설정 변경을 참조하십시오. AWS CodeBuild환경 변수에 대해 아무것도 선택되지 않았는지 확인하십시오.

민감한 값이 포함된 환경 변수를 AWS Systems Manager 파라미터 저장소에 저장하거나 AWS Secrets Manager 빌드 사양에서 검색할 수 있습니다. 지침은 AWS CodeBuild 사용 설명서의 환경 섹션에서 중요라고 표시된 상자를 참조하십시오.

[CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SI-7(6)

범주: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 낮음

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-s3-logs-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS CodeBuild 프로젝트의 Amazon S3 로그가 암호화되었는지 확인합니다. CodeBuild 프로젝트의 S3 로그에 대해 암호화가 비활성화되면 제어가 실패합니다.

저장 데이터 암호화는 데이터 주위에 액세스 관리 계층을 추가하기 위해 권장되는 모범 사례입니다. 저장된 로그를 AWS 암호화하면 인증을 받지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. 이는 승인되지 않은 사용자가 데이터에 액세스하는 능력을 제한하기 위해 또 다른 액세스 제어 세트를 추가합니다.

이제 Security Hub가 와 통합되었습니다

CodeBuild 프로젝트 S3 로그의 암호화 설정을 변경하려면 AWS CodeBuild 사용 설명서의 빌드 프로젝트 설정 변경을 참조하십시오. AWS CodeBuild

[CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(12), NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2,

NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 CodeBuild 프로젝트 환경에 S3 또는 CloudWatch 활성화된 로그에 대한 로그 옵션이 하나 이상 있는지 확인합니다. CodeBuild 프로젝트 환경에 하나 이상의 로그 옵션이 활성화되어 있지 않으면 이 제어가 실패합니다.

보안 관점에서 볼 때 로깅은 보안 사고 발생 시 향후 포렌식 활동을 가능하게 하는 중요한 기능입니다. CodeBuild 프로젝트의 이상 징후를 위협 탐지와 연관시키면 해당 위협 탐지의 정확성에 대한 신뢰도를 높일 수 있습니다.

이제 Security Hub가 와 통합되었습니다

CodeBuild 프로젝트 로그 설정을 구성하는 방법에 대한 자세한 내용은 사용 설명서의 빌드 프로젝트 만들기 (콘솔) 를 참조하십시오. CodeBuild

[CodeBuild.5] CodeBuild 프로젝트 환경에는 권한 모드가 활성화되어 있지 않아야 합니다.

> **Important**
>
> Security Hub는 2024년 4월에 이 제어를 폐기했습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(10), NIST.800-53.r5 AC-6(2)

범주: 보호 > 보안 액세스 관리

심각도: 높음

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-environment-privileged-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS CodeBuild 프로젝트 환경의 권한 모드 활성화 또는 비활성화 여부를 확인합니다. CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있는 경우 제어가 실패합니다.

기본적으로 Docker 컨테이너는 모든 디바이스에 대한 액세스를 허용하지 않습니다. 권한 모드는 빌드 프로젝트의 Docker 컨테이너에 모든 디바이스에 대한 액세스 권한을 부여합니다. 값 `true`을 사용하여 `privilegedMode`를 설정하면 Docker 대몬(daemon)을 Docker 컨테이너 내에서 실행할 수 있습니다. Docker 대몬(daemon)은 Docker API 요청을 수신하고 이미지, 컨테이너, 네트워크 및 볼륨과 같은 Docker 객체를 관리합니다. 이 파라미터는 빌드 프로젝트가 Docker 이미지를 빌드하는 데 사용되는 경우에만 true로 설정해야 합니다. 그렇지 않으면 Docker API와 컨테이너의 기본 하드웨어에 대한 의도하지 않은 액세스를 방지하기 위해 이 설정을 비활성화해야 합니다. `privilegedMode`를 `false`로 설정하면 중요한 리소스가 변조 및 삭제되지 않도록 보호하는 데 도움이 됩니다.

이제 Security Hub가 와 통합되었습니다

CodeBuild 프로젝트 환경 설정을 구성하려면 CodeBuild 사용 안내서의 빌드 프로젝트 만들기 (콘솔)를 참조하십시오. 환경 섹션에서 권한 설정을 선택하지 마십시오.

AWS Config 컨트롤

이러한 컨트롤은 AWS Config 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/2.5, CIS 재단 벤치마크 v1.4.0/3.5, CIS AWS AWS 재단 벤치마크 v3.0.0/3.3, NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-6 (1), NIST.800-53.r5 CM-8 (2), PC.I DSS v3.2.1/10.5.2, PCI DSS v3.2.1/11.5

범주: 식별 > 인벤토리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: 없음 (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

이 AWS Config 컨트롤은 현재 계정에서 활성화되어 있는지 확인하고 AWS 리전, 현재 지역에서 활성화된 컨트롤에 해당하는 모든 리소스를 기록하고, 서비스 연결 AWS Config 역할을 사용합니다. 서비스 연결 역할을 사용하지 않으면 리소스를 정확하게 기록하는 AWS Config 데 필요한 권한이 다른 역할에 없을 수 있으므로 제어가 실패합니다.

이 AWS Config 서비스는 계정에서 지원되는 AWS 리소스의 구성 관리를 수행하고 사용자에게 로그 파일을 제공합니다. 기록되는 정보에는 구성 항목 (AWS 리소스), 구성 항목 간의 관계, 리소스 내의 모든 구성 변경 사항이 포함됩니다. 글로벌 리소스는 모든 지역에서 사용할 수 있는 리소스입니다.

컨트롤은 다음과 같이 평가됩니다.

- 현재 리전이 집계 리전으로 설정된 경우 AWS Identity and Access Management (IAM) 글로벌 리소스가 기록된 경우에만 컨트롤이 `PASSED` 결과를 생성합니다 (필요한 컨트롤을 활성화한 경우).
- 현재 지역이 연결 지역으로 설정된 경우 컨트롤은 IAM 글로벌 리소스의 기록 여부를 평가하지 않습니다.
- 현재 지역이 애그리게이터에 없거나 계정에 교차 지역 집계가 설정되어 있지 않은 경우, 컨트롤은 IAM 글로벌 리소스가 기록된 경우에만 `PASSED` 결과를 생성합니다 (필요한 컨트롤을 활성화한 경우).

에서 리소스 상태 변경에 대한 일일 기록을 선택하든 연속 기록을 선택하든 제어 결과는 영향을 받지 않습니다. AWS Config하지만 새 컨트롤을 자동으로 사용하도록 구성했거나 새 컨트롤을 자동으로 사용하도록 설정하는 중앙 구성 정책이 있는 경우 새 컨트롤이 출시되면 이 컨트롤의 결과가 변경될 수 있습니다. 이러한 경우 모든 리소스를 기록하지 않으면 새 컨트롤과 연결된 리소스에 대한 기록을 구성해야 `PASSED` 검색 결과를 받을 수 있습니다.

Security Hub 보안 검사는 모든 AWS Config 지역에서 활성화하고 이를 필요로 하는 컨트롤에 대해 리소스 기록을 구성한 경우에만 의도한 대로 작동합니다.

> **Note**
>
> Config.1을 사용하려면 Security Hub를 사용하는 모든 지역에서 사용하도록 설정해야 합니다. AWS Config
> Security Hub는 지역 서비스이므로 이 컨트롤에 대해 수행된 검사는 계정의 현재 지역만 평가합니다.
> 지역의 IAM 글로벌 리소스에 대한 보안 검사를 허용하려면 해당 지역의 IAM 글로벌 리소스를 기록해야 합니다. IAM 글로벌 리소스가 기록되지 않은 지역은 IAM 글로벌 리소스를 확인하는 컨트롤에 대한 기본 PASSED 검색 결과를 받게 됩니다. IAM 글로벌 리소스는 전체적으로 AWS 리전동일하므로 IAM 글로벌 리소스를 홈 지역에만 기록하는 것이 좋습니다 (계정에서 지역 간 집계가 활성화된 경우). IAM 리소스는 글로벌 리소스 기록이 활성화된 지역에서만 기록됩니다. AWS Config 지원되는 IAM 글로벌 기록 리소스 유형은 IAM 사용자, 그룹, 역할 및 고객 관리형 정책입니다. 글로벌 리소스 기록이 해제된 리전에서 이러한 리소스 유형을 검사하는 Security Hub 제어를 비활성화하는 것을 고려할 수 있습니다. 자세한 정보는 비활성화할 수 있는 Security Hub 제어을 참조하세요.

이제 Security Hub가 와 통합되었습니다

각 컨트롤에 기록해야 하는 리소스 목록은 을 참조하십시오. AWS Config 제어 결과를 생성하는 데 필요한 리소스

애그리게이터에 속하지 않는 홈 리전 및 리전에는 IAM 글로벌 리소스를 필요로 하는 컨트롤을 활성화한 경우 IAM 글로벌 리소스를 포함하여 현재 리전에서 활성화된 컨트롤에 필요한 모든 리소스를 기록해 두십시오.

연결 지역에서는 현재 지역에서 활성화된 컨트롤에 해당하는 모든 리소스를 기록하기만 하면 모든 AWS Config 녹화 모드를 사용할 수 있습니다. 연결 지역에서 IAM 글로벌 리소스 기록이 필요한 컨트롤을 활성화한 경우 FAILED 검색 결과를 받을 수 없습니다 (다른 리소스에 대한 기록이면 충분합니다).

리소스를 기록하도록 AWS Config 활성화하고 구성하려면 AWS Config 개발자 안내서의 콘솔 설정을 AWS Config 참조하십시오. AWS CloudFormation 템플릿을 사용하여 이 프로세스를 자동화할 수도 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation StackSets 샘플 템플릿을 참조하십시오.

Amazon Data Firehose 컨트롤

이러한 컨트롤은 Amazon Data Firehose 리소스와 관련이 있습니다.

이러한 제어 기능을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.R5 AC-3, NIST.800-53.R5 AU-3, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::KinesisFirehose::DeliveryStream`

AWS Config 규칙: `kinesis-firehose-delivery-stream-encrypted`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Amazon Data Firehose 전송 스트림이 서버 측 암호화를 사용하여 유휴 상태에서 암호화되는지 여부를 확인합니다. Firehose 전송 스트림이 서버 측 암호화로 유휴 상태에서 암호화되지 않으면 이 제어가 실패합니다.

서버 측 암호화는 Amazon Data Firehose 전송 스트림의 기능으로, 데이터가 저장되기 전에 () 에서 생성된 키를 사용하여 데이터를 자동으로 암호화합니다. AWS Key Management Service AWS KMS데이터는 Data Firehose 스트림 스토리지 레이어에 기록되기 전에 암호화되고 스토리지에서 검색된 후에 복호화됩니다. 이를 통해 규제 요구 사항을 준수하고 데이터 보안을 강화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Firehose 전송 스트림에서 서버 측 암호화를 활성화하려면 Amazon Data Firehose 개발자 안내서의 Amazon Data Firehose의 데이터 보호를 참조하십시오.

아마존 디텍티브 컨트롤

이러한 컨트롤은 Detective 리소스와 관련이 있습니다.

이러한 제어 기능을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Detective::Graph`

AWS Config 규칙: `tagged-detective-graph` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon Detective 동작 그래프에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 동작 그래프에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 동작 그래프에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Detective 행동 그래프에 태그를 추가하려면 Amazon Detective 관리 가이드의 행동 그래프에 태그 추가를 참조하십시오.

AWS Database Migration Service 컨트롤:

이러한 컨트롤은 AWS DMS 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::DMS::ReplicationInstance`

AWS Config 규칙: `dms-replication-not-public`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 AWS DMS 복제 인스턴스가 퍼블릭인지 여부를 확인합니다. 이를 위해 `PubliclyAccessible` 필드의 값을 검사합니다.

프라이빗 복제 인스턴스에는 복제 네트워크 외부에서 액세스할 수 없는 프라이빗 IP 주소가 있습니다. 소스 및 대상 데이터베이스가 동일한 네트워크에 있는 경우 복제 인스턴스에는 사설 IP 주소가 있어야 합니다. 또한 네트워크는 VPN 또는 VPC 피어링을 사용하여 복제 인스턴스의 VPC에 연결되어야 합니다. AWS Direct Connect퍼블릭 및 프라이빗 복제 인스턴스에 대해 자세히 알아보려면 AWS Database Migration Service 사용 설명서의 퍼블릭 및 프라이빗 복제 인스턴스를 참조하십시오.

또한 AWS DMS 인스턴스 구성에 대한 액세스가 승인된 사용자로만 제한되도록 해야 합니다. 이렇게 하려면 AWS DMS 설정과 리소스를 수정할 수 있는 사용자의 IAM 권한을 제한해야 합니다.

이제 Security Hub가 와 통합되었습니다

DMS 복제 인스턴스를 생성한 후에는 해당 인스턴스의 퍼블릭 액세스 설정을 변경할 수 없습니다. 퍼블릭 액세스 설정을 변경하려면 현재 인스턴스를 삭제한 다음 다시 생성하십시오. 퍼블릭 액세스 가능 옵션을 선택하지 마십시오.

[DMS.2] DMS 인증서에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::DMS::Certificate`

AWS Config 규칙: `tagged-dms-certificate` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS DMS 인증서에 매개변수에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 인증서에 태그 키가 없거나 매개변수에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 인증서에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성,

검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

DMS 인증서에 태그를 추가하려면 사용 설명서의 리소스 태그 지정을 참조하십시오 AWS Database Migration Service.AWS Database Migration Service

[DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::DMS::EventSubscription`

AWS Config 규칙: `tagged-dms-eventsubscription` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS DMS 이벤트 구독에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다requiredTagKeys. 이벤트 구독에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 컨트롤이 requiredTagKeys 실패합니다. 매개 변수를 requiredTagKeys 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 이벤트 구독에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 aws: 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

DMS 이벤트 구독에 태그를 추가하려면 사용 설명서의 리소스 태깅을 참조하십시오. AWS Database Migration ServiceAWS Database Migration Service

[DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::DMS::ReplicationInstance`

AWS Config 규칙: `tagged-dms-replicationinstance` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS DMS 복제 인스턴스에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 복제 인스턴스에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 복제 인스턴스에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

DMS 복제 인스턴스에 태그를 추가하려면 사용 설명서의 리소스 태그 지정을 참조하십시오. AWS Database Migration ServiceAWS Database Migration Service

[DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::DMS::ReplicationSubnetGroup`

AWS Config 규칙: `tagged-dms-replicationsubnetgroup` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS DMS 복제 서브넷 그룹에 `requiredTagKeys` 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 복제 서브넷 그룹에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 복제 서브넷 그룹에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

DMS 복제 서브넷 그룹에 태그를 추가하려면 사용 설명서의 리소스 태깅을 참조하십시오. AWS Database Migration ServiceAWS Database Migration Service

[DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::DMS::ReplicationInstance`

AWS Config 규칙: `dms-auto-minor-version-upgrade-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 복제 인스턴스에 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. AWS DMS DMS 복제 인스턴스에 자동 마이너 버전 업그레이드가 활성화되어 있지 않으면 제어가 실패합니다.

DMS는 지원되는 각 복제 엔진에 자동 마이너 버전 업그레이드를 제공하므로 복제 인스턴스를 up-to-date 유지할 수 있습니다. 마이너 버전은 새로운 소프트웨어 기능, 버그 수정, 보안 패치 및 성능 개선을 도입할 수 있습니다. DMS 복제 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하면 유지 관리 기간 중에 마이너 업그레이드가 자동으로 적용되거나 변경 사항 즉시 적용 옵션을 선택한 경우 즉시 적용됩니다.

이제 Security Hub가 와 통합되었습니다

DMS 복제 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하려면 AWS Database Migration Service 사용 설명서의 복제 인스턴스 수정을 참조하십시오.

[DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,

NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::DMS::ReplicationTask`

AWS Config 규칙: `dms-replication-task-targetdb-logging`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 DMS 복제 작업 `TARGET_APPLY` 및 `TARGET_LOAD`에 대해 최소 심각도 수준 `LOGGER_SEVERITY_DEFAULT`으로 로깅이 활성화되어 있는지 확인합니다. 이러한 작업에 대한 로깅이 활성화되지 않았거나 최소 심각도 수준이 `LOGGER_SEVERITY_DEFAULT`보다 낮으면 제어가 실패합니다.

DMS는 마이그레이션 프로세스 중에 CloudWatch Amazon을 사용하여 정보를 기록합니다. 로깅 작업 설정을 사용하면 기록할 구성 요소 활동과 기록할 정보의 양을 지정할 수 있습니다. 다음 작업에 대한 로깅을 지정해야 합니다.

- `TARGET_APPLY` – 데이터 및 데이터 정의 언어(DDL) 문이 대상 데이터베이스에 적용됩니다.
- `TARGET_LOAD` – 데이터가 대상 데이터베이스에 로드됩니다.

로깅은 모니터링, 문제 해결, 감사, 성능 분석, 오류 탐지, 복구, 기간별 분석 및 보고를 가능하게 함으로써 DMS 복제 작업에서 중요한 역할을 합니다. 이를 통해 데이터 무결성을 유지하고 규제 요구 사항을 준수하면서 데이터베이스 간에 데이터를 성공적으로 복제할 수 있습니다. 문제 해결 중에 이러한 구성 요소에는 `DEFAULT` 이외의 로깅 수준이 거의 필요하지 않습니다. AWS Support에서 특별히 변경을 요청하지 않는 한 이러한 구성 요소에 대한 로깅 수준을 `DEFAULT`으로 유지하는 것이 좋습니다. 최소 로깅 수준 `DEFAULT`을 사용하면 정보 메시지, 경고 및 오류 메시지가 로그에 기록됩니다. 이 제어는 이전 복제 작업에 대한 로깅 수준이 `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` 또는 `LOGGER_SEVERITY_DETAILED_DEBUG` 중 하나 이상인지 확인합니다.

이제 Security Hub가 와 통합되었습니다

대상 데이터베이스 DMS 복제 작업에 대한 로깅을 활성화하려면 사용 AWS Database Migration Service 설명서의 AWS DMS 작업 로그 보기 및 관리를 참조하십시오.

[DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::DMS::ReplicationTask`

AWS Config 규칙: `dms-replication-task-sourcedb-logging`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 DMS 복제 작업 `SOURCE_CAPTURE` 및 `SOURCE_UNLOAD`에 대해 최소 심각도 수준 `LOGGER_SEVERITY_DEFAULT`으로 로깅이 활성화되어 있는지 확인합니다. 이러한 작업에 대한 로깅이 활성화되지 않았거나 최소 심각도 수준이 `LOGGER_SEVERITY_DEFAULT`보다 낮으면 제어가 실패합니다.

DMS는 마이그레이션 프로세스 중에 CloudWatch Amazon을 사용하여 정보를 기록합니다. 로깅 작업 설정을 사용하면 기록할 구성 요소 활동과 기록할 정보의 양을 지정할 수 있습니다. 다음 작업에 대한 로깅을 지정해야 합니다.

- `SOURCE_CAPTURE` - 진행 중인 복제 또는 변경 데이터 캡처(CDC) 데이터는 소스 데이터베이스 또는 서비스에서 캡처되어 `SORTER` 서비스 구성 요소로 전달됩니다.
- `SOURCE_UNLOAD` - 전체 로드 중에 소스 데이터베이스 또는 서비스에서 데이터가 언로드됩니다.

로깅은 모니터링, 문제 해결, 감사, 성능 분석, 오류 탐지, 복구, 기간별 분석 및 보고를 가능하게 함으로써 DMS 복제 작업에서 중요한 역할을 합니다. 이를 통해 데이터 무결성을 유지하고 규제 요구 사항을 준수하면서 데이터베이스 간에 데이터를 성공적으로 복제할 수 있습니다. 문제 해결 중에 이러한 구성 요소에는 `DEFAULT` 이외의 로깅 수준이 거의 필요하지 않습니다. AWS Support에서 특별히 변경을 요청하지 않는 한 이러한 구성 요소에 대한 로깅 수준을 `DEFAULT`으로 유지하는 것이 좋습니다. 최소 로깅 수준 `DEFAULT`을 사용하면 정보 메시지, 경고 및 오류 메시지가 로그에 기록됩니다. 이 제어는 이전 복제 작업에 대한 로깅 수준이 `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` 또는 `LOGGER_SEVERITY_DETAILED_DEBUG` 중 하나 이상인지 확인합니다.

이제 Security Hub가 와 통합되었습니다

원본 데이터베이스 DMS 복제 작업에 대한 로깅을 활성화하려면 사용 AWS Database Migration Service 설명서의 AWS DMS 작업 로그 보기 및 관리를 참조하십시오.

[DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2)

범주: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::DMS::Endpoint`

AWS Config 규칙: `dms-endpoint-ssl-configured`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS DMS 엔드포인트가 SSL 연결을 사용하는지 여부를 확인합니다. 엔드포인트가 SSL을 사용하지 않으면 제어가 실패합니다.

SSL/TLS 연결은 DMS 복제 인스턴스와 데이터베이스 간의 연결을 암호화하여 보안 계층을 제공합니다. 인증서를 사용하면 예상 데이터베이스에 연결 중인지 확인하여 추가 보안 계층을 제공합니다. 프로비저닝하는 모든 데이터베이스 인스턴스에 자동으로 설치되는 서버 인증서를 확인하여 이를 수행합니다. DMS 엔드포인트에서 SSL 연결을 활성화하면 마이그레이션 중에 데이터의 기밀을 보호할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

새 DMS 엔드포인트 또는 기존 DMS 엔드포인트에 SSL 연결을 추가하려면 AWS Database Migration Service 사용 설명서의 AWS Database Migration Service와 함께 SSL 사용을 참조하십시오.

[DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.R5 AC-2, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-17, NIST.800-53.r5 IA-2, NIST.800-53.r5 IA-5 IA-5

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::DMS::Endpoint`

AWS Config 규칙: `dms-neptune-iam-authorization-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon Neptune 데이터베이스의 AWS DMS 엔드포인트가 IAM 인증을 사용하여 구성되었는지 여부를 확인합니다. DMS 엔드포인트에 IAM 승인이 활성화되어 있지 않으면 제어가 실패합니다.

AWS Identity and Access Management (IAM) 은 전체에 걸쳐 세밀한 액세스 제어를 제공합니다. AWS IAM을 사용하면 누가 어떤 조건에서 어떤 서비스와 리소스에 액세스할 수 있는지 지정할 수 있습니다. IAM 정책을 사용하면 인력과 시스템에 대한 권한을 관리하여 권한이 최소한으로 유지되도록 할 수 있습니다. Neptune 데이터베이스의 AWS DMS 엔드포인트에서 IAM 인증을 활성화하면 파라미터에 지정된 서비스 역할을 사용하여 IAM 사용자에게 권한 부여 권한을 부여할 수 있습니다. `ServiceAccessRoleARN`

이제 Security Hub가 와 통합되었습니다

Neptune 데이터베이스의 DMS 엔드포인트에서 IAM 인증을 활성화하려면 사용 설명서의 Amazon Neptune을 대상으로 사용을 참조하십시오. AWS Database Migration ServiceAWS Database Migration Service

[DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-6, NIST.800-53.r5 IA-2, NIST.800-53.r5 IA-5 IA-5

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::DMS::Endpoint`

AWS Config 규칙: `dms-mongo-db-authentication-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 MongoDB의 AWS DMS 엔드포인트가 인증 메커니즘으로 구성되어 있는지 확인합니다. 엔드포인트에 인증 유형이 설정되지 않은 경우 제어가 실패합니다.

AWS Database Migration Service MongoDB에 대한 두 가지 인증 방법, 즉 몽고DB 버전 2.x의 경우 MongoDB-CR, MongoDB 버전 3.x 이상을 위한 SCRAM-SHA-1 인증 방법을 지원합니다. 이러한 인증 방법은 사용자가 암호를 사용하여 데이터베이스에 액세스하려는 경우 MongoDB 암호를 인증하고 암호화하는 데 사용됩니다. AWS DMS 엔드포인트 인증을 통해 인증된 사용자만 데이터베이스 간에 마이그레이션되는 데이터에 액세스하고 수정할 수 있습니다. 적절한 인증을 받지 않으면 권한이 없는 사용자가 마이그레이션 프로세스 중에 민감한 데이터에 액세스할 수 있습니다. 이로 인해 데이터 침해, 데이터 손실 또는 기타 보안 사고가 발생할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

MongoDB용 DMS 엔드포인트에서 인증 메커니즘을 활성화하려면 사용 설명서의 MongoDB를 소스로 사용을 참조하십시오. AWS DMSAWS Database Migration Service

[DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.R5 SC-8, NIST.800-53.r5 SC-13

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::DMS::Endpoint`

AWS Config 규칙: `dms-redis-tls-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Redis용 AWS DMS 엔드포인트가 TLS 연결로 구성되어 있는지 확인합니다. 엔드포인트에 TLS가 활성화되어 있지 않으면 제어가 실패합니다.

TLS는 인터넷을 통해 애플리케이션 또는 데이터베이스 간에 데이터를 전송할 때 end-to-end 보안을 제공합니다. DMS 엔드포인트에 SSL 암호화를 구성하면 마이그레이션 프로세스 중에 원본 및 대상 데이터베이스 간의 암호화된 통신이 가능해집니다. 이렇게 하면 악의적인 공격자가 민감한 데이터를 도청하고 가로채는 것을 방지할 수 있습니다. SSL 암호화를 사용하지 않으면 민감한 데이터에 액세스하여 데이터 침해, 데이터 손실 또는 기타 보안 사고가 발생할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Redis용 DMS 엔드포인트에서 TLS 연결을 활성화하려면 사용 설명서의 Redis를 대상으로 사용을 참조하십시오. AWS Database Migration ServiceAWS Database Migration Service

Amazon DocumentDB 제어

이러한 제어는 Amazon DocumentDB 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다. AWS 리전자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `docdb-cluster-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DocumentDB 클러스터가 저장 시 암호화되는지 확인합니다. Amazon DocumentDB 클러스터가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 이러한 데이터의 기밀을 보호하여 권한이 없는 사용자가 데이터에 액세스할 위험을 줄일 수 있습니다. Amazon DocumentDB 클러스터의 데이터는 추가 보안 계층을 위해 저장 시 암호화되어야 합니다. Amazon DocumentDB는 256비트 고급 암호화 표준(AES-256)을 사용하여 AWS Key Management Service (AWS KMS)에 저장된 암호화 키를 사용하여 데이터를 암호화합니다.

이제 Security Hub가 와 통합되었습니다

Amazon DocumentDB 클러스터를 생성할 때 저장 시 암호화를 활성화할 수 있습니다. 클러스터를 생성한 후에는 암호화 설정을 변경할 수 없습니다. 자세한 내용은 Amazon DocumentDB 개발자 안내서의 Amazon DocumentDB 클러스터에 대한 저장 시 암호화 활성화를 참조하십시오.

[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-12

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `docdb-cluster-backup-retention-check`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
`minimumBackupRetentionPeriod`	백업 보존 기간(일수)	Integer	7~35	7	

이 제어는 Amazon DocumentDB 클러스터의 백업 보존 기간이 지정된 기간 이상인지 여부를 확인합니다. 백업 보존 기간이 지정된 기간 미만인 경우 제어가 실패합니다. 백업 보존 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 7일을 사용합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구하고 시스템의 복원력을 강화할 수 있습니다. Amazon DocumentDB 클러스터의 백업을 자동화하면 시스템을 특정 시점으로 복원하고 가동 중지 시간과 데이터 손실을 최소화할 수 있습니다. Amazon DocumentDB에서 클러스터의 기본 백업 보존 기간은 1일입니다. 이 제어를 통과하려면 이 값을 7일에서 35일 사이의 값으로 늘려야 합니다.

이제 Security Hub가 와 통합되었습니다

Amazon DocumentDB 클러스터의 백업 보존 기간을 변경하려면 Amazon DocumentDB 개발자 안내서의 Amazon DocumentDB 클러스터 수정을 참조하세요. 백업에서 백업 보존 기간을 선택합니다.

[DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS:DBSnapshot`

AWS Config 규칙: `docdb-cluster-snapshot-public-prohibited`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인지 여부를 확인합니다. 수동 클러스터 스냅샷이 퍼블릭인 경우 제어가 실패합니다.

Amazon DocumentDB 수동 클러스터 스냅샷은 의도한 경우가 아니면 공개해서는 안 됩니다. 암호화되지 않은 수동 스냅샷을 공개로 공유하면 모든 AWS 계정에서 해당 스냅샷을 사용할 수 있습니다. 퍼블릭 스냅샷은 의도하지 않은 데이터 노출을 초래할 수 있습니다.

> **Note**
>
> 이 제어는 수동 클러스터 스냅샷을 평가합니다. Amazon DocumentDB 자동 클러스터 스냅샷은 공유할 수 없습니다. 그러나 자동 스냅샷을 복사하여 수동 스냅샷을 생성한 다음 복사본을 공유할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Amazon DocumentDB 수동 클러스터 스냅샷에 대한 퍼블릭 액세스를 제거하려면 Amazon DocumentDB 개발자 안내서의 스냅샷 공유를 참조하십시오. 프로그래밍 방식으로 Amazon DocumentDB 작업 `modify-db-snapshot-attribute`을 사용할 수 있습니다. `attribute-name`를 `restore`으로 설정하고 `values-to-remove`을 `all`로 설정합니다.

[DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `docdb-cluster-audit-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon DocumentDB 클러스터가 감사 로그를 Amazon Logs에 게시하는지 여부를 확인합니다. CloudWatch 클러스터가 감사 로그를 Logs에 게시하지 않으면 제어가 실패합니다. CloudWatch

Amazon DocumentDB(MongoDB 호환)를 사용하면 클러스터에서 수행된 이벤트를 감사할 수 있습니다. 기록되는 이벤트의 예로는 성공 또는 실패한 인증 시도, 데이터베이스에서 모음 삭제 또는 인덱스 생성이 있습니다. Amazon DocumentDB에서는 기본적으로 감사가 비활성화되어 있으므로 이를 활성화하려면 조치를 취해야 합니다.

이제 Security Hub가 와 통합되었습니다

Amazon DocumentDB 감사 로그를 CloudWatch 로그에 게시하려면 Amazon DocumentDB 개발자 안내서의 감사 활성화를 참조하십시오.

[DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `docdb-cluster-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DocumentDB 클러스터의 삭제 방지 기능 활성화 여부를 확인합니다. 클러스터에 삭제 방지 기능이 활성화되지 않은 경우 제어가 실패합니다.

클러스터 삭제 방지를 활성화하면 우발적인 데이터베이스 삭제 또는 권한 없는 사용자에 의한 삭제에 대한 추가 보호 계층이 제공됩니다. 삭제 방지가 활성화되어 있는 동안에는 Amazon DocumentDB 클러스터가 삭제될 수 없습니다. 삭제 요청이 성공하려면 먼저 삭제 방지를 비활성화해야 합니다. Amazon DocumentDB 콘솔에서 클러스터를 생성하면 삭제 방지 기능이 기본적으로 활성화됩니다.

이제 Security Hub가 와 통합되었습니다

기존 Amazon DocumentDB 클러스터에 대한 삭제 방지를 활성화하려면 Amazon DocumentDB 개발자 안내서의 Amazon DocumentDB 클러스터 수정을 참조하십시오. 클러스터 수정 섹션에서 삭제 방지 활성화를 선택합니다.

Amazon DynamoDB 제어

이러한 제어는 DynamoDB 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다. AWS 리전자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::DynamoDB::Table`

AWS Config 규칙: dynamodb-autoscaling-enabled

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	유효한 사용자 지정 값	Security Hub 기본값
minProvisionedReadCapacity	DynamoDB Auto Scaling에 프로비저닝된 최소 읽기 용량 유닛 수	Integer	1~40000	기본값 없음
targetReadUtilization	읽기 용량의 목표 사용률(%)	Integer	20~90	기본값 없음
minProvisionedWriteCapacity	DynamoDB Auto Scaling에 프로비저닝된 최소 쓰기 용량 유닛 수	Integer	1~40000	기본값 없음
targetWriteUtilization	쓰기 용량의 목표 사용률(%)	Integer	20~90	기본값 없음

이 제어는 Amazon DynamoDB 테이블이 필요에 따라 읽기 및 쓰기 용량을 확장할 수 있는지 여부를 확인합니다. 테이블이 온디맨드 용량 모드 또는 Auto Scaling이 구성된 프로비저닝 모드를 사용하는 경우 이 제어가 실패합니다. 기본적으로 이 제어는 특정 수준의 읽기 또는 쓰기 용량에 관계없이 이러한 모드 중 하나만 구성하면 됩니다. 필요에 따라 특정 수준의 읽기 및 쓰기 용량 또는 목표 사용률을 요구하는 사용자 지정 파라미터 값을 제공할 수 있습니다.

수요에 따라 용량을 확장하면 제한 예외를 방지하여 애플리케이션의 가용성을 유지하는 데 도움이 됩니다. 온디맨드 용량 모드의 DynamoDB 테이블은 DynamoDB 처리량 기본 테이블 할당량에 의해서만 제한됩니다. 할당량을 늘리려면 Auto Scaling을 사용하는 프로비저닝 AWS Support모드에서.DynamoDB 테이블로 지원 티켓을 제출하고 트래픽 패턴에 따라 프로비저닝된 처리 용량을 동적으로 조정하면 됩니다. DynamoDB 요청 제한에 대한 자세한 내용은 Amazon DynamoDB 개발자 안내서의 요청 제한 및 버스트 용량을 참조하세요.

이제 Security Hub가 와 통합되었습니다

용량 모드에서 기존 테이블에 대해 DynamoDB Auto Scaling을 활성화하려면 Amazon DynamoDB 개발자 안내서의 기존 테이블에 대한 DynamoDB Auto Scaling 활성화를 참조하십시오.

[DynamoDB.2] DynamoDB 테이블에는 복구가 활성화되어 있어야 합니다. point-in-time

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::DynamoDB::Table`

AWS Config 규칙: `dynamodb-pitr-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon DynamoDB 테이블에 대해 point-in-time 복구 (PITR) 가 활성화되었는지 여부를 확인합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구할 수 있습니다. 또한 시스템의 복원력을 강화합니다. point-in-time DynamoDB 복구는 DynamoDB 테이블의 백업을 자동화합니다. 이는 실수로 인한 삭제 또는 쓰기 작업을 복구하는 데 걸리는 시간을 줄여줍니다. PITR이 활성화된 DynamoDB 테이블은 최근 35일 중 원하는 시점으로 복원할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

DynamoDB 테이블을 특정 시점으로 복원하려면 Amazon DynamoDB 개발자 안내서의 DynamoDB 테이블을 특정 시점으로 복원을 참조하십시오.

[DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::DAX::Cluster`

AWS Config 규칙: `dax-encryption-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Amazon DynamoDB 액셀러레이터 (DAX) 클러스터가 유휴 상태에서 암호화되었는지 여부를 확인합니다. DAX 클러스터가 유휴 상태에서 암호화되지 않으면 제어가 실패합니다.

저장된 데이터를 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. AWS암호화는 권한이 없는 사용자가 데이터에 액세스하는 능력을 제한하기 위해 또 다른 액세스 제어 세트를 추가합니다. 예를 들어 데이터를 읽기 전에 해독하려면 API 권한이 필요합니다.

이제 Security Hub가 와 통합되었습니다

클러스터가 생성된 후에는 저장 시 암호화를 활성화하거나 비활성화할 수 없습니다. 저장 시 암호화를 활성화하려면 클러스터를 다시 생성해야 합니다. 저장 시 암호화가 활성화된 DAX 클러스터를 생성하는 방법에 대한 자세한 지침은 Amazon DynamoDB 개발자 안내서의 AWS Management Console를 사용하여 저장 시 암호화 활성화를 참조하십시오.

[DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::DynamoDB::Table`

AWS Config 규칙: **`dynamodb-resources-protected-by-backup-plan`**

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`backupVaultLockCheck`	컨트롤은 매개변수가 로 `PASSED` 설정되어 `true` 있고 리소스가 AWS Backup Vault Lock을 사용하는지 여부를 확인합니다.	불	`true` 또는 `false`	기본값 없음

이 제어는 `ACTIVE` 상태의 Amazon DynamoDB 테이블이 백업 계획에 포함되는지 여부를 평가합니다. DynamoDB 테이블이 백업 계획에 포함되지 않는 경우 제어가 실패합니다. `backupVaultLockCheck`파라미터를 로 `true` 설정하면 DynamoDB 테이블이 잠긴 저장소에 백업된 경우에만 제어가 통과합니다. AWS Backup

AWS Backup 데이터 백업을 중앙 집중화하고 자동화하는 데 도움이 되는 완전 관리형 백업 서비스입니다. AWS 서비스를 사용하면 데이터 백업 빈도 및 백업 보존 기간과 같은 백업 요구 사항을 정의하는 백업 계획을 만들 수 있습니다. AWS Backup백업 계획에 DynamoDB 테이블을 포함하면 의도하지 않은 손실이나 삭제로부터 데이터를 보호할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

DynamoDB 테이블을 백업 계획에 추가하려면 개발자 안내서의 백업 계획에 리소스 할당을 참조하십시오. AWS Backup AWS Backup

[DynamoDB.5] DynamoDB 테이블에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::DynamoDB::Table`

AWS Config 규칙: `tagged-dynamodb-table` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon DynamoDB 테이블에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 테이블에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 테이블에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

DynamoDB 테이블에 태그를 추가하려면 Amazon DynamoDB 개발자 안내서의 DynamoDB 리소스 태그 지정을 참조하십시오.

[DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 중간

리소스 유형: `AWS::DynamoDB::Table`

AWS Config 규칙: **`dynamodb-table-deletion-protection-enabled`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DynamoDB 테이블의 삭제 방지 기능 활성화 여부를 확인합니다. DynamoDB 테이블에 삭제 방지 기능이 활성화되지 않은 경우 제어가 실패합니다.

삭제 보호 속성을 사용하여 DynamoDB 테이블이 실수로 삭제되지 않도록 보호할 수 있습니다. 테이블에 이 속성을 활성화하면 관리자가 일반적인 테이블 관리 작업을 수행하는 동안 테이블이 실수로 삭제되는 것을 방지할 수 있습니다. 이렇게 하면 정상적인 비즈니스 운영이 중단되는 것을 방지하는 데 도움이 됩니다.

이제 Security Hub가 와 통합되었습니다

DynamoDB 테이블에 대한 삭제 보호를 활성화하려면 Amazon DynamoDB 개발자 안내서의 삭제 보호 사용을 참조하세요.

[DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-17, NIST.800-53.R5 SC-8, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::DynamoDB::Table`

AWS Config 규칙: **`dax-tls-endpoint-encryption`**

스케줄 유형: 주기적

파라미터: 없음

이 제어는 엔드포인트 암호화 유형이 TLS로 설정된 상태에서 Amazon DynamoDB 가속기 (DAX) 클러스터가 전송 중에 암호화되는지 여부를 확인합니다. DAX 클러스터가 전송 중에 암호화되지 않으면 제어가 실패합니다.

HTTPS (TLS) 는 잠재적 공격자가 네트워크 트래픽을 도청하거나 조작하기 위해 person-in-the-middle 또는 유사한 공격을 사용하는 것을 방지하는 데 사용할 수 있습니다. TLS를 통한 암호화된 연결만 DAX 클러스터에 액세스하도록 허용해야 합니다. 하지만 전송 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 암호화를 켠 상태에서 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 파악해야 합니다.

이제 Security Hub가 와 통합되었습니다

DAX 클러스터를 생성한 후에는 TLS 암호화 설정을 변경할 수 없습니다. 기존 DAX 클러스터를 암호화하려면 전송 중 암호화가 활성화된 새 클러스터를 생성하고 애플리케이션의 트래픽을 해당 클러스터로 이동한 다음 이전 클러스터를 삭제하십시오. 자세한 내용은 Amazon DynamoDB 개발자 안내서의 삭제 보호 기능 사용을 참조하세요.

Amazon Elastic Container Registry 제어

이러한 제어는 Amazon ECR 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 RA-5

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::ECR::Repository`

AWS Config 규칙: `ecr-private-image-scanning-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 프라이빗 Amazon ECR 리포지토리에 이미지 스캔이 구성되어 있는지 확인합니다. 프라이빗 ECR 리포지토리가 푸시 시 스캔 또는 연속 스캔에 대해 구성되지 않은 경우 제어가 실패합니다.

ECR 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 구성하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.

이제 Security Hub가 와 통합되었습니다

ECR 리포지토리의 이미지 스캔을 구성하려면 Amazon Elastic Container 레지스트리 사용 설명서의 이미지 스캔을 참조하십시오.

[ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-8(1)

범주: 식별 > 인벤토리 > 태깅

심각도: 중간

리소스 유형: `AWS::ECR::Repository`

AWS Config 규칙: `ecr-private-tag-immutability-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 프라이빗 ECR 리포지토리에 태그 불변성이 활성화되어 있는지 확인합니다. 프라이빗 ECR 리포지토리에 태그 불변성이 비활성화된 경우 이 제어가 실패합니다. 이 규칙은 태그 불변성이 활성화되고 값이 `IMMUTABLE`인 경우 통과됩니다.

Amazon ECR Tag Immuability를 사용하면 고객은 이미지를 추적하고 고유하게 식별하는 안정적인 메커니즘으로 이미지 설명 태그를 활용할 수 있습니다. 불변 태그는 정적입니다. 즉, 각 태그는 고유한 이미지를 참조합니다. 정적 태그를 사용하면 항상 동일한 이미지가 배포되므로 안정성과 확장성이 향상됩니다. 태그 불변성을 구성하면 태그 불변성으로 인해 태그가 재정의되지 않아 공격 표면이 줄어듭니다.

이제 Security Hub가 와 통합되었습니다

변경할 수 없는 태그가 구성된 리포지토리를 만들거나 기존 리포지토리의 이미지 태그 변경 가능성 설정을 업데이트하려면 Amazon Elastic Container Registry 사용 설명서의 이미지 태그 변경 가능성을 참조하십시오.

[ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::ECR::Repository`

AWS Config 규칙: `ecr-private-lifecycle-policy-configured`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECR 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 저장소에 수명 주기 정책이 구성되어 있지 않으면 이 제어가 실패합니다.

Amazon ECR 수명 주기 정책을 통해 리포지토리의 이미지에 대한 수명 주기 관리를 지정할 수 있습니다. 수명 주기 정책을 구성하면 사용하지 않는 이미지의 정리 및 사용 기간 또는 개수에 따른 이미지 만료를 자동화할 수 있습니다. 이러한 작업을 자동화하면 저장소에서 오래된 이미지를 실수로 사용하는 것을 방지할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

수명 주기 정책을 구성하려면 Amazon Elastic Container Registry 사용 설명서의 수명 주기 정책 미리 보기 생성을 참조하십시오.

[ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::ECR::PublicRepository`

AWS Config 규칙: `tagged-ecr-publicrepository` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon ECR 퍼블릭 리포지토리에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. 퍼블릭 리포지토리에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 공용 저장소에 키 태그가 지정되지 않은 경우에는 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

ECR 퍼블릭 리포지토리에 태그를 추가하려면 Amazon Elastic 컨테이너 레지스트리 사용 설명서의 Amazon ECR 퍼블릭 리포지토리에 태그 지정을 참조하십시오.

Amazon ECS 제어

이러한 제어는 Amazon ECS 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: `ecs-task-definition-user-for-host-mode-check`

스케줄 유형: 변경이 트리거됨

파라미터:

- `SkipInactiveTaskDefinitions`: `true`(사용자 지정할 수 없음)

이 제어는 호스트 네트워킹 모드를 사용하는 활성 Amazon ECS 작업 정의에 `privileged` 또는 `user` 컨테이너 정의가 있는지 확인합니다. 호스트 네트워크 모드가 있는 작업 정의와 `privileged=false`, 비어 있음 및 `user=root`, 또는 비어 있는 컨테이너 정의에 대한 제어가 실패합니다.

이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다.

이 제어의 목적은 호스트 네트워크 모드를 사용하는 작업을 실행할 때 액세스가 의도적으로 정의되도록 하는 것입니다. 작업 정의에 상승된 권한이 있는 것은 해당 구성을 선택했기 때문입니다. 이 제어는 태스크 정의에 호스트 네트워킹이 활성화되어 있고 사용자가 상승된 권한을 선택하지 않은 경우 예기치 않은 권한 상승을 확인합니다.

이제 Security Hub가 와 통합되었습니다

태스크 정의를 업데이트하는 방법에 대한 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 작업 정의 업데이트를 참조하십시오.

작업 정의를 업데이트하면 이전 작업 정의에서 시작된 실행 중인 작업은 업데이트되지 않습니다. 실행 중인 작업을 업데이트하려면 새 작업 정의를 사용하여 작업을 재배포해야 합니다.

[ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::ECS::Service`

AWS Config규칙: `ecs-service-assign-public-ip-disabled` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

- `exemptEcsServiceArns`(사용자 지정할 수 없음). Security Hub는 이 파라미터를 채우지 않습니다. 이 규칙에서 제외되는 Amazon ECS 서비스의 ARN을 쉼표로 구분한 목록입니다.

  Amazon ECS 서비스의 `AssignPublicIP`가 `ENABLED`으로 설정되어 있고 이 파라미터 목록에 지정된 경우 이 규칙은 `COMPLIANT`입니다.

  Amazon ECS 서비스의 `AssignPublicIP`가 `ENABLED`으로 설정되어 있고 이 파라미터 목록에 지정되지 않은 경우 이 규칙은 `NON_COMPLIANT`입니다.

이 제어는 Amazon ECS 서비스가 퍼블릭 IP 주소를 자동으로 할당하도록 구성되었는지 여부를 확인합니다. 이 제어는 `AssignPublicIP`가 `ENABLED`인 경우 실패합니다. 이 제어는 `AssignPublicIP`가 `DISABLED`인 경우 통과됩니다.

퍼블릭 IP 주소는 인터넷을 통해 연결할 수 있는 IPv 주소입니다. 퍼블릭 IP 주소로 Amazon ECS 인스턴스를 시작하면 인터넷에서 Amazon ECS 인스턴스에 연결할 수 있습니다. Amazon ECS 서비스는 공개적으로 액세스할 수 없어야 합니다. 이렇게 하면 컨테이너 애플리케이션 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

이제 Security Hub가 와 통합되었습니다

자동 퍼블릭 IP 할당을 비활성화하려면 Amazon Elastic Container Service 개발자 안내서의 서비스에 대한 VPC 및 보안 그룹 설정을 구성하려면을 참조하십시오.

[ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 식별 > 리소스 구성

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config규칙: ecs-task-definition-pid -모드 확인

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 작업 정의가 호스트의 프로세스 네임스페이스를 컨테이너와 공유하도록 구성되어 있는지 확인합니다. 태스크 정의가 호스트의 프로세스 네임스페이스를 호스트에서 실행되는 컨테이너와 공유하면 제어가 실패합니다. 이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다.

프로세스 ID(PID) 네임스페이스는 프로세스 간 분리를 제공합니다. 시스템 프로세스가표시되는 것을 방지하고 PID 1을 포함한 PID를 재사용할 수 있습니다. 호스트의 PID 네임스페이스를 컨테이너와 공유하면 컨테이너는 호스트 시스템의 모든 프로세스를 볼 수 있습니다. 이렇게 하면 호스트와 컨테이너 간의 프로세스 수준 격리의 이점이 줄어듭니다. 이러한 상황에서는 프로세스를 조작하고 종료하는 기능을 포함하여 호스트 자체에 있는 프로세스에 대한 무단 액세스가 발생할 수 있습니다. 고객은 호스트의 프로세스 네임스페이스를 호스트에서 실행되는 컨테이너와 공유해서는 안 됩니다.

이제 Security Hub가 와 통합되었습니다

태스크 정의에 대해 `pidMode`를 구성하려면 Amazon Elastic Container Service 개발자 안내서의 태스크 정의 파라미터를 참조하십시오.

[ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리 > 루트 사용자 액세스 제한

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config규칙: ecs-containers-nonprivileged

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 태스크 정의의 컨테이너 정의에 있는 `privileged` 파라미터가 `true`로 설정되어 있는지 확인합니다. 이 파라미터가 `true`과 같으면 제어가 실패합니다. 이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다.

ECS 태스크 정의에서 상승된 권한을 제거하는 것이 좋습니다. 권한 파라미터가 `true`인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 상승된 권한을 부여받습니다(루트 사용자와 비슷함).

이제 Security Hub가 와 통합되었습니다

태스크 정의에 대한 `privileged` 파라미터를 구성하려면 Amazon Elastic Container Service 개발자 안내서의 고급 컨테이너 정의 파라미터를 참조하십시오.

[ECS.5] ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config규칙: ecs-containers-readonly-access

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 컨테이너가 마운트된 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되는지 확인합니다. `readonlyRootFilesystem` 파라미터가 `false`로 설정되거나 파라미터가 작업 정의 내 컨테이너 정의에 없는 경우 제어가 실패합니다. 이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다.

이 옵션을 활성화하면 파일 시스템 폴더 및 디렉터리에 대한 명시적인 읽기-쓰기 권한이 없는 한 컨테이너 인스턴스의 파일 시스템을 조작하거나 쓸 수 없으므로 보안 공격 벡터가 줄어듭니다. 이 제어는 또한 최소 권한 원칙을 준수합니다.

이제 Security Hub가 와 통합되었습니다

컨테이너 정의를 루트 파일 시스템에 대한 읽기 전용 액세스로 제한

1. https://console.aws.amazon.com/ecs/에서 Amazon ECS 클래식 콘솔을 엽니다.
2. 탐색 창에서 태스크 정의를 선택합니다.
3. 업데이트해야 하는 컨테이너 정의가 있는 작업 정의를 선택합니다. 각각에 대해 다음 단계를 완료하십시오.
   - 드롭다운에서 JSON으로 새 개정 생성을 선택합니다.
   - `readonlyRootFilesystem` 파라미터를 추가하고 작업 정의 내 컨테이너 정의에서 `true`로 설정합니다.
   - 생성을 선택합니다.

[ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 개발 > 하드 코딩되지 않은 보안 인증

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config규칙: ecs-no-environment-secrets

스케줄 유형: 변경이 트리거됨

파라미터:

- secretKeys = `AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`,`ECS_ENGINE_AUTH_DATA`(사용자 지정할 수 없음)

이 제어는 컨테이너 정의의 `environment` 파라미터에 있는 변수의 키 값에 `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` 또는 `ECS_ENGINE_AUTH_DATA`가 포함되어 있는지 확인합니다.

컨테이너 정의의 단일 환경 변수가 `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` 또는 `ECS_ENGINE_AUTH_DATA`와 같으면 이 제어가 실패합니다. 이 제어에는 Amazon S3와 같은 다른 위치에서 전달된 환경 변수는 포함되지 않습니다. 이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다.

AWS Systems Manager 파라미터 스토어는 조직의 보안 태세를 개선하는 데 도움이 될 수 있습니다. 암호와 보안 인증을 컨테이너 인스턴스로 직접 전달하거나 코드에 하드 코딩하는 대신 Parameter Store를 사용하여 암호와 보안 인증을 저장하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

SSM을 사용하여 파라미터를 생성하려면 AWS Systems Manager 사용 설명서의 Systems Manager 파라미터 생성을 참조하십시오. 암호를 지정하는 작업 정의 생성에 대한 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 Secrets Manager를 사용하여 중요한 데이터 지정을 참조하십시오.

[ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config규칙: ecs-task-definition-log -구성

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어 최신 활성 Amazon ECS 작업 정의에 로깅 구성이 지정되어 있는지 확인합니다. 작업 정의에 정의된 `logConfiguration` 속성이 없거나 하나 이상의 컨테이너 정의에서 `logDriver`의 값이 null인 경우 제어가 실패합니다.

로깅은 Amazon ECS의 안정성, 가용성 및 성능을 유지하는 데 도움이 됩니다. 작업 정의에서 데이터를 수집하면 가시성이 제공되므로 프로세스를 디버깅하고 오류의 근본 원인을 찾는 데 도움이 됩니다.

ECS 작업 정의에 정의할 필요가 없는 로깅 솔루션(예: 타사 로깅 솔루션)을 사용하는 경우 로그가 제대로 캡처되고 전달되었는지 확인한 후 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Amazon ECS 작업 정의의 로그 구성을 정의하려면 Amazon Elastic Container Service 개발자 안내서의 작업 정의에 로그 구성 지정을 참조하십시오.

[ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::ECS::Service`

AWS Config규칙: `ecs-fargate-latest-platform-version`

스케줄 유형: 변경이 트리거됨

파라미터:

- `latestLinuxVersion: 1.4.0`(사용자 지정할 수 없음)
- `latestWindowsVersion: 1.0.0`(사용자 지정할 수 없음)

이 제어는 Amazon ECS Fargate 서비스가 최신 Fargate 플랫폼 버전을 실행하고 있는지 확인합니다. 플랫폼 버전이 최신 버전이 아닌 경우 이 제어가 실패합니다.

AWS Fargate 플랫폼 버전은 커널과 컨테이너 런타임 버전의 조합인 Fargate 작업 인프라의 특정 런타임 환경을 나타냅니다. 런타임 환경이 발전함에 따라 새 플랫폼 버전이 출시됩니다. 예를 들어 커널 또는 운영 체제 업데이트, 새로운 기능, 버그 수정 또는 보안 업데이트용으로 새 버전이 릴리스될 수 있습니다. 보안 업데이트 및 패치는 Fargate 태스크에서 자동 배포됩니다. 플랫폼 버전에 영향을 미치는 보안 문제가 발견되면 플랫폼 버전을 AWS 패치합니다.

이제 Security Hub가 와 통합되었습니다

플랫폼 버전을 비롯한 기존 서비스를 업데이트하려면 Amazon Elastic Container Service 개발자 안내서의 서비스 업데이트를 참조하십시오.

[ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::ECS::Cluster`

AWS Config규칙: `ecs-container-insights-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 ECS 클러스터가 컨테이너 인사이트를 사용하는지 확인합니다. Container Insights가 클러스터에 설정되지 않은 경우 이 제어는 실패합니다.

모니터링은 Amazon ECS 클러스터의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. CloudWatch Container Insights를 사용하여 컨테이너화된 애플리케이션 및 마이크로서비스의 지표와 로그를 수집, 집계 및 요약할 수 있습니다. CloudWatch CPU, 메모리, 디스크, 네트워크 등 많은 리소스에 대한 메트릭을 자동으로 수집합니다. 또한 Container Insights는 컨테이너 재시작 오류 같은 진단 정보를 제공하여 문제를 격리하고 신속하게 해결할 수 있도록 도와줍니다. 또한 컨테이너 인사이트가 수집하는 지표에 대해 CloudWatch 경보를 설정할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

컨테이너 인사이트를 사용하려면 Amazon 사용 CloudWatch 설명서의 서비스 업데이트를 참조하십시오.

[ECS.13] ECS 서비스에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::ECS::Service`

AWS Config규칙: `tagged-ecs-service` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon ECS 서비스에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. 서비스에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 서비스에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

ECS 서비스에 태그를 추가하려면 Amazon Elastic 컨테이너 서비스 개발자 안내서의 Amazon ECS 리소스 태그 지정을 참조하십시오.

[ECS.14] ECS 클러스터에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::ECS::Cluster`

AWS Config규칙: `tagged-ecs-cluster` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon ECS 클러스터에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. 클러스터에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 클러스터에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

ECS 클러스터에 태그를 추가하려면 Amazon Elastic 컨테이너 서비스 개발자 안내서의 Amazon ECS 리소스 태그 지정을 참조하십시오.

[ECS.15] ECS 작업 정의에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config규칙: `tagged-ecs-taskdefinition` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon ECS 작업 정의에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. 작업 정의에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 작업 정의에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

ECS 작업 정의에 태그를 추가하려면 Amazon Elastic 컨테이너 서비스 개발자 안내서의 Amazon ECS 리소스 태그 지정을 참조하십시오.

Amazon Elastic Compute Cloud 제어

이러한 제어는 Amazon EC2 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[EC2.1] Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: `ebs-snapshot-public-restorable-check`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Elastic Block Store 스냅샷이 퍼블릭이 아닌지 여부를 확인합니다. 누구나 Amazon EBS 스냅샷을 복원할 수 있는 경우 제어가 실패합니다.

EBS 스냅샷은 특정 시점에 EBS 볼륨의 데이터를 Amazon S3에 백업하는 데 사용됩니다. 스냅샷을 사용하여 EBS 볼륨의 이전 상태를 복원할 수 있습니다. 스냅샷을 퍼블릭과 공유하는 것은 거의 허용되지 않습니다. 일반적으로 스냅샷을 공개적으로 공유하기로 결정한 것은 오류이거나 그 의미를 완전히 이해하지 못한 채 이루어졌습니다. 이 확인을 통해 이러한 모든 공유가 완전히 계획되고 의도적으로 이루어졌는지 확인할 수 있습니다.

퍼블릭 EBS 스냅샷을 비공개로 만들려면 Amazon EC2 사용 설명서의 스냅샷 공유를 참조하십시오. 작업, 권한 수정에서 비공개를 선택합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/2.1, CIS 재단 벤치마크 v1.2.0/4.3, CIS 재단 벤치마크 v1.4.0/5.3, CIS AWS 재단 벤치마크 v3.0.0/5.4, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4, AWS NIST.800-53.r5 AC -4 (21), NIST.800-53.r5 SC-7, AWS NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (4) (5)

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `vpc-default-security-group-closed`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 VPC의 기본 보안 그룹이 인바운드 또는 아웃바운드 트래픽을 허용하는지 여부를 확인합니다. 보안 그룹이 인바운드 또는 아웃바운드 트래픽을 허용하는 경우 제어가 실패합니다.

기본 보안 그룹의 규칙은 동일한 보안 그룹에 할당된 네트워크 인터페이스(및 연결된 인스턴스)로부터의 모든 아웃바운드 및 인바운드 트래픽을 허용합니다. 기본 보안 정책을 사용하지 않는 것이 좋습니다. 기본 보안 그룹은 삭제할 수 없으므로 기본 보안 그룹 규칙 설정을 변경하여 인바운드 및 아웃바운드 트래픽을 제한해야 합니다. 이렇게 하면 EC2 인스턴스와 같은 리소스에 대해 기본 보안 그룹이 실수로 구성된 경우, 의도하지 않은 트래픽을 방지할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

이 문제를 해결하려면 먼저 최소 권한의 보안 그룹을 새로 만들어야 합니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 생성을 참조하십시오. 그런 다음 새 보안 그룹을 EC2 인스턴스에 할당합니다. 지침은 Amazon EC2 사용 설명서의 인스턴스 보안 그룹 변경을 참조하십시오.

새 보안 그룹을 리소스에 할당한 후 기본 보안 그룹에서 모든 인바운드 및 아웃바운드 규칙을 제거합니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 규칙 삭제를 참조하십시오.

[EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::EC2::Volume`

AWS Config 규칙: `encrypted-volumes`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 연결 상태인 EBS 볼륨이 암호화되었는지 확인합니다. 이 확인을 통과하려면 EBS 볼륨이 사용 중이고 암호화되어야 합니다. EBS 볼륨이 연결되어 있지 않으면 이 확인 범위에 속하지 않습니다.

EBS 볼륨에서 중요한 데이터의 보안을 강화하려면 유휴 상태에서 EBS 암호화를 활성화해야 합니다. Amazon EBS 암호화는 자체 키 관리 인프라를 사용자가 직접 구축, 유지 및 보호할 필요가 없는 EBS 리소스에 대한 간단한 암호화 솔루션을 제공합니다. 암호화된 볼륨과 스냅샷을 생성할 때 KMS 키를 사용합니다.

Amazon EBS 암호화에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EBS 암호화를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

기존의 암호화되지 않은 볼륨 또는 스냅샷을 암호화하는 직접적인 방법은 없습니다. 새 볼륨이나 스냅샷을 생성할 때만 암호화할 수 있습니다.

암호화를 기본적으로 활성화한 경우 Amazon EBS는 Amazon EBS 암호화에 대한 사용자의 기본 키를 사용하여, 결과로 얻은 새로운 볼륨 또는 스냅샷을 암호화합니다. 암호화를 기본적으로 활성화하지 않은 경우라도 개별 볼륨 또는 스냅샷을 생성할 때 암호화를 활성화할 수 있습니다. 두 경우 모두 Amazon EBS 암호화의 기본 키를 재정의하고 대칭 고객 관리형 키를 선택할 수 있습니다.

자세한 내용은 Amazon EC2 사용 설명서의 Amazon EBS 볼륨 생성 및 Amazon EBS 스냅샷 복사를 참조하십시오.

[EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리

심각도: 중간

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `ec2-stopped-instance`

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`AllowedDays`	결과 실패를 생성하기 전에 EC2 인스턴스를 중지된 상태로 둘 수 있는 기간(일수)	Integer	`1~365`	`30`

이 제어는 Amazon EC2 인스턴스가 허용된 일수보다 오랫동안 중지되어 있는지 확인합니다. EC2 인스턴스가 최대 허용 기간보다 오랫동안 중지되면 제어가 실패합니다. 최대 허용 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 30일을 사용합니다.

EC2 인스턴스를 상당 기간 실행하지 않으면 인스턴스가 활발하게 유지 관리(분석, 패치, 업데이트)되지 않아 보안 위험이 발생합니다. 나중에 출시할 경우 적절한 유지 관리가 이루어지지 않아 사용자 환경에 예상치 못한 문제가 발생할 수 있습니다. AWS 일정 기간 동안 EC2 인스턴스를 비활성 상태로 안전하게 유지 관리하려면 유지 관리를 위해 주기적으로 시작한 다음 유지 관리 후에 중지하세요. 이 프로세스는 자동화된 것이 이상적입니다.

이제 Security Hub가 와 통합되었습니다

비활성 EC2 인스턴스를 종료하려면 Amazon EC2 사용 설명서의 인스턴스 종료를 참조하십시오.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/2.9, CIS 재단 벤치마크 v1.4.0/3.9, AWS CIS 재단 벤치마크 v3.0.0/3.7, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.6, AWS NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-7, 5 SI-7 (8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::EC2::VPC`

AWS Config 규칙: `vpc-flow-logs-enabled`

스케줄 유형: 주기적

파라미터:

- `trafficType`: `REJECT`(사용자 지정할 수 없음)

이 제어는 Amazon VPC 흐름 로그가 발견되어 VPC에 대해 활성화되어 있는지 확인합니다. 트래픽 유형이 `Reject`로 설정되어 있습니다.

VPC 흐름 로그 기능을 사용하면 VPC의 네트워크 인터페이스에서 들어오고 나가는 IP 주소 트래픽에 대한 정보를 캡처할 수 있습니다. 흐름 로그를 만든 후 CloudWatch Logs에서 해당 데이터를 보고 검색할 수 있습니다. 비용을 줄이기 위해 Amazon S3로 흐름 로그를 전송할 수도 있습니다.

Security Hub에서는 VPC에 대한 패킷 거부에 대한 흐름 로깅을 활성화할 것을 권장합니다. 흐름 로그는 VPC를 통과하는 네트워크 트래픽에 대한 가시성을 제공하고 비정상적인 트래픽을 감지하거나 보안 워크플로 중에 통찰력을 제공할 수 있습니다.

기본적으로 레코드에는 소스, 대상 및 프로토콜을 포함하여 IP 주소 흐름의 다른 구성 요소에 대한 값이 포함됩니다. 로그 필드에 대한 자세한 내용 및 설명은 Amazon VPC 사용 설명서의 VPC 흐름 로그를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

VPC 흐름 로그를 생성하려면 Amazon VPC 사용 설명서의 흐름 로그 생성을 참조하십시오. Amazon VPC 콘솔을 연 다음 VPC를 선택합니다. 필터에서 거부 또는 전부를 선택합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.4.0/2.2.1, CIS AWS 재단 벤치마크 v3.0.0/2.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6) SC-13

범주: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `ec2-ebs-encryption-by-default`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Elastic Block Store(Amazon EBS)에 대해 계정 수준 암호화가 기본적으로 활성화되어 있는지 확인합니다. 계정 수준 암호화가 활성화되지 않은 경우 제어가 실패합니다.

계정에 암호화가 활성화되면 Amazon EBS 볼륨과 스냅샷 사본이 저장 중 암호화됩니다. 그러면 데이터 보호 계층이 하나 더 추가됩니다. 자세한 내용은 Amazon EC2 사용 설명서에서 기본적으로 암호화를 참조하세요.

단, R1, C1, M1의 인스턴스 유형은 암호화를 지원하지 않습니다.

이제 Security Hub가 와 통합되었습니다

Amazon EBS 볼륨의 기본 암호화를 구성하려면 Amazon EC2 사용 설명서의 기본 암호화를 참조하십시오.

[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v3.0.0/5.6, NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.r5 AC-6

카테고리: 보호 > 네트워크 보안

심각도: 높음

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `ec2-imdsv2-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 EC2 인스턴스 메타데이터 버전이 IMDSv2(인스턴스 메타데이터 서비스 버전 2)로 구성되어 있는지 확인합니다. IMDSv2에 대해 `HttpTokens`이 필수로 설정된 경우 제어가 통과됩니다. `HttpTokens`을 `optional`로 설정하면 제어가 실패합니다.

인스턴스 메타데이터를 사용하여 실행 중인 인스턴스를 구성하거나 관리합니다. IMDS는 자주 교체되는 임시 보안 인증 정보에 대한 액세스를 제공합니다. 이러한 보안 인증을 사용하면 민감한 보안 인증 정보를 수동으로 또는 프로그래밍 방식으로 인스턴스에 하드 코딩하거나 배포할 필요가 없습니다. IMDS는 모든 EC2 인스턴스에 로컬로 연결됩니다. 이는 특수한 "링크 로컬" IP 주소 169.254.169.254에서 실행됩니다. 이 IP 주소는 인스턴스에서 실행되는 소프트웨어에서만 액세스할 수 있습니다.

IMDS 버전 2에는 다음 유형의 취약성에 대한 새로운 보호 기능이 추가되었습니다. 이러한 취약성을 이용하여 IMDS에 액세스할 수 있습니다.

- 개방형 웹사이트 애플리케이션 방화벽
- 개방형 리버스 프록시
- 서버 측 요청 위조(SSRF) 취약성
- 개방형 Layer 3 방화벽 및 Network Address Translation(NAT)

Security Hub에서는 IMDSv2로 EC2 인스턴스를 구성할 것을 권장합니다.

이제 Security Hub가 와 통합되었습니다

IMDSv2를 사용하여 EC2 인스턴스를 구성하려면 Amazon EC2 사용 설명서의 IMDSv2를 요구하는 권장 경로를 참조하십시오.

[EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `ec2-instance-no-public-ip`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 EC2 인스턴스에 퍼블릭 IP 주소가 있는지 여부를 확인합니다. `publicIp` 필드가 EC2 인스턴스 구성 항목에 있으면 제어가 실패합니다. 이 제어는 IPv4 주소에만 적용됩니다.

퍼블릭 IPv4 주소는 인터넷을 통해 연결할 수 있는 IP 주소입니다. 퍼블릭 IP 주소로 인스턴스를 시작하는 경우 인터넷에서 EC2 인스턴스에 연결할 수 있습니다. 프라이빗 IPv4 주소는 인터넷을 통해 연결할 수 없는 IP 주소입니다. 동일한 VPC 또는 연결된 프라이빗 네트워크에 있는 EC2 인스턴스 간의 통신에 프라이빗 IPv4 주소를 사용할 수 있습니다.

IPv6 주소는 전역적으로 고유하므로 인터넷으로 접속할 수 있습니다. 그러나 기본적으로 모든 서브넷에는 IPv6 주소 지정 속성이 false로 설정되어 있습니다. IPv6에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC에서 IP 주소 지정을 참조하십시오.

퍼블릭 IP 주소를 사용하여 EC2 인스턴스를 유지 관리하는 합법적인 사용 사례가 있는 경우 이 제어에서 조사 결과를 숨길 수 있습니다. 프런트 엔드 아키텍처 옵션에 대한 자세한 내용은 AWS 아키텍처 블로그 또는 This Is My Architecture 시리즈를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

기본적으로 인스턴스에 퍼블릭 IP 주소가 할당되지 않도록 기본이 아닌 VPC를 사용하십시오.

EC2 인스턴스를 기본 VPC로 시작하면 퍼블릭 IP 주소가 할당됩니다. 기본 VPC가 아닌 VPC에서 EC2 인스턴스를 시작하는 경우 서브넷 구성에 따라 퍼블릭 IP 주소를 수신할지 여부가 결정됩니다. 서브넷에는 서브넷의 새 EC2 인스턴스가 퍼블릭 IPv4 주소 풀에서 퍼블릭 IP 주소를 수신하는지 확인하는 속성이 있습니다.

EC2 인스턴스에서 자동으로 할당된 퍼블릭 IP 주소를 수동으로 연결하거나 연결 해제할 수 없습니다. EC2 인스턴스가 퍼블릭 IP 주소를 수신하는지 여부를 제어하려면 다음 중 하나를 수행하십시오.

- 서브넷의 퍼블릭 IP 주소 지정 속성을 수정합니다. 자세한 내용은 Amazon VPC 사용 설명서의 서브넷의 퍼블릭 IPv4 주소 지정 속성 수정 단원을 참조하십시오.

- 시작 시 퍼블릭 IP 주소 지정 기능을 활성화 또는 비활성화합니다. 이는 서브넷의 퍼블릭 IP 주소 지정 속성을 재정의합니다. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 시작 시 퍼블릭 IPv4 주소 할당을 참조하십시오.

자세한 내용은 Amazon EC2 사용 설명서의 퍼블릭 IPv4 주소 및 외부 DNS 호스트 이름을 참조하세요.

EC2 인스턴스가 탄력적 IP 주소와 연결되어 있으면 인터넷에서 EC2 인스턴스에 연결할 수 있습니다. 언제든지 인스턴스 또는 네트워크 인터페이스에서 탄력적 IP 주소의 연결을 해제할 수 있습니다. 엘라스틱 IP 주소 연결을 끊으려면 Amazon EC2 사용 설명서의 엘라스틱 IP 주소 연결 해제를 참조하십시오.

[EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4)

범주: 보호 > 보안 네트워크 구성 > API 프라이빗 액세스

심각도: 중간

리소스 유형: `AWS::EC2::VPC`

AWS Config 규칙: `service-vpc-endpoint-enabled`

스케줄 유형: 주기적

파라미터:

- `serviceName`: `ec2`(사용자 지정할 수 없음)

이 제어는 각 VPC에 대해 Amazon EC2용 서비스 엔드포인트가 생성되었는지 여부를 확인합니다. Amazon EC2 서비스용으로 생성된 VPC 엔드포인트가 VPC에 없으면 제어가 실패합니다.

이 제어는 단일 계정의 리소스를 평가합니다. 계정 외부에 있는 리소스는 설명할 수 없습니다. Security Hub는 계정 간 검사를 수행하지 않으므로 계정 간에 공유되는 VPC에 대한 `FAILED` 결과를 확인할 수 있습니다. AWS Config Security Hub는 이러한 `FAILED` 조사 결과를 숨길 것을 권장합니다.

VPC의 보안 상태를 개선하기 위해 인터페이스 VPC 엔드포인트를 사용하도록 Amazon EC2를 구성할 수 있습니다. 인터페이스 엔드포인트는 Amazon EC2 API 작업에 비공개로 액세스할 수 있는 기술인 에 의해 AWS PrivateLink구동됩니다. 이는 VPC 및 Amazon ECR 간의 모든 네트워크 트래픽을 Amazon 네트워크로 제한합니다. 엔드포인트는 동일한 리전 내에서만 지원되므로 VPC와 다른 리전의 서비스 간에 엔드포인트를 생성할 수 없습니다. 이렇게 하면 다른 리전에 대한 의도하지 않은 Amazon EC2 API 호출을 방지할 수 있습니다.

Amazon EC2용 VPC 엔드포인트를 생성하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 및 인터페이스 VPC 엔드포인트를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Amazon VPC 콘솔에서 Amazon EC2에 대한 인터페이스 엔드포인트를 생성하려면 AWS PrivateLink 안내서의 VPC 엔드포인트 생성을 참조하십시오. 서비스 이름에 com.amazonaws.***region***.ec2를 선택합니다.

또한 엔드포인트 정책을 생성하고 VPC 엔드포인트에 연결하여 Amazon EC2 API에 대한 액세스를 제어할 수도 있습니다. VPC 엔드포인트 정책 생성에 대한 지침은 Amazon EC2 사용 설명서의 엔드포인트 정책 생성을 참조하십시오.

[EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CM-8(1)

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::EC2::EIP`

AWS Config 규칙: `eip-attached`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 VPC에 할당된 탄력적 IP(EIP) 주소가 EC2 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스(ENI)에 연결되어 있는지 확인합니다.

실패한 결과는 사용되지 않은 EC2 EIP가 있을 수 있음을 나타냅니다.

이는 카드 소지자 데이터 환경(CDE)에서 EIP의 정확한 자산 목록을 유지하는 데 도움이 됩니다.

미사용 EIP를 릴리스하려면 Amazon EC2 사용 설명서의 엘라스틱 IP 주소 해제를 참조하십시오.

[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/4.1, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/2.2.2, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CM-5, NIST.800-53.r5 CM-5, NIST.800-53.r5 CM-57, NIST.800-53.r5 CM-57, NIST.800-53.r5 CM-57, NIST.800-53.r5 CM-57, NIST.800-53.r5 CM-57, NIST.800-53.r5 CM-57, NIST.800-3.r5 SC-7, Nist.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (5)

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `restricted-ssh`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 보안 그룹이 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용하는지 확인합니다. 보안 그룹에서 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용하면 제어가 실패합니다.

보안 그룹을 통해 AWS 리소스에 대한 수신 및 발신 네트워크 트래픽을 상태 저장 필터링할 수 있습니다. 어떤 보안 그룹에서도 포트 22에 대한 무제한 수신 액세스를 허용하지 않는 것이 좋습니다. SSH와 같은 원격 콘솔 서비스에 대한 불가항력적인 연결성을 제거하면 서버가 위험에 노출될 가능성이 줄어듭니다.

이제 Security Hub가 와 통합되었습니다

포트 22에 대한 수신을 금지하려면 VPC와 연결된 각 보안 그룹에 대해 이러한 액세스를 허용하는 규칙을 제거하십시오. 지침은 Amazon EC2 사용 설명서의 보안 그룹 규칙 업데이트를 참조하십시오. Amazon EC2 콘솔에서 보안 그룹을 선택한 후 작업, 인바운드 규칙 편집을 선택합니다. 포트 22에 대한 액세스를 허용하는 규칙을 제거합니다.

[EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/4.2

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: (생성된 규칙은 다음과 같습니다.) `restricted-common-ports``restricted-rdp`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 보안 그룹이 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용하는지 확인합니다. 보안 그룹에서 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용하면 제어가 실패합니다.

보안 그룹을 통해 AWS 리소스에 대한 수신 및 발신 네트워크 트래픽을 상태 저장 필터링할 수 있습니다. 어떤 보안 그룹에서도 포트 3389에 대한 무제한 수신 액세스를 허용하지 않는 것이 좋습니다. RDP와 같은 원격 콘솔 서비스에 대한 불가항력적인 연결성을 제거하면 서버가 위험에 노출될 가능성이 줄어듭니다.

이제 Security Hub가 와 통합되었습니다

포트 3389에 대한 수신을 금지하려면 VPC와 연결된 각 보안 그룹에 대해 이러한 액세스를 허용하는 규칙을 제거하십시오. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 규칙 업데이트를 참조하십시오. Amazon VPC 콘솔에서 보안 그룹을 선택한 후 작업, 인바운드 규칙 편집을 선택합니다. 포트 3389에 대한 액세스를 허용하는 규칙을 제거합니다.

[EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 네트워크 보안

심각도: 중간

리소스 유형: `AWS::EC2::Subnet`

AWS Config 규칙: subnet-auto-assign-public-ip-disabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Virtual Private Cloud(VPC) 서브넷의 퍼블릭 IP 할당 시 MapPublicIpOnLaunch이 FALSE으로 설정되어 있는지 확인합니다. 플래그가 FALSE로 설정되면 제어가 전달됩니다.

모든 서브넷에는 해당 서브넷에 생성된 네트워크 인터페이스가 퍼블릭 IPv4 주소를 자동으로 수신하는지 여부를 결정하는 속성이 있습니다. 이 속성이 활성화된 서브넷에서 시작되는 인스턴스에는 기본 네트워크 인터페이스에 퍼블릭 IP 주소가 할당됩니다.

이제 Security Hub가 와 통합되었습니다

퍼블릭 IP 주소를 할당하지 않도록 서브넷을 구성하려면 Amazon VPC 사용 설명서의 서브넷에 대한 퍼블릭 IPv4 주소 지정 속성 수정을 참조하십시오. 퍼블릭 IPv4 주소 자동 할당 활성화 확인란의 선택을 취소합니다.

[EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.

관련 요구 사항: NIST.800-53.r5 CM-8(1)

범주: 보호 > 네트워크 보안

심각도: 낮음

리소스 유형: AWS::EC2::NetworkAcl

AWS Config 규칙: vpc-network-acl-unused-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 가상 사설 클라우드 (VPC) 에 사용되지 않은 네트워크 액세스 제어 목록 (네트워크 ACL) 이 있는지 확인합니다. 네트워크 ACL이 서브넷과 연결되어 있지 않으면 제어가 실패합니다. 컨트롤은 사용되지 않은 기본 네트워크 ACL에 대한 검색 결과를 생성하지 않습니다.

제어는 리소스 AWS::EC2::NetworkAcl의 항목 구성을 확인하고 네트워크 ACL의 관계를 결정합니다.

유일한 관계가 네트워크 ACL의 VPC인 경우 제어가 실패합니다.

다른 관계가 나열되면 제어가 통과합니다.

이제 Security Hub가 와 통합되었습니다

사용하지 않는 네트워크 ACL 삭제에 대한 지침은 Amazon VPC 사용 설명서의 네트워크 ACL 삭제를 참조하십시오. 기본 네트워크 ACL 또는 서브넷에 연결된 ACL은 삭제할 수 없습니다.

[EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21)

카테고리: 보호 > 네트워크 보안

심각도: 낮음

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `ec2-instance-multiple-eni-check`

스케줄 유형: 변경이 트리거됨

파라미터:

- `Adapterids` – EC2 인스턴스에 연결된 네트워크 인터페이스 ID 목록(사용자 지정할 수 없음)

이 제어는 EC2 인스턴스가 여러 탄력적 네트워크 인터페이스(ENI) 또는 Elastic Fabric Adapter(EFA)를 사용하는지 여부를 확인합니다. 이 제어는 단일 네트워크 어댑터를 사용하는 경우 통과됩니다. 제어에는 허용되는 ENI를 식별하기 위한 선택적 파라미터 목록이 포함되어 있습니다. Amazon EKS 클러스터에 속하는 EC2 인스턴스가 둘 이상의 ENI를 사용하는 경우에도 이 제어는 실패합니다. EC2 인스턴스에 Amazon EKS 클러스터의 일부로서 여러 ENI가 있어야 하는 경우 이러한 제어 조사 결과를 숨길 수 있습니다.

ENI가 여러 개이면 듀얼 홈 인스턴스, 즉 서브넷이 여러 개 있는 인스턴스가 발생할 수 있습니다. 이로 인해 네트워크 보안이 복잡해지고 의도하지 않은 네트워크 경로와 액세스가 발생할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

EC2 인스턴스에서 네트워크 인터페이스를 분리하려면 Amazon EC2 사용 설명서의 인스턴스에서 네트워크 인터페이스 분리를 참조하십시오.

[EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(5)

범주: 보호 > 보안 네트워크 구성 > 보안 그룹 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `vpc-sg-open-only-to-authorized-ports`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`authorizedTcpPorts`	승인된 TCP 포트 목록	IntegerList (최대 32개 항목)	`1~65535`	`[80,443]`
`authorizedUdpPorts`	승인된 UDP 포트 목록	IntegerList (최대 32개 항목)	`1~65535`	기본값 없음

이 제어는 Amazon EC2 보안 그룹이 승인되지 않은 포트로부터의 무제한 수신 트래픽을 허용하는지 확인합니다. 제어 상태는 다음과 같이 결정합니다.

- `authorizedTcpPorts`의 기본값을 사용하는 경우 보안 그룹이 포트 80 및 443 외 모든 포트로부터의 무제한 수신 트래픽을 허용하면 제어가 실패합니다.
- `authorizedTcpPorts` 또는 `authorizedUdpPorts`에 사용자 지정 값을 제공하는 경우 보안 그룹이 목록에 없는 포트로부터의 무제한 수신 트래픽을 허용하면 제어가 실패합니다.
- 파라미터를 사용하지 않으면 무제한 인바운드 규칙이 있는 보안 그룹에 대한 제어가 실패합니다.

보안 그룹은 AWS에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공합니다. 보안 그룹 규칙은 최소 권한 액세스 원칙을 따라야 합니다. 무제한 액세스 (접미사가 /0인 IP 주소) 는 해킹, denial-of-service 공격, 데이터 손실과 같은 악의적인 활동의 기회를 증가시킵니다. 포트가 특별히 허용되지 않는 한, 포트는 무제한 액세스를 거부해야 합니다.

이제 Security Hub가 와 통합되었습니다

보안 그룹을 수정하려면 Amazon VPC 사용 설명서에서 보안 그룹 작업을 참조하세요.

[EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(5)

범주: 보호 > 제한된 네트워크 액세스

심각도: 심각

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: (생성된 규칙은 다음과 같습니다. **`restricted-common-ports`**) `vpc-sg-restricted-common-ports`

스케줄 유형: 변경이 트리거됨

파라미터: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` 용자 지정할 수 없음)

이 제어는 Amazon EC2 보안 그룹에 대한 무제한 수신 트래픽이 가장 위험이 높은 지정된 포트에 액세스할 수 있는지 여부를 확인합니다. 보안 그룹의 규칙 중 하나라도 '0.0.0.0/0' 또는 '::/0'에서 해당 포트로의 수신 트래픽을 허용하는 경우 이 제어는 실패합니다.

보안 그룹을 통해 AWS 리소스에 대한 수신 및 발신 네트워크 트래픽을 상태 저장 필터링할 수 있습니다. 무제한 액세스 (0.0.0.0/0) 는 해킹, denial-of-service 공격, 데이터 손실과 같은 악의적인 활동의 기회를 증가시킵니다. 어떤 보안 그룹도 다음 포트에 대한 무제한 수신 액세스를 허용해서는 안 됩니다.

- 20, 21 (FTP)
- 22 (SSH)

- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000 (Go, Node.js, Ruby 웹 개발 프레임워크)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Python 웹 개발 프레임워크)
- 5432 (postgresql)
- 5500 fcp-addr-srvr (1)
- 5601 (대시보드) OpenSearch
- 8080 (프록시)
- 8088 (레거시 HTTP 포트)
- 8888 (대체 HTTP 포트)
- 9200 또는 9300 () OpenSearch

이제 Security Hub가 와 통합되었습니다

보안 그룹에서 규칙을 삭제하려면 Amazon EC2 사용 설명서의 보안 그룹에서 규칙 삭제를 참조하십시오.

[EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형:`AWS::EC2::VPNConnection`

AWS Config 규칙: `vpc-vpn-2-tunnels-up`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

VPN 터널은 데이터가 고객 네트워크에서 AWS Site-to-Site VPN 연결 간에 또는 사이트 간 VPN 연결 AWS 내에서 전달될 수 있는 암호화된 링크입니다. 각 VPN 연결에는 고가용성을 위해 동시에 사용할 수 있는 두 개의 VPN 터널이 포함되어 있습니다. AWS VPC와 원격 네트워크 간의 안전하고 가용성이 높은 연결을 확인하려면 두 VPN 터널이 모두 VPN 연결에 적합한지 확인하는 것이 중요합니다.

이 컨트롤은 AWS Site-to-Site VPN에서 제공하는 두 VPN 터널이 모두 UP 상태인지 확인합니다. 터널 중 하나 또는 두 개가 DOWN 상태인 경우 제어가 실패합니다.

이제 Security Hub가 와 통합되었습니다

VPN 터널 옵션을 수정하려면 사이트 간 VPN 사용 설명서의 사이트 간 VPN 터널 옵션 수정을 참조하십시오. AWS

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.4.0/5.1, CIS AWS 재단 벤치마크 v3.0.0/5.1, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-2 (2) -7, Nist.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (5)

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형:`AWS::EC2::NetworkAcl`

AWS Config 규칙: `nacl-no-unrestricted-ssh-rdp`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 네트워크 ACL (액세스 제어 목록) 이 SSH/RDP 인그레스 트래픽의 기본 TCP 포트에 대한 무제한 액세스를 허용하는지 여부를 확인합니다. 네트워크 ACL 인바운드 엔트리에서 TCP 포트 22 또는 3389에 대해 '0.0.0.0/0' 또는 ': :/0'의 소스 CIDR 블록을 허용하는 경우 제어가 실패합니다. 컨트롤은 기본 네트워크 ACL에 대한 결과를 생성하지 않습니다.

포트 22(SSH) 및 포트 3389(RDP)와 같은 원격 서버 관리 포트에 대한 액세스는 공개적으로 액세스할 수 없어야 합니다. 이렇게 하면 VPC 내의 리소스에 의도하지 않은 액세스가 허용될 수 있습니다.

이제 Security Hub가 와 통합되었습니다

네트워크 ACL 트래픽 규칙을 편집하려면 Amazon VPC 사용 설명서의 네트워크 ACL 사용을 참조하십시오.

[EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.

> **Important**
>
> 특정 표준에서 사용 중지 — Security Hub는 2023년 9월 20일에 AWS 기본 보안 모범 사례 표준 및 NIST SP 800-53 개정 5에서 이 제어 기능을 제거했습니다. 이 제어는 여전히 서비스 관리형 표준:의 일부입니다. AWS Control Tower이 제어는 보안 그룹이 EC2 인스턴스 또는 탄력적 네트워크 인터페이스에 연결된 경우 통과된 결과를 생성합니다. 하지만, 특정 사용 사례에 대해서는 연결되지 않은 보안 그룹이 보안 위험을 초래하지는 않습니다. EC2.2, EC2.13, EC2.14, EC2.18, EC2.19 등의 다른 EC2 제어를 사용하여 보안 그룹을 모니터링할 수 있습니다.

범주: 식별 > 인벤토리

심각도: 중간

리소스 유형:`AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`

AWS Config 규칙: `ec2-security-group-attached-to-eni-periodic`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 보안 그룹이 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스에 연결되어 있는지 또는 탄력적 네트워크 인터페이스에 연결되어 있는지 확인합니다. 보안 그룹이 Amazon EC2 인스턴스 또는 Elastic Network 인터페이스와 연결되어 있지 않으면 제어가 실패합니다.

이제 Security Hub가 와 통합되었습니다

보안 그룹을 생성, 할당 및 삭제하려면 Amazon EC2 사용 설명서의 보안 그룹을 참조하십시오.

[EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21), NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형:`AWS::EC2::TransitGateway`

AWS Config 규칙: `ec2-transit-gateway-auto-vpc-attach-disabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 EC2 전송 게이트웨이가 공유 VPC 연결을 자동으로 수락하는지 확인합니다. 공유된 VPC 연결 요청을 자동으로 수락하는 전송 게이트웨이에서는 이 제어가 실패합니다.

`AutoAcceptSharedAttachments`을 켜면 요청 또는 연결이 시작된 계정을 확인하지 않고 모든 교차 계정 VPC 연결 요청을 자동으로 수락하도록 전송 게이트웨이가 구성됩니다. 권한 부여 및 인증의 모범 사례를 따르려면 승인된 VPC 연결 요청만 허용되도록 이 기능을 끄는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

전송 게이트웨이를 수정하려면 Amazon VPC 개발자 안내서의 전송 게이트웨이 수정을 참조하십시오.

[EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.

관련 요구 사항: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형:`AWS::EC2::Instance`

AWS Config 규칙: `ec2-paravirtual-instance-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 EC2 인스턴스의 가상화 유형이 반가상화인지 여부를 확인합니다. EC2 인스턴스의 `virtualizationType`가 `paravirtual`로 설정된 경우 제어가 실패합니다.

Linux Amazon Machine Image(AMI)는 PV(반가상화) 또는 HVM(하드웨어 가상 머신)의 두 가지 유형의 가상화를 사용합니다. PV AMI와 HVM AMI의 주요 차이점은 부팅 방법과 더 나은 성능을 위해 특수 하드웨어 확장(CPU, 네트워크, 스토리지)을 활용할 수 있는지 여부에 있습니다.

이전에는 대부분의 경우 PV 게스트가 HVM 게스트보다 더 나은 성능을 제공했지만, HVM 가상화 기능이 향상되고 HVM AMI용 PV 드라이버가 제공되는 현재는 더 이상 그렇지 않습니다. 자세한 내용은 Amazon EC2 사용 설명서의 Linux AMI 가상화 유형을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

EC2 인스턴스를 새 인스턴스 유형으로 업데이트하려면 Amazon EC2 사용 설명서의 인스턴스 유형 변경을 참조하십시오.

[EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형:`AWS::EC2::LaunchTemplate`

AWS Config 규칙: `ec2-launch-template-public-ip-disabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 시작 템플릿이 시작 시 네트워크 인터페이스에 퍼블릭 IP 주소를 할당하도록 구성되어 있는지 확인합니다. 네트워크 인터페이스에 퍼블릭 IP 주소를 할당하도록 EC2 시작 템플릿이 구성되어 있거나 퍼블릭 IP 주소가 있는 네트워크 인터페이스가 하나 이상 있는 경우 제어가 실패합니다.

퍼블릭 IP 주소는 인터넷을 통해 연결할 수 있는 주소입니다. 퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스와 연결된 리소스에 연결할 수 있습니다. EC2 리소스는 워크로드에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개적으로 액세스하면 안 됩니다.

이제 Security Hub가 와 통합되었습니다

EC2 시작 템플릿을 업데이트하려면 Amazon EC2 Auto Scaling 사용 설명서의 기본 네트워크 인터페이스 설정 변경을 참조하십시오.

[EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.

범주: 복구 > 복원력 > 백업 활성화

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)

심각도: 낮음

리소스 유형: `AWS::EC2::Volume`

AWS Config 규칙: **`ebs-resources-protected-by-backup-plan`**

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`backupVaultLockCheck`	컨트롤은 매개변수가 로 PASSED 설정되어 `true` 있고 리소스가 AWS Backup Vault Lock을 사용하는지 여부를 확인합니다.	불	`true` 또는 `false`	기본값 없음

이 제어는 `in-use` 상태의 Amazon EBS 볼륨이 백업 계획에 포함되는지 여부를 평가합니다. EBS 볼륨에 백업 계획이 적용되지 않는 경우 제어가 실패합니다. `backupVaultLockCheck`매개 변수를 다음과 같이 설정하면 EBS 볼륨이 AWS Backup 잠긴 저장소에 백업된 경우에만 컨트롤이 통과합니다. `true`

백업을 통해 보안 사고로부터 더 빨리 복구할 수 있습니다. 또한 시스템의 복원력을 강화합니다. 백업 계획에 Amazon EBS 볼륨을 포함하면 의도하지 않은 손실 또는 삭제로부터 데이터를 보호할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Amazon EBS 볼륨을 AWS Backup 백업 계획에 추가하려면 AWS Backup 개발자 안내서의 백업 계획에 리소스 할당을 참조하십시오.

[EC2.33] EC2 트랜짓 게이트웨이 첨부 파일에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::TransitGatewayAttachment`

AWS Config 규칙: `tagged-ec2-transitgatewayattachment` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 트랜짓 게이트웨이 첨부 파일에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 트랜짓 게이트웨이 첨부 파일에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 트랜짓 게이트웨이 첨부 파일에 어떤 키로도 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성,

검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 트랜짓 게이트웨이 첨부 파일에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::TransitGatewayRouteTable`

AWS Config 규칙: `tagged-ec2-transitgatewayroutetable` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 트랜짓 게이트웨이 라우팅 테이블에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 트랜짓 게이트웨이 라우팅 테이블에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 트랜짓 게이트웨이 라우팅 테이블에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 전송 게이트웨이 라우팅 테이블에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.35] EC2 네트워크 인터페이스에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::NetworkInterface`

AWS Config 규칙: `tagged-ec2-networkinterface` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 네트워크 인터페이스에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 네트워크 인터페이스에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 네트워크 인터페이스에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 네트워크 인터페이스에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.36] EC2 고객 게이트웨이에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::CustomerGateway`

AWS Config 규칙: `tagged-ec2-customergateway` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 고객 게이트웨이에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 고객 게이트웨이에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 고객 게이트웨이에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 고객 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.37] EC2 엘라스틱 IP 주소에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::EIP`

AWS Config 규칙: `tagged-ec2-eip` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 엘라스틱 IP 주소에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 엘라스틱 IP 주소에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 엘라스틱 IP 주소에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 엘라스틱 IP 주소에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.38] EC2 인스턴스에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `tagged-ec2-instance` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 인스턴스에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 인스턴스에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든

키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 인스턴스에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 인스턴스에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.39] EC2 인터넷 게이트웨이에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::InternetGateway`

AWS Config 규칙: `tagged-ec2-internetgateway` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 인터넷 게이트웨이에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 인터넷 게이트웨이에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 인터넷 게이트웨이에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 인터넷 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::NatGateway`

AWS Config 규칙: `tagged-ec2-natgateway` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 네트워크 주소 변환 (NAT) 게이트웨이에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` NAT 게이트웨이에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 NAT 게이트웨이에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 NAT 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.41] EC2 네트워크 ACL에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::NetworkAcl`

AWS Config 규칙: `tagged-ec2-networkacl` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 제어는 Amazon EC2 네트워크 액세스 제어 목록 (네트워크 ACL) 에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 네트워크 ACL에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 네트워크 ACL에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 네트워크 ACL에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.42] EC2 라우팅 테이블에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::RouteTable`

AWS Config 규칙: `tagged-ec2-routetable` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 라우팅 테이블에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 라우팅 테이블에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정

된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 라우팅 테이블에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 라우팅 테이블에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.43] EC2 보안 그룹에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `tagged-ec2-securitygroup` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 보안 그룹에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 보안 그룹에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 보안 그룹에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 보안 그룹에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.44] EC2 서브넷에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::Subnet`

AWS Config 규칙: `tagged-ec2-subnet` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 서브넷에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 서브넷에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 서브넷에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 서브넷에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.45] EC2 볼륨에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::Volume`

AWS Config 규칙: `tagged-ec2-subnet` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 볼륨에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 볼륨에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 볼륨에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 볼륨에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.46] 아마존 VPC는 태그가 지정되어야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::VPC`

AWS Config 규칙: `tagged-ec2-vpc` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon VPC (가상 사설 클라우드) 에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` Amazon VPC에 태그 키가 없거나 파라미터에 지정된 모든 키가

없는 경우 제어가 실패합니다. `requiredTagKeys` 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 Amazon VPC에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

VPC에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.47] Amazon VPC 엔드포인트 서비스는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::VPCEndpointService`

AWS Config 규칙: `tagged-ec2-vpcendpointservice` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon VPC 엔드포인트 서비스에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 엔드포인트 서비스에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 엔드포인트 서비스에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Amazon VPC 엔드포인트 서비스에 태그를 추가하려면 안내서의 엔드포인트 서비스 구성 섹션에서 태그 관리를 참조하십시오.AWS PrivateLink

[EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::FlowLog`

AWS Config 규칙: `tagged-ec2-flowlog` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon VPC 흐름 로그에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 흐름 로그에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 제공하지 `requiredTagKeys` 않는 경우 컨트롤은 태그 키의 존재 여부만 확인하고 흐름 로그에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Amazon VPC 흐름 로그에 태그를 추가하려면 Amazon VPC 사용 설명서의 흐름 로그에 태그 지정을 참조하십시오.

[EC2.49] Amazon VPC 피어링 연결에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::VPCPeeringConnection`

AWS Config 규칙: `tagged-ec2-vpcpeeringconnection` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon VPC 피어링 연결에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 피어링 연결에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 피어링 연결에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Amazon VPC 피어링 연결에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.50] EC2 VPN 게이트웨이에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::VPNGateway`

AWS Config 규칙: `tagged-ec2-vpngateway` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 VPN 게이트웨이에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` VPN 게이트웨이에 태그 키가 없거나 `requiredTagKeys` 파라미터에

지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 VPN 게이트웨이에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 VPN 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(12), NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 낮음

리소스 유형: `AWS::EC2::ClientVpnEndpoint`

AWS Config 규칙: **ec2-client-vpn-connection-log-enabled**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS Client VPN 엔드포인트에 클라이언트 연결 로깅이 활성화되어 있는지 확인합니다. 엔드포인트에 클라이언트 연결 로깅이 활성화되어 있지 않으면 제어가 실패합니다.

클라이언트 VPN 엔드포인트를 사용하면 원격 클라이언트가 AWS의 Virtual Private Cloud(VPC) 리소스에 안전하게 연결할 수 있습니다. 연결 로그를 사용하면 VPN 엔드포인트에서 사용자 활동을 추적하고 가시성을 제공할 수 있습니다. 연결 로깅을 활성화하면 로그 그룹에서 로그 스트림의 이름을 지정할 수 있습니다. 로그 스트림을 지정하지 않으면 Client VPN 서비스에서 자동으로 로그 스트림을 생성합니다.

이제 Security Hub가 와 통합되었습니다

연결 로깅을 활성화하려면 AWS Client VPN 관리자 안내서의 기존 Client VPN 엔드포인트에 연결 로깅 활성화를 참조하세요.

[EC2.52] EC2 트랜짓 게이트웨이에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::TransitGateway`

AWS Config 규칙: `tagged-ec2-transitgateway` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon EC2 트랜짓 게이트웨이에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 트랜짓 게이트웨이에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 트랜짓 게이트웨이에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EC2 전송 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태그 지정을 참조하십시오.

[EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.

관련 요구 사항: AWS CIS 재단 벤치마크 v3.0.0/5.2

범주: 보호 > 보안 네트워크 구성 > 보안 그룹 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `vpc-sg-port-restriction-check`

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`ipType`	IP 버전	String	사용자 지정할 수 없음	`IPv4`
`restrictPorts`	인그레스 트래픽을 거부해야 하는 포트 목록	IntegerList	사용자 지정할 수 없음	`22,3389`

이 컨트롤은 Amazon EC2 보안 그룹이 0.0.0.0/0에서 원격 서버 관리 포트 (포트 22 및 3389) 로의 수신을 허용하는지 여부를 확인합니다. 보안 그룹이 0.0.0.0/0에서 포트 22 또는 3389로의 수신을 허용하면 제어가 실패합니다.

보안 그룹은 리소스에 대한 인그레스 및 아웃바운드 네트워크 트래픽의 스테이트풀 필터링을 제공합니다. AWS TDP (6), UDP (17) 또는 ALL (-1) 프로토콜을 사용하여 포트 22로의 SSH 및 포트 3389에 대한 RDP와 같은 원격 서버 관리 포트에 대한 무제한 인그레스 액세스를 허용하는 보안 그룹은 없는 것이 좋습니다. 이러한 포트에 대한 공개 액세스를 허용하면 리소스 공격 대상이 증가하고 리소스 손상 위험이 높아집니다.

이제 Security Hub가 와 통합되었습니다

지정된 포트로의 수신 트래픽을 금지하도록 EC2 보안 그룹 규칙을 업데이트하려면 Amazon EC2 사용 설명서의 보안 그룹 규칙 업데이트를 참조하십시오. Amazon EC2 콘솔에서 보안 그룹을 선택한 후 작업, 인바운드 규칙 편집을 선택합니다. 포트 22 또는 포트 3389에 대한 액세스를 허용하는 규칙을 제거합니다.

[EC2.54] EC2 보안 그룹은: :/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.

관련 요구 사항: CIS 재단 벤치마크 v3.0.0/5.3 AWS

범주: 보호 > 보안 네트워크 구성 > 보안 그룹 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: vpc-sg-port-restriction-check

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
ipType	IP 버전	String	사용자 지정할 수 없음	IPv6
restrictPorts	인그레스 트래픽을 거부해야 하는 포트 목록	IntegerList	사용자 지정할 수 없음	22,3389

이 제어는 Amazon EC2 보안 그룹이: :/0에서 원격 서버 관리 포트 (포트 22 및 3389) 로의 수신을 허용하는지 여부를 확인합니다. 보안 그룹이: :/0에서 포트 22 또는 3389로의 수신을 허용하면 제어가 실패합니다.

보안 그룹은 리소스에 대한 인그레스 및 아웃바운드 네트워크 트래픽의 스테이트풀 필터링을 제공합니다. AWS TDP (6), UDP (17) 또는 ALL (-1) 프로토콜을 사용하여 포트 22로의 SSH 및 포트 3389에 대한 RDP와 같은 원격 서버 관리 포트에 대한 무제한 인그레스 액세스를 허용하는 보안 그룹은 없는 것이 좋습니다. 이러한 포트에 대한 공개 액세스를 허용하면 리소스 공격 대상이 증가하고 리소스 손상 위험이 높아집니다.

이제 Security Hub가 와 통합되었습니다

지정된 포트로의 수신 트래픽을 금지하도록 EC2 보안 그룹 규칙을 업데이트하려면 Amazon EC2 사용 설명서의 보안 그룹 규칙 업데이트를 참조하십시오. Amazon EC2 콘솔에서 보안 그룹을 선택한 후 작업, 인바운드 규칙 편집을 선택합니다. 포트 22 또는 포트 3389에 대한 액세스를 허용하는 규칙을 제거합니다.

Amazon EC2 Auto Scaling 제어

이러한 제어는 Amazon EC2 Auto Scaling 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/2.2, NIST.800-53.r5 CA-7, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 SI-2

범주: 식별 > 인벤토리

심각도: 낮음

리소스 유형: `AWS::AutoScaling::AutoScalingGroup`

AWS Config 규칙: `autoscaling-group-elb-healthcheck-required`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 로드 밸런서와 연결된 Amazon EC2 Auto Scaling 그룹이 Elastic Load Balancing (ELB) 상태 확인을 사용하는지 여부를 확인합니다. Auto Scaling 그룹이 ELB 상태 확인을 사용하지 않으면 제어가 실패합니다.

ELB 상태 확인을 통해 Auto Scaling 그룹이 로드 밸런서에서 제공하는 추가 테스트를 기반으로 인스턴스의 상태를 확인할 수 있습니다. Elastic Load Balancing 상태 확인을 사용하면 EC2 Auto Scaling 그룹을 사용하는 애플리케이션의 가용성을 지원하는 데도 도움이 됩니다.

이제 Security Hub가 와 통합되었습니다

Elastic Load Balancing 상태 확인을 추가하려면 Amazon EC2 Auto Scaling 사용 설명서 의 Elastic Load Balancing 상태 확인 추가를 참조하십시오.

[AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포함해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::AutoScaling::AutoScalingGroup`

AWS Config 규칙: autoscaling-multiple-az

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
minAvailabilityZones	최소 가용 영역의 수	Enum	2, 3, 4, 5, 6	2	

이 제어는 Amazon EC2 Auto Scaling 그룹이 지정된 수 이상의 가용 영역(AZ)에 걸쳐 있는지 확인합니다. Auto Scaling 그룹이 최소한 지정된 수의 AZ에 걸쳐 있지 않으면 제어가 실패합니다. 최소 AZ 수에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 두 AZ를 사용합니다.

여러 AZ에 걸쳐 있지 않은 Auto Scaling 그룹은 구성된 단일 AZ를 사용할 수 없게 될 경우 이를 보완하기 위해 다른 AZ에서 인스턴스를 시작할 수 없습니다. 그러나 일괄 작업이나 AZ 간 전송 비용을 최소로 유지해야 하는 경우와 같은 일부 사용 사례에서는 단일 가용 영역이 있는 Auto Scaling 그룹이 선호될 수 있습니다. 이 경우 이 제어를 비활성화하거나 결과를 숨길 수 있습니다.

이제 Security Hub가 와 통합되었습니다

기존 Auto Scaling 그룹에 AZ를 추가하려면 Amazon EC2 Auto Scaling 사용 설명서의 가용 영역 추가 및 제거를 참조하세요.

[AutoScaling.3] Auto Scaling 그룹 시작 구성에서는 인스턴스 메타데이터 서비스 버전 2 (IMDSv2) 를 요구하도록 EC2 인스턴스를 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: AWS::AutoScaling::LaunchConfiguration

AWS Config 규칙: `autoscaling-launchconfig-requires-imdsv2`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 Auto Scaling 그룹에서 시작한 모든 인스턴스에서 IMDSv2가 활성화되어 있는지 확인합니다. 시작 구성에 인스턴스 메타데이터 서비스(IMDS) 버전이 포함되지 않거나 IMDSv1 및 IMDSv2가 모두 활성화된 경우 제어가 실패합니다.

IMDS는 실행 중인 인스턴스를 구성하거나 관리하는 데 사용할 수 있는 인스턴스에 대한 데이터를 제공합니다.

IMDS 버전 2에는 IMDSv1에서 사용할 수 없었던 새로운 보호 기능이 추가되어 EC2 인스턴스를 더욱 안전하게 보호할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Auto Scaling 그룹 은 한 번에 한 개의 시작 구성과 연결됩니다. 시작 구성을 생성한 후에는 수정할 수 없습니다. Auto Scaling 그룹 의 시작 구성을 변경하려면 기존 시작 구성을 IMDSv2가 활성화된 새 시작 구성의 기초로 사용합니다. 자세한 내용은 Amazon EC2 사용 설명서의 새 인스턴스에 대한 인스턴스 메타데이터 옵션 구성을 참조하십시오.

[AutoScaling.4] Auto Scaling 그룹 시작 구성의 메타데이터 응답 홉 제한은 1보다 커서는 안 됩니다.

> **Important**
>
> Security Hub는 2024년 4월에 이 제어를 폐기했습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::AutoScaling::LaunchConfiguration`

AWS Config 규칙: `autoscaling-launch-config-hop-limit`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 메타데이터 토큰이 이동할 수 있는 네트워크 홉 수를 확인합니다. 메타데이터 응답 홉 제한이 1보다 크면 제어가 실패합니다.

인스턴스 메타데이터 서비스(IMDS)는 Amazon EC2 인스턴스에 대한 메타데이터 정보를 제공하며 애플리케이션 구성에 유용합니다. 메타데이터 서비스에 대한 HTTP PUT 응답을 EC2 인스턴스로만 제한하면 IMDS를 무단으로 사용하지 못하도록 보호할 수 있습니다.

IP 패킷의 TTL(Time To Live) 필드는 모든 홉에서 1씩 감소됩니다. 이렇게 감소되면 패킷이 EC2 외부로 이동하지 않도록 할 수 있습니다. IMDSv2는 개방형 라우터, 계층 3 방화벽, VPN, 터널 또는 NAT 디바이스로 잘못 구성되었을 수 있는 EC2 인스턴스를 보호하여 권한이 없는 사용자가 메타데이터를 검색하지 못하도록 합니다. IMDSv2를 사용하면 기본 메타데이터 응답 홉 제한이 1로 설정되어 있기 때문에 비밀 토큰이 포함된 PUT 응답이 인스턴스 외부로 이동할 수 없습니다. 하지만 이 값이 1보다 크면 토큰이 EC2 인스턴스를 벗어날 수 있습니다.

이제 Security Hub가 와 통합되었습니다

기존 시작 구성의 메타데이터 응답 홉 제한을 수정하려면 Amazon EC2 사용 설명서의 기존 인스턴스에 대한 인스턴스 메타데이터 옵션 수정을 참조하십시오.

[Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::AutoScaling::LaunchConfiguration`

AWS Config 규칙: `autoscaling-launch-config-public-ip-disabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Auto Scaling 그룹 의 관련 시작 구성이 그룹 인스턴스에 퍼블릭 IP 주소를 할당하는지 여부를 확인합니다. 연결된 시작 구성이 퍼블릭 IP 주소를 할당하면 제어가 실패합니다.

Auto Scaling 그룹 시작 구성의 Amazon EC2 인스턴스에는 제한된 엣지 케이스를 제외하고 연결된 퍼블릭 IP 주소가 없어야 합니다. Amazon EC2 인스턴스는 인터넷에 직접 노출되지 않고 로드 밸런서 뒤에서만 액세스할 수 있어야 합니다.

이제 Security Hub가 와 통합되었습니다

Auto Scaling 그룹 은 한 번에 한 개의 시작 구성과 연결됩니다. 시작 구성을 생성한 후에는 수정할 수 없습니다. 기존 Auto Scaling 그룹 의 시작 구성을 변경하기 위해 기존 시작 구성을 새 시작 구성의 기초로 사용할 수 있습니다. 그런 다음 새로운 시작 구성을 사용하도록 Auto Scaling 그룹을 업데이트합니다. step-by-step 지침은 Amazon EC2 Auto Scaling 사용 설명서에서 Auto Scaling 그룹의 시작 구성 변경을 참조하십시오. 새 시작 구성을 생성할 때, 추가 구성에서 고급 세부 정보, IP 주소 유형에서 어떤 인스턴스에도 퍼블릭 IP 주소를 할당하지 않음을 선택합니다.

시작 구성을 변경한 후 Auto Scaling은 새 구성 옵션을 사용하여 새 인스턴스를 시작합니다. 기존 인스턴스는 영향을 받지 않습니다. 기존 인스턴스를 업데이트하려면 인스턴스를 새로 고치거나 자동 조정을 허용하여 종료 정책에 따라 이전 인스턴스를 새 인스턴스로 점진적으로 교체하는 것이 좋습니다. Auto Scaling 인스턴스 업데이트에 대한 자세한 내용은 Amazon EC2 Auto Scaling 사용 설명서의 Auto Scaling 인스턴스 업데이트를 참조하십시오.

[AutoScaling.6] Auto Scaling 그룹은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::AutoScaling::AutoScalingGroup`

AWS Config 규칙: `autoscaling-multiple-instance-types`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 Auto Scaling 그룹이 여러 인스턴스 유형을 사용하는지 여부를 확인합니다. Auto Scaling 그룹 에 정의된 인스턴스 유형이 하나만 있는 경우 제어가 실패합니다.

여러 가용 영역에서 실행되는 여러 인스턴스 유형에 애플리케이션을 배포하여 가용성을 높일 수 있습니다. Security Hub는 선택한 가용 영역에 인스턴스 용량이 부족한 경우 Auto Scaling 그룹 에서 다른 인스턴스 유형을 시작할 수 있도록 여러 인스턴스 유형을 사용할 것을 권장합니다.

이제 Security Hub가 와 통합되었습니다

여러 인스턴스 유형이 포함된 Auto Scaling 그룹 을 생성하려면 Amazon EC2 Auto Scaling 사용 설명서의 여러 인스턴스 유형 및 구매 옵션이 포함된 오토 스케일링을 참조하십시오.

[AutoScaling.9] Amazon EC2 Auto Scaling 그룹은 Amazon EC2 시작 템플릿을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::AutoScaling::AutoScalingGroup`

AWS Config 규칙: `autoscaling-launch-template`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 Auto Scaling 그룹 이 EC2 시작 템플릿에서 생성되었는지 여부를 확인합니다. Amazon EC2 Auto Scaling 그룹 이 시작 템플릿으로 생성되지 않았거나 혼합 인스턴스 정책에 시작 템플릿이 지정되지 않은 경우 이 제어가 실패합니다.

EC2 Auto Scaling 그룹 은 EC2 시작 템플릿이나 시작 구성에서 생성할 수 있습니다. 하지만 시작 템플릿을 사용하여 Auto Scaling 그룹 을 생성하면 최신 기능과 개선 사항을 이용할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

EC2 시작 템플릿을 사용하여 Auto Scaling 그룹 을 생성하려면 Amazon EC2 Auto Scaling 사용 설명서의 시작 템플릿을 사용하여 오토 스케일링 생성을 참조하십시오. 시작 구성을 시작 템플릿으로 교체하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 시작 구성을 시작 템플릿으로 바꾸기를 참조하십시오.

[AutoScaling.10] EC2 Auto Scaling 그룹에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AutoScaling::AutoScalingGroup`

AWS Config 규칙: `tagged-autoscaling-autoscalinggroup` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EC2 Auto Scaling 그룹에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` Auto Scaling 그룹에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 Auto Scaling 그룹에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Auto Scaling 그룹에 태그를 추가하려면 Amazon EC2 Auto Scaling 사용 설명서의 Auto Scaling 그룹 및 인스턴스에 태그 지정 섹션을 참조하십시오.

Amazon EC2 Systems Manager 제어

이러한 제어는 에서 관리하는 Amazon EC2 인스턴스와 관련이 있습니다. AWS Systems Manager

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager

관련 요구 사항: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8(1), NIST.800-53.r5 CM-8(2), NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SA-15(2), NIST.800-53.r5 SA-15(8), NIST.800-53.r5 SA-3, NIST.800-53.r5 SI-2(3)

범주: 식별 > 인벤토리

심각도: 중간

평가된 리소스: `AWS::EC2::Instance`

필수 AWS Config 기록 리소스:, `AWS::EC2::Instance` `AWS::SSM::ManagedInstanceInventory`

AWS Config 규칙: `ec2-instance-managed-by-systems-manager`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 계정에서 중지되고 실행 중인 EC2 인스턴스가 에서 관리되는지 여부를 확인합니다. AWS Systems Manager Systems Manager는 AWS 서비스 AWS 인프라를 보고 제어하는 데 사용할 수 있는 도구입니다.

Systems Manager는 보안과 규정 준수를 유지하는 데 도움이 되도록 중지 및 실행 중인 관리형 인스턴스를 검사합니다. 관리형 인스턴스는 Systems Manager에 사용하도록 구성된 시스템입니다. 그

런 다음 Systems Manager는 탐지된 모든 정책 위반에 대해 보고하거나 수정 조치를 취합니다. 또한 Systems Manager는 관리형 인스턴스를 구성하고 유지 관리하는 데 도움이 됩니다.

자세한 내용은 AWS Systems Manager 사용 설명서를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Systems Manager로 EC2 인스턴스를 관리하려면 AWS Systems Manager 사용 설명서의 Amazon EC2 호스트 관리를 참조하십시오. 구성 옵션 섹션에서 기본 선택 사항을 유지하거나 원하는 구성에 맞게 필요에 따라 변경할 수 있습니다.

[SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.

관련 요구 사항: PCI DSS v3.2.1/6.2, NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(3), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::SSM::PatchCompliance`

AWS Config 규칙: `ec2-managedinstance-patch-compliance-status-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 인스턴스에 패치를 설치한 후 Systems Manager 패치 준수 상태가 `COMPLIANT` 또는 `NON_COMPLIANT`인지 확인합니다. 규정 준수 상태가 `NON_COMPLIANT`인 경우 제어가 실패합니다. 제어는 Systems Manager 패치 관리자가 관리하는 인스턴스만 확인합니다.

조직의 필요에 따라 EC2 인스턴스를 완전히 패치하면 AWS 계정의 공격 표면이 줄어듭니다.

이제 Security Hub가 와 통합되었습니다

Systems Manager는 패치 정책을 사용하여 관리형 인스턴스에 대한 패치를 구성할 것을 권장합니다. 또한 다음 절차에서 설명한 대로 Systems Manager 문서를 사용하여 인스턴스를 패치할 수 있습니다.

규정 미준수 패치를 해결하려면

1. https://console.aws.amazon.com/systems-manager/ 에서 AWS Systems Manager 콘솔을 엽니다.

2. 노드 관리에서 명령 실행을 선택한 다음 명령 실행을 선택합니다.
3. AWS-에 대한 옵션을 선택합니다RunPatchBaseline.
4. 작업을 설치로 변경합니다.
5. 수동으로 인스턴스 선택을 선택한 다음 규정 비준수 인스턴스를 선택합니다.
6. Run(실행)을 선택합니다.
7. 명령이 완료된 후 패치가 적용된 인스턴스의 새 규정 준수 상태를 모니터링하려면 탐색 창에서 규정 준수를 선택합니다.

[SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

관련 요구 사항: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8(1), NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SI-2(3)

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::SSM::AssociationCompliance`

AWS Config 규칙: `ec2-managedinstance-association-compliance-status-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 `COMPLIANT` 인스턴스에서 AWS Systems Manager 연결이 실행된 `NON_COMPLIANT` 이후인지 연결 상태인지 여부를 확인합니다. 연결 규정 준수 상태가 `NON_COMPLIANT`이면 제어가 실패합니다.

State Manager 연결은 관리형 인스턴스에 할당되는 구성입니다. 이러한 구성은 인스턴스에서 관리하려는 상태를 정의합니다. 예를 들어, 연결은 인스턴스에서 안티바이러스 소프트웨어가 설치되어 실행 중이어야 하는지 또는 특정 포트가 닫혀 있어야 하는지를 지정할 수 있습니다.

State Manager 연결을 하나 이상 생성하고 나면 규정 준수 상태 정보를 즉시 볼 수 있습니다. 콘솔에서 또는 AWS CLI 명령 또는 해당 Systems Manager API 작업에 대한 응답으로 규정 준수 상태를 볼 수 있

습니다. 연결의 경우 구성 규정 준수에는 규정 준수 상태(`Compliant` 또는 `Non-compliant`)가 표시됩니다. 또한 연결에 할당된 심각도 수준(예: `Critical` 또는 `Medium`)도 표시됩니다.

State Manager 연결 규정 준수에 대한 자세한 내용은 AWS Systems Manager 사용자 가이드에서 State Manager 연결 규정 준수 정보를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

실패한 연결은 대상 및 SSM 문서 이름을 비롯한 다양한 요인과 관련될 수 있습니다. 이 문제를 해결하려면 먼저 연결 기록을 확인하여 연결을 식별하고 조사해야 합니다. 연결 기록을 보는 방법에 대한 지침은 AWS Systems Manager 사용 설명서의 연결 기록 보기를 참조하십시오.

조사를 마친 후 연결을 편집하여 식별된 문제를 수정할 수 있습니다. 연결을 편집하여 새 이름, 일정, 심각도 수준 또는 대상을 지정할 수 있습니다. 연결을 편집한 후 새 버전을 AWS Systems Manager 생성합니다. 연결을 편집하는 방법에 대한 지침은 AWS Systems Manager 사용 설명서의 연결 편집 및 새 버전 생성을 참조하십시오.

[SSM.4] SSM 문서는 공개해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::SSM::Document`

AWS Config 규칙: `ssm-document-not-public`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 해당 계정이 소유한 AWS Systems Manager 문서가 공개되었는지 여부를 확인합니다. 소유자가 `Self`인 SSM 문서가 공개되면 이 제어가 실패합니다.

공개된 SSM 문서는 문서에 의도하지 않은 액세스를 허용할 수 있습니다. 공개 SSM 문서는 계정, 리소스, 내부 프로세스에 대한 중요한 정보를 노출할 수 있습니다.

사용 사례에서 퍼블릭 공유가 필요한 경우가 아니면 Self가 소유한 Systems Manager 문서에 대한 퍼블릭 공유 설정을 차단하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

SSM 문서의 공개 공유를 차단하려면 AWS Systems Manager 사용 설명서의 SSM 문서에 대한 공개 공유 차단을 참조하십시오.

Amazon Elastic File System 제어

이러한 제어는 Amazon EFS 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/2.4.1, NIST.800-53.R5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.R5 SC-13, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6) SC-28

범주: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: AWS::EFS::FileSystem

AWS Config 규칙: efs-encrypted-check

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Amazon Elastic File System이 를 사용하여 AWS KMS파일 데이터를 암호화하도록 구성되어 있는지 여부를 확인합니다. 다음과 같은 경우에는 확인에 실패합니다.

- Encrypted는 DescribeFileSystems 응답에서 false로 설정됩니다.
- DescribeFileSystems 응답의 KmsKeyId 키가 efs-encrypted-check의 KmsKeyId 파라미터와 일치하지 않습니다.

참고로 이 제어는 efs-encrypted-check에 KmsKeyId 파라미터를 사용하지 않습니다. 이는 Encrypted 값만 확인합니다.

Amazon EFS의 중요한 데이터에 대한 보안 계층을 추가하려면 암호화된 파일 시스템을 생성해야 합니다. Amazon EFS는 저장 중인 파일 시스템에 대한 암호화를 지원합니다. Amazon EFS 파일 시스템을 생성할 때 저장 데이터 암호화를 활성화할 수 있습니다. Amazon EFS 암호화에 대한 자세한 내용은 Amazon Elastic File System 사용 설명서의 Amazon EFS의 데이터 암호화를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

새 Amazon EFS 파일 시스템을 암호화하는 방법에 대한 자세한 내용은 Amazon Elastic File System 사용 설명서의 미사용 데이터 암호화를 참조하십시오.

[EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 백업

심각도: 중간

리소스 유형: AWS::EFS::FileSystem

AWS Config 규칙: efs-in-backup-plan

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS Backup의 백업 계획에 추가되었는지 확인합니다. Amazon EFS 파일 시스템이 백업 계획에 포함되지 않은 경우 제어가 실패합니다.

백업 계획에 EFS 파일 시스템을 포함하면 데이터가 삭제되거나 손실되지 않도록 보호할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

기존 Amazon EFS 파일 시스템의 자동 백업을 활성화하려면 AWS Backup 개발자 안내서의 시작하기 4: Amazon EFS 자동 백업 생성을 참조하십시오.

[EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-6(10)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::EFS::AccessPoint`

AWS Config 규칙: `efs-access-point-enforce-root-directory`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EFS 액세스 포인트가 루트 디렉터리를 적용하도록 구성되어 있는지 확인합니다. `Path`의 값을 `/`(파일 시스템의 기본 루트 디렉터리)로 설정하면 제어가 실패합니다.

루트 디렉터리를 적용할 때 액세스 포인트를 사용하는 NFS 클라이언트는 파일 시스템의 루트 디렉터리 대신 액세스 포인트에 구성된 루트 디렉터리를 사용합니다. 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

이제 Security Hub가 와 통합되었습니다

Amazon EFS 액세스 포인트에 루트 디렉터리를 적용하는 방법에 대한 지침은 Amazon Elastic File System 사용 설명서의 액세스 포인트를 사용하여 루트 디렉터리 적용을 참조하십시오.

[EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-6(2)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::EFS::AccessPoint`

AWS Config 규칙: `efs-access-point-enforce-user-identity`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EFS 액세스 포인트가 사용자 자격 증명을 적용하도록 구성되었는지 여부를 확인합니다. EFS 액세스 포인트를 생성하는 동안 POSIX 사용자 자격 증명이 정의되지 않으면 이 제어가 실패합니다.

Amazon EFS 액세스 포인트는 EFS 파일 시스템에 대한 애플리케이션별 진입점으로, 공유 데이터 세트에 대한 애플리케이션 액세스를 더 쉽게 관리할 수 있도록 합니다. 액세스 포인트는 액세스 포인트를 통해 이루어지는 모든 파일 시스템 요청에 대해 사용자의 POSIX 그룹을 포함한 사용자 자격 증명을 적용할 수 있습니다. 또한 클라이언트가 지정된 디렉터리 또는 하위 디렉터리의 데이터에만 액세스할 수 있도록 파일 시스템에 대해 다른 루트 디렉터리를 적용할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Amazon EFS 액세스 포인트에 대한 사용자 자격 증명을 적용하려면 Amazon Elastic File System 사용 설명서의 액세스 포인트를 사용하여 사용자 자격 증명 적용을 참조하십시오.

[EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EFS::AccessPoint`

AWS Config규칙: `tagged-efs-accesspoint` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 제어는 Amazon EFS 액세스 포인트에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 액세스 포인트에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우

제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 액세스 포인트에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EFS 액세스 포인트에 태그를 추가하려면 Amazon Elastic File System 사용 설명서의 Amazon EFS 리소스 태그 지정을 참조하십시오.

[EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 중간

리소스 유형: `AWS::EFS::FileSystem`

AWS Config 규칙: `efs-mount-target-public-accessible`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon EFS 탑재 대상이 프라이빗 서브넷과 연결되어 있는지 여부를 확인합니다. 탑재 대상이 퍼블릭 서브넷과 연결되어 있는 경우 제어가 실패합니다.

기본적으로 파일 시스템은 생성한 가상 사설 클라우드 (VPC) 에서만 액세스할 수 있습니다. 인터넷에서 액세스할 수 없는 프라이빗 서브넷에 EFS 탑재 대상을 생성하는 것이 좋습니다. 이렇게 하면 인증된 사용자만 파일 시스템에 액세스할 수 있고 무단 액세스나 공격에 취약하지 않도록 할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

탑재 대상을 생성한 후에는 EFS 탑재 대상과 서브넷 간의 연결을 변경할 수 없습니다. 기존 탑재 대상을 다른 서브넷에 연결하려면 사설 서브넷에 새 탑재 대상을 만든 다음 이전 탑재 대상을 제거해야 합니다. 탑재 대상 관리에 대한 자세한 내용은 Amazon Elastic File System 사용 설명서의 탑재 대상 및 보안 그룹 생성 및 관리를 참조하십시오.

Amazon Elastic Kubernetes 서비스 제어

이러한 제어는 Amazon EKS 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::EKS::Cluster`

AWS Config 규칙: `eks-endpoint-no-public-access`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon EKS 클러스터 엔드포인트에 공개적으로 액세스할 수 있는지 여부를 확인합니다. EKS 클러스터에 공개적으로 액세스할 수 있는 엔드포인트가 있는 경우 제어가 실패합니다.

새 클러스터를 생성하면 Amazon EKS는 클러스터와 통신하는 데 사용하는 관리형 Kubernetes API 서버에 대한 엔드포인트를 생성합니다. 기본적으로 이 API 서버 엔드포인트는 인터넷에 공개적으로 사용

할 수 있습니다. API 서버에 대한 액세스는 AWS Identity and Access Management (IAM) 과 네이티브 쿠버네티스 역할 기반 액세스 제어 (RBAC) 의 조합을 사용하여 보호됩니다. 엔드포인트에 대한 퍼블릭 액세스를 제거하면 클러스터에 대한 의도하지 않은 노출 및 액세스를 방지할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

기존 EKS 클러스터의 엔드포인트 액세스를 수정하려면 Amazon EKS 사용 설명서의 클러스터 엔드포인트 액세스 수정을 참조하십시오. 새 EKS 클러스터를 생성할 때 해당 클러스터에 대한 엔드포인트 액세스를 설정할 수 있습니다. 새 Amazon EKS 클러스터 생성에 대한 지침은 Amazon EKS 사용 설명서의 Amazon EKS 클러스터 생성을 참조하십시오.

[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::EKS::Cluster`

AWS Config 규칙: `eks-cluster-supported-version`

스케줄 유형: 변경이 트리거됨

파라미터:

- `oldestVersionSupported`: `1.26`(사용자 지정할 수 없음)

이 제어는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터가 지원되는 Kubernetes 버전에서 실행되고 있는지 여부를 확인합니다. EKS 클러스터가 지원되지 않는 버전에서 실행 중인 경우 제어가 실패합니다.

애플리케이션에 특정 버전의 Kubernetes가 필요하지 않은 경우 클러스터에 대해 EKS에서 지원하는 사용 가능한 최신 Kubernetes 버전을 사용하는 것이 좋습니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS Kubernetes 릴리스 일정과 Amazon EKS 버전 지원 및 FAQ를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

EKS 클러스터를 업데이트하려면 Amazon EKS 사용 설명서의 Amazon EKS 클러스터 Kubernetes 버전 업데이트를 참조하세요.

[EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.

관련 요구 사항: NIST.800-53.R5 SC-8, NIST.800-53.R5 SC-12, NIST.800-53.r5 SC-13, NIST.800-53.r5 SI-28

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::EKS::Cluster`

AWS Config 규칙: `eks-secrets-encrypted`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Amazon EKS 클러스터가 암호화된 Kubernetes 암호를 사용하는지 여부를 확인합니다. 클러스터의 Kubernetes 암호가 암호화되지 않으면 제어가 실패합니다.

암호를 암호화할 때 AWS Key Management Service (AWS KMS) 키를 사용하여 클러스터의 etcd에 저장된 Kubernetes 암호를 봉투 암호화할 수 있습니다. 이 암호화는 EKS 클러스터의 일부로 etcd에 저장되는 모든 데이터 (암호 포함) 에 대해 기본적으로 활성화되는 EBS 볼륨 암호화에 추가됩니다. EKS 클러스터에 암호 암호화를 사용하면 사용자가 정의하고 관리하는 KMS 키로 Kubernetes 암호를 암호화하여 Kubernetes 애플리케이션을 위한 심층 방어 전략을 구축할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

EKS 클러스터에서 비밀 암호화를 활성화하려면 Amazon EKS 사용 설명서의 기존 클러스터에서 비밀 암호화 활성화를 참조하십시오.

[EKS.6] EKS 클러스터에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EKS::Cluster`

AWS Config규칙: `tagged-eks-cluster` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EKS 클러스터에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. 클러스터에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 클러스터에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EKS 클러스터에 태그를 추가하려면 Amazon EKS 사용 설명서의 Amazon EKS 리소스 태그 지정을 참조하십시오.

[EKS.7] EKS ID 공급자 구성에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EKS::IdentityProviderConfig`

AWS Config규칙: `tagged-eks-identityproviderconfig` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EKS ID 공급자 구성에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. 구성에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 구성에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EKS ID 공급자 구성에 태그를 추가하려면 Amazon EKS 사용 설명서의 Amazon EKS 리소스 태그 지정을 참조하십시오.

[EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(12), NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::EKS::Cluster`

AWS Config 규칙: `eks-cluster-logging-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon EKS 클러스터에 감사 로깅이 활성화되어 있는지 여부를 확인합니다. 클러스터에 감사 로깅이 활성화되어 있지 않으면 제어가 실패합니다.

EKS 컨트롤 플레인 로깅은 EKS 컨트롤 플레인의 감사 및 진단 로그를 계정의 Amazon CloudWatch Logs로 직접 제공합니다. 필요한 로그 유형을 선택할 수 있으며, 로그는 각 EKS 클러스터의 그룹에 로그 스트림으로 전송됩니다. CloudWatch 로깅은 EKS 클러스터의 액세스 및 성능에 대한 가시성을 제공합니다. EKS 클러스터의 EKS 컨트롤 플레인 로그를 CloudWatch Logs로 전송하면 감사 및 진단을 위한 작업을 중앙 위치에 기록할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

EKS 클러스터의 감사 로그를 활성화하려면 Amazon EKS 사용 설명서의 컨트롤 플레인 로그 활성화 및 비활성화를 참조하세요.

아마존 ElastiCache 컨트롤

이러한 컨트롤은 ElastiCache 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 백업 활성화

심각도: 높음

리소스 유형: `AWS::ElastiCache::CacheCluster`

AWS Config 규칙: **`elasticache-redis-cluster-automatic-backup-check`**

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`snapshotRetentionPeriod`	최소 스냅샷 보존 기간(일수)	Integer	1~35	1

이 컨트롤은 Amazon ElastiCache for Redis 클러스터에 자동 백업이 예약되어 있는지 평가합니다. Redis 클러스터에 대한 `SnapshotRetentionLimit`가 지정된 기간 미만이면 제어가 실패합니다. 스냅샷 보존 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 1일을 사용합니다.

Amazon ElastiCache for Redis 클러스터는 데이터를 백업할 수 있습니다. 클러스터를 복원하거나 새 클러스터를 시드하기 위해 백업을 사용할 수 있습니다. 백업은 클러스터의 모든 데이터와 클러스터의 메타데이터로 구성됩니다. 모든 백업은 Amazon Simple Storage Service(S3)에 쓰여지므로 내구성 있는 스토리지가 확보됩니다. 새로운 Redis 클러스터를 생성하고 백업 데이터로 채워 데이터를 복원할 수 있습니다. AWS Management Console, AWS Command Line Interface (AWS CLI) 및 ElastiCache API를 사용하여 백업을 관리할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

ElastiCache Redis용 클러스터에서 자동 백업을 예약하려면 Amazon ElastiCache 사용 설명서의 자동 백업 일정 잡기를 참조하십시오.

[ElastiCache.2] Redis 캐시 ElastiCache 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::ElastiCache::CacheCluster`

AWS Config 규칙: `elasticache-auto-minor-version-upgrade-check`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 ElastiCache for Redis가 마이너 버전 업그레이드를 캐시 클러스터에 자동으로 적용하는지 여부를 평가합니다. Redis 캐시 ElastiCache 클러스터의 경우 마이너 버전 업그레이드가 자동으로 적용되지 않으면 이 제어가 실패합니다.

`AutoMinorVersionUpgrade`새로운 마이너 캐시 엔진 버전이 출시되면 Redis에서 ElastiCache 캐시 클러스터를 자동으로 업그레이드하도록 설정할 수 있는 기능입니다. 이러한 업그레이드에는 보안 패치 및 버그 수정이 포함될 수 있습니다. 패치 설치 상태를 유지하는 up-to-date 것은 시스템 보안을 유지하기 위한 중요한 단계입니다.

이제 Security Hub가 와 통합되었습니다

기존 ElastiCache Redis용 캐시 클러스터에 자동 마이너 버전 업그레이드를 적용하려면 Amazon ElastiCache 사용 설명서의 엔진 버전 업그레이드를 참조하십시오.

[ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElastiCache::ReplicationGroup`

AWS Config 규칙: `elasticache-repl-grp-auto-failover-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Redis 복제 그룹에 자동 장애 조치가 활성화되어 있는지 ElastiCache 확인합니다. Redis 복제 그룹에 자동 장애 조치가 활성화되어 있지 않으면 이 제어가 실패합니다.

복제 그룹에 대해 자동 장애 조치가 활성화된 경우 기본 노드의 역할은 자동으로 읽기 전용 복제본 중 하나로 장애 조치됩니다. 이러한 장애 조치 및 복제본 승격을 통해 승격이 완료된 후 새 기본 복제본에 대한 쓰기를 재개할 수 있으므로 실패 시 전체 가동 중지 시간이 줄어듭니다.

이제 Security Hub가 와 통합되었습니다

기존 ElastiCache Redis용 복제 그룹의 자동 장애 조치를 활성화하려면 Amazon ElastiCache 사용 설명서의 ElastiCache 클러스터 수정을 참조하십시오. ElastiCache 콘솔을 사용하는 경우 자동 장애 조치를 활성화됨으로 설정하십시오.

[ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::ElastiCache::ReplicationGroup`

AWS Config 규칙: `elasticache-repl-grp-encrypted-at-rest`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Redis 복제 그룹이 유휴 상태에서 암호화되었는지 ElastiCache 확인합니다. ElastiCache Redis용 복제 그룹이 유휴 상태에서 암호화되지 않으면 이 제어가 실패합니다.

데이터를 저장 시 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. ElastiCache Redis의 경우 추가 보안 계층을 위해 복제 그룹을 유휴 상태에서 암호화해야 합니다.

이제 Security Hub가 와 통합되었습니다

ElastiCache Redis용 복제 그룹에서 유휴 암호화를 구성하려면 Amazon ElastiCache 사용 설명서의 유휴 암호화 활성화를 참조하십시오.

[ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::ElastiCache::ReplicationGroup`

AWS Config 규칙: `elasticache-repl-grp-encrypted-in-transit`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Redis 복제 그룹이 전송 중에 암호화되었는지 ElastiCache 확인합니다. ElastiCache Redis용 복제 그룹이 전송 중에 암호화되지 않으면 이 제어가 실패합니다.

전송 데이터를 암호화하면 권한이 없는 사용자가 네트워크 트래픽을 도청할 위험이 줄어듭니다. ElastiCache Redis용 복제 그룹에서 전송 중 암호화를 활성화하면 클러스터의 노드 간 또는 클러스터와 애플리케이션 간과 같이 데이터가 한 위치에서 다른 위치로 이동할 때마다 데이터가 암호화됩니다.

이제 Security Hub가 와 통합되었습니다

Redis 복제 그룹에서 전송 중 암호화를 구성하려면 Amazon ElastiCache 사용 설명서의 전송 중 암호화 활성화를 참조하십시오. ElastiCache

[ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::ElastiCache::ReplicationGroup`

AWS Config 규칙: `elasticache-repl-grp-redis-auth-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Redis 복제 그룹에 Redis ElastiCache AUTH가 활성화되어 있는지 확인합니다. Redis 버전의 노드가 6.0 미만이고 사용 중이 아닌 경우 ElastiCache Redis용 복제 그룹에 대한 제어가 실패합니다. `AuthToken`

Redis 인증 토큰 또는 비밀번호를 사용하는 경우 Redis는 클라이언트가 명령을 실행하도록 허용하기 전에 비밀번호를 요구하므로 데이터 보안이 향상됩니다. Redis 6.0 이상 버전의 경우 RBAC(역할 기반 액세스 제어)를 사용하는 것이 좋습니다. 6.0 이전의 Redis 버전에서는 RBAC가 지원되지 않으므로 이 제어는 RBAC 기능을 사용할 수 없는 버전만 평가합니다.

이제 Security Hub가 와 통합되었습니다

ElastiCache Redis용 복제 그룹에서 Redis AUTH를 사용하려면 Amazon 사용 설명서의 기존 ElastiCache Redis용 클러스터의 AUTH 토큰 수정을 참조하십시오. ElastiCache

[ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(5)

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::ElastiCache::CacheCluster`

AWS Config 규칙: `elasticache-subnet-group-check`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 ElastiCache 클러스터가 사용자 지정 서브넷 그룹으로 구성되어 있는지 확인합니다. 값이 `default` 있는 경우 ElastiCache 클러스터에 대한 `CacheSubnetGroupName` 제어가 실패합니다.

ElastiCache 클러스터를 시작할 때 기본 서브넷 그룹이 아직 없는 경우 기본 서브넷 그룹이 생성됩니다. 기본 그룹은 기본 Virtual Private Cloud(VPC)의 서브넷을 사용합니다. 클러스터가 있는 서브넷과 클러스터가 서브넷에서 상속하는 네트워킹을 더욱 제한하는 사용자 지정 서브넷 그룹을 사용하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

ElastiCache 클러스터의 새 서브넷 그룹을 생성하려면 Amazon ElastiCache 사용 설명서의 서브넷 그룹 생성을 참조하십시오.

AWS Elastic Beanstalk 제어:

이러한 제어는 Elastic Beanstalk 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다. AWS 리전자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7,NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::ElasticBeanstalk::Environment`

AWS Config 규칙: `beanstalk-enhanced-health-reporting-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Elastic Beanstalk 환경에 향상된 상태 보고가 활성화되어 있는지 여부를 확인합니다.

Elastic Beanstalk의 향상된 상태 보고 기능을 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다.

Elastic Beanstalk 고급 상태 보고는 식별된 문제의 심각도를 측정하고 조사할 수 있는 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다. 지원되는 Amazon 머신 이미지(AMI)에 포함된 Elastic Beanstalk 상태 에이전트는 환경 EC2 인스턴스의 로그와 지표를 평가합니다.

자세한 내용은 AWS Elastic Beanstalk 개발자 안내서의 향상된 상태 보고 및 모니터링을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

향상된 상태 보고를 활성화하는 방법에 대한 지침은 AWS Elastic Beanstalk 개발자 안내서의 Elastic Beanstalk 콘솔을 사용하여 향상된 상태 보고 활성화를 참조하십시오.

[ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-2,NIST.800-53.r5 SI-2(2),NIST.800-53.r5 SI-2(4),NIST.800-53.r5 SI-2(5)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::ElasticBeanstalk::Environment`

AWS Config 규칙: `elastic-beanstalk-managed-updates-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`UpdateLevel`	버전 업데이트 수준	Enum	`minor`, `patch`	기본값 없음

이 제어는 Elastic Beanstalk 환경에 대해 관리형 플랫폼 업데이트가 활성화되었는지 여부를 확인합니다. 관리형 플랫폼 업데이트가 활성화되지 않은 경우 제어가 실패합니다. 기본적으로 모든 유형의 플랫폼 업데이트가 활성화되면 제어가 통과됩니다. 필요에 따라 특정 업데이트 수준을 요구하는 사용자 지정 파라미터 값을 제공할 수 있습니다.

관리형 플랫폼 업데이트를 활성화하면 해당 환경에 사용 가능한 최신 플랫폼 수정 사항, 업데이트 및 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것은 시스템 보안의 중요한 단계입니다.

이제 Security Hub가 와 통합되었습니다

관리형 플랫폼 업데이트를 활성화하려면 AWS Elastic Beanstalk 개발자 안내서의 관리형 플랫폼 업데이트에서 관리형 플랫폼 업데이트를 구성하려면을 참조하세요.

[ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch

범주: 식별 > 로깅

심각도: 높음

리소스 유형: `AWS::ElasticBeanstalk::Environment`

AWS Config 규칙: `elastic-beanstalk-logs-to-cloudwatch`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`RetentionInDays`	만료 전 로그 이벤트를 유지할 일수	Enum	`1`, `3`, `5`, `7`, `14`, `30`, `60`, `90`, `120`, `150`, `180`, `365` , `400`, `545`, `731`, `1827`, `3653`	기본값 없음

이 컨트롤은 Elastic Beanstalk 환경이 로그를 Logs로 전송하도록 구성되어 있는지 여부를 확인합니다. CloudWatch Elastic Beanstalk 환경이 로그를 Logs로 전송하도록 구성되지 않은 경우 제어가 실패합니다. CloudWatch 필요에 따라 만료 전 지정된 일 수 동안 로그가 보존되는 경우에만 제어가 통과되도록 하려면 `RetentionInDays` 파라미터에 대한 사용자 지정 값을 제공하면 됩니다.

CloudWatch 애플리케이션 및 인프라 리소스에 대한 다양한 메트릭을 수집하고 모니터링할 수 있도록 도와줍니다. 또한 CloudWatch 사용하여 특정 지표를 기반으로 경보 조치를 구성할 수 있습니다. Elastic Beanstalk 환경에 대한 가시성을 높이려면 Elastic CloudWatch Beanstalk를 와 통합하는 것이 좋습니다. Elastic Beanstalk 로그에는 eb-activity.log, nginx 또는 Apache 프록시 서버 환경의 액세스 로그, 환경별 로그가 포함됩니다.

이제 Security Hub가 와 통합되었습니다

Elastic CloudWatch Beanstalk를 로그와 통합하려면 개발자 안내서의 인스턴스 CloudWatch 로그를 로그로 스트리밍을 참조하십시오.AWS Elastic Beanstalk

Elastic Load Balancing 제어

이러한 제어는 Elastic Load Balancing 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/2.3,PCI DSS v3.2.1/4.1, NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

범주: 감지 > 감지 서비스

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: `alb-http-to-https-redirection-check`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Application Load Balancer의 모든 HTTP 리스너에 HTTP에서 HTTPS로의 리디렉션이 구성되어 있는지 확인합니다. Application Load Balancer의 HTTP 리스너 중 하나라도 HTTP에서 HTTPS로의 리디렉션이 구성되어 있지 않으면 제어가 실패합니다.

Application Load Balancer를 사용하기 전에 리스너를 하나 이상 추가해야 합니다. 리스너는 구성한 프로토콜 및 포트를 사용하여 연결 요청을 확인하는 프로세스입니다. 리스너는 HTTP 및 HTTPS 프로토콜 모두를 지원합니다. HTTPS 리스너를 사용하여 암호화 및 암호 해독 작업을 로드 밸런서로 오프로드할 수 있습니다. 전송 중 암호화를 적용하려면 Application Load Balancer와 함께 리디렉션 작업을 사용하여 클라이언트 HTTP 요청을 포트 443의 HTTPS 요청으로 리디렉션해야 합니다.

자세한 정보는 Application Load Balancers 사용 설명서의 Application Load Balancer용 리스너를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

HTTP 요청을 HTTPS로 리디렉션하려면 Application Load Balancer 리스너 규칙을 추가하거나 기존 규칙을 편집해야 합니다.

새 규칙을 추가하는 방법에 대한 지침은 Application Load Balancer 사용 설명서의 규칙 추가를 참조하십시오. 프로토콜: 포트의 경우 HTTP를 선택한 다음 **80**를 입력합니다. 작업 추가, 리디렉션 대상에서 HTTPS를 선택한 다음 **443**를 입력합니다.

기존 규칙을 편집하는 방법에 대한 지침은 Application Load Balancer 사용 설명서의 규칙 편집을 참조하십시오. 프로토콜: 포트의 경우 HTTP를 선택한 다음 **80**를 입력합니다. 작업 추가, 리디렉션 대상에서 HTTPS를 선택한 다음 **443**를 입력합니다.

[ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(5), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: `elb-acm-certificate-required`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Certificate Manager (ACM)에서 제공하는 HTTPS/SSL 인증서를 Classic Load Balancer에서 사용하는지 여부를 확인합니다. HTTPS/SSL 리스너로 구성된 Classic Load Balancer가 ACM에서 제공한 인증서를 사용하지 않는 경우 제어가 실패합니다.

인증서를 생성하려면 ACM이나 SSL 및 TLS 프로토콜을 지원하는 도구(예: OpenSSL)를 사용할 수 있습니다. Security Hub에서는 ACM을 사용하여 로드 밸런서에 대한 인증서를 생성하거나 가져올 것을 권장합니다.

ACM은 Classic Load Balancer와 통합되므로 로드 밸런서에 인증서를 배포할 수 있습니다. 또한 이러한 인증서를 자동으로 갱신해야 합니다.

이제 Security Hub가 와 통합되었습니다

ACM SSL/TLS 인증서를 Classic Load Balancer와 연결하는 방법에 대한 자세한 내용은 AWS 지식 센터 문서 ACM SSL/TLS 인증서를 Classic, Application 또는 Network Load Balancer와 연결하려면 어떻게 해야 합니까?를 참조하십시오.

[ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

범주: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: `elb-tls-https-listeners-only`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Classic Load Balancer 리스너가 프런트엔드(클라이언트에서 로드 밸런서로) 연결을 위해 HTTPS 또는 TLS 프로토콜로 구성되어 있는지 확인합니다. 이 제어는 Classic Load Balancer에 리스너가 있는 경우에 적용할 수 있습니다. Classic Load Balancer에 리스너가 구성되어 있지 않은 경우 제어는 조사 결과를 보고하지 않습니다.

Classic Load Balancer 리스너가 프런트 엔드 연결용 TLS 또는 HTTPS로 구성된 경우 제어가 통과됩니다.

리스너가 프런트엔드 연결에 대해 TLS 또는 HTTPS로 구성되지 않은 경우 제어가 실패합니다.

로드 밸런서 사용을 시작하기 전에 하나 이상의 리스너를 추가해야 합니다. 리스너는 구성한 프로토콜 및 포트를 사용하여 연결 요청을 확인하는 프로세스입니다. 리스너는 HTTP 및 HTTPS/TLS 프로토콜을 모두 지원합니다. 로드 밸런서가 전송 중에 암호화 및 복호화 작업을 수행하도록 하려면 항상 HTTPS 또는 TLS 리스너를 사용해야 합니다.

이제 Security Hub가 와 통합되었습니다

이 문제를 해결하려면 TLS 또는 HTTPS 프로토콜을 사용하도록 리스너를 업데이트하십시오.

모든 비준수 리스너를 TLS/HTTPS 리스너로 변경하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 선택합니다.
3. Classic Load Balancer를 선택합니다.
4. 리스너 탭에서 편집을 선택합니다.
5. 로드 밸런서 프로토콜이 HTTPS 또는 SSL로 설정되지 않은 모든 리스너의 경우 설정을 HTTPS 또는 SSL로 변경합니다.
6. 수정된 모든 리스너의 경우 인증서 탭에서 기본값 변경을 선택합니다.
7. ACM 및 IAM 인증서에서 인증서를 선택합니다.
8. 기본값으로 저장을 선택합니다.
9. 리스너를 모두 업데이트한 후 저장을 선택합니다.

[ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.

관련 요구 사항: NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8(2)

범주: 보호 > 네트워크 보안

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: `alb-http-drop-invalid-header-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS 애플리케이션 로드 밸런서를 평가하여 잘못된 HTTP 헤더를 삭제하도록 구성되었는지 확인합니다. `routing.http.drop_invalid_header_fields.enabled` 값이 `false`로 설정되면 제어가 실패합니다.

기본적으로 Application Load Balancer는 잘못된 HTTP 헤더 값을 삭제하도록 구성되지 않습니다. 이러한 헤더 값을 제거하면 HTTP 비동기화 공격이 방지됩니다.

ELB.12가 활성화된 경우 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

이 문제를 해결하려면 잘못된 헤더 필드를 삭제하도록 로드 밸런서를 구성하십시오.

잘못된 헤더 필드를 삭제하도록 로드 밸런서를 구성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 로드 밸런서를 선택합니다.
3. Application Load Balancer를 선택합니다.
4. 작업에서 속성 편집을 선택합니다.
5. 잘못된 헤더 필드 삭제에서 활성화를 선택합니다.
6. 저장을 선택합니다.

[ELB.5] 애플리케이션 및 Classic Load Balancer 로깅이 활성화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: `elb-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Application Load Balancer와 Classic Load Balancer의 로깅이 활성화되었는지 확인합니다. `access_logs.s3.enabled` 이 `false`이면 제어는 실패합니다.

Elastic Load Balancing은 로드 밸런서에 전송된 요청에 대한 자세한 정보를 캡처하는 액세스 로그를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다. 이러한 액세스 로그를 사용하여 트래픽 패턴을 분석하고 문제를 해결할 수 있습니다.

자세한 정보는 Classic Load Balancer 사용 설명서의 Classic Load Balancer에 대한 액세스 로그를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

액세스 로그를 활성화하려면 Application Load Balancer 사용 설명서의 3단계: 액세스 로그 구성을 참조하십시오.

[ELB.6] 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: `elb-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 애플리케이션, 게이트웨이 또는 Network Load Balancer에 삭제 보호가 활성화되어 있는지 확인합니다. 삭제 보호를 사용하지 않도록 설정하면 제어가 실패합니다.

삭제 보호를 활성화하여 애플리케이션, 게이트웨이 또는 Network Load Balancer가 삭제되지 않도록 보호합니다.

이제 Security Hub가 와 통합되었습니다

로드 밸런서가 실수로 삭제되지 않도록 삭제 방지 기능을 활성화할 수 있습니다. 기본 설정상 로드 밸런서에 대한 삭제 방지 기능은 비활성화되어 있습니다.

로드 밸런서용 삭제 방지 기능을 활성화하는 경우 로드 밸런서를 삭제하기 전에 삭제 방지를 먼저 비활성화해야 합니다.

Application Load Balancer에 대한 삭제 보호를 활성화하려면 애플리케이션 로드 밸런서 사용 설명서의 삭제 보호를 참조하십시오. 게이트웨이 로드 밸런서에 대한 삭제 보호를 활성화하려면 게이트웨이 로드 밸런서 사용 설명서의 삭제 보호를 참조하십시오. Network Load Balancer에 대한 삭제 보호를 활성화하려면 네트워크 로드 밸런서 사용 설명서의 삭제 보호를 참조하십시오.

[ELB.7] Classic Load Balancer connection draining닝이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 복구 > 복원력

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config규칙: `elb-connection-draining-enabled` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Classic Load Balancer connection draining닝 활성화 여부를 확인합니다.

Classic Load Balancer connection draining닝을 활성화하면 로드 밸런서가 등록 취소 중이거나 비정상 상태인 인스턴스로의 요청 전송을 중지합니다. 이는 기존 연결을 열린 상태로 유지합니다. 이는 Auto Scaling 그룹의 인스턴스에서 연결이 갑자기 끊어지지 않도록 하는 데 특히 유용합니다.

이제 Security Hub가 와 통합되었습니다

Classic Load Balancer connection draining닝을 활성화하려면 Classic Load Balancer 사용 설명서의 Classic Load Balancer connection draining닝 구성을 참조하십시오.

[ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: `elb-predefined-security-policy-ssl-check`

스케줄 유형: 변경이 트리거됨

파라미터:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01`(사용자 지정할 수 없음)

이 제어는 Classic Load Balancer HTTPS/SSL 리스너가 사전 정의된 정책 `ELBSecurityPolicy-TLS-1-2-2017-01`을 사용하는지 여부를 확인합니다. Classic Load Balancer HTTPS/SSL 리스너가 `ELBSecurityPolicy-TLS-1-2-2017-01`을 사용하지 않으면 제어가 실패합니다.

보안 정책은 SSL 프로토콜, 암호 및 서버 순서 기본 설정 옵션의 조합입니다. 사전 정의된 정책은 클라이언트와 로드 밸런서 간의 SSL 협상 동안 지원할 암호, 프로토콜 및 기본 설정 순서를 제어합니다.

`ELBSecurityPolicy-TLS-1-2-2017-01`를 사용하면 특정 버전의 SSL 및 TLS를 비활성화해야 하는 규정 준수 및 보안 표준을 충족하는 데 도움이 됩니다. 자세한 정보는 Classic Load Balancer 사용 설명서의 Classic Load Balancer에 대한 사전 정의된 SSL 보안 정책을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Classic Load Balancer와 함께 사전 정의된 보안 정책 `ELBSecurityPolicy-TLS-1-2-2017-01`을 사용하는 방법에 대한 자세한 내용은 Classic Load Balancer 사용 설명서의 보안 설정 구성을 참조하십시오.

[ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: `elb-cross-zone-load-balancing-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 CLB(Classic Load Balancer)에 대해 영역 간 로드 밸런싱이 활성화되어 있는지 확인합니다. CLB에 대해 교차 영역 로드 밸런싱이 활성화되어 있지 않은 경우 제어가 실패합니다.

로드 밸런서 노드는 가용 영역에 등록된 대상에만 트래픽을 분산합니다. 교차 영역 로드 밸런싱을 비활성화하면 각 로드 밸런서 노드가 해당 가용 영역에 있는 등록된 대상 간에만 트래픽을 분산합니다. 등록된 대상의 수가 가용 영역 전체에 동일하지 않으면 트래픽이 균등하게 분산되지 않아 한 영역의 인스턴스가 다른 영역의 인스턴스와 비교하여 과도하게 사용될 수 있습니다. 교차 영역 로드 밸런싱이 활성화되면 Classic Load Balancer에 대한 각각의 로드 밸런서 노드가 활성화된 모든 가용 영역에 있는 등록된 인스턴스 간에 요청을 균등하게 분산합니다. 자세한 내용은 Elastic Load Balancing 사용 설명서의 교차 영역 로드 밸런싱을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Classic Load Balancer에서 교차 영역 로드 밸런싱을 활성화하려면 Classic Load Balancer 사용 설명서의 교차 영역 로드 밸런싱 활성화를 참조하십시오.

[ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: `clb-multiple-az`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`minAvailabilityZones`	최소 가용 영역의 수	Enum	`2, 3, 4, 5, 6`	2

이 제어는 Classic Load Balancer가 최소한 지정된 수의 가용 영역(AZ)에 걸쳐 구성되었는지 확인합니다. Classic Load Balancer가 최소한 지정된 수의 AZ에 걸쳐 있지 않으면 제어가 실패합니다. 최소 AZ 수에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 두 AZ를 사용합니다.

단일 가용 영역 또는 여러 가용 영역의 Amazon EC2 인스턴스에 수신 요청을 분산하도록 Classic Load Balancer를 설정할 수 있습니다. 여러 가용 영역에 걸쳐 있지 않은 Classic Load Balancer는 단독으로 구성된 가용 영역을 사용할 수 없게 되면 트래픽을 다른 가용 영역의 대상으로 리디렉션할 수 없습니다.

이제 Security Hub가 와 통합되었습니다

Classic Load Balancer에 가용 영역을 추가하려면 Classic Load Balancer 사용 설명서에서 Classic Load Balancer에 대한 서브넷 추가 또는 제거를 참조하세요.

[ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21), NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 데이터 보호 > 데이터 무결성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: `alb-desync-mode-check`

스케줄 유형: 변경이 트리거됨

파라미터:

- `desyncMode`: `defensive, strictest`(사용자 지정할 수 없음)

이 제어는 Application Load Balancer가 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어 있는지 확인합니다. Application Load Balancer가 방어 모드 또는 가장 엄격한 비동기 완화 모드로 구성되지 않은 경우 제어가 실패합니다.

HTTP 비동기화 문제로 인해 요청 밀수가 발생하고 애플리케이션이 요청 대기열이나 캐시 중독에 취약해질 수 있습니다. 결과적으로 이러한 취약성으로 인해 보안 인증 정보가 스터핑되거나 승인되지 않은 명령이 실행될 수 있습니다. 방어적 또는 가장 엄격한 비동기화 완화 모드로 구성된 애플리케이션 로드 밸런서는 HTTP 비동기화로 인해 발생할 수 있는 보안 문제로부터 애플리케이션을 보호합니다.

이제 Security Hub가 와 통합되었습니다

Application Load Balancer의 비동기화 완화 모드를 업데이트하려면 Application Load Balancer 사용 설명서의 비동기화 완화 모드를 참조하십시오.

[ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: `elbv2-multiple-az`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`minAvailabilityZones`	최소 가용 영역의 수	Enum	`2, 3, 4, 5, 6`	2

이 제어는 Elastic Load Balancer V2(애플리케이션, 네트워크 또는 게이트웨이 로드 밸런서)에 최소한 지정된 가용 영역(AZ) 수의 인스턴스가 등록되어 있는지 확인합니다. Elastic Load Balancer V2에 최소한 지정된 AZ 수의 인스턴스가 등록되어 있지 않으면 제어가 실패합니다. 최소 AZ 수에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 두 AZ를 사용합니다.

Elastic Load Balancing은 둘 이상의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. Elastic Load Balancing은 수신 트래픽이 시간이 지남에 따라 변경됨에 따라 로드 밸런서를 확장합니다. Elastic Load Balancer는 하나를 사용할 수 없는 경우 다른 가용성 영역으로 트래픽을 전달할 수 있으므로 서비스 가용성을 보장하기 위해 최소 두 개의 가용성 영역을 구성하는 것이 좋습니다. 가용 영역을 여러 개 구성하면 애플리케이션에 단일 장애 지점이 발생하는 것을 방지할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Application Load Balancer에 가용 영역을 추가하려면 Application Load Balancer 사용 설명서의 Application Load Balancer의 가용 영역을 참조하십시오. Network Load Balancer에 가용 영역을 추가하려면 네트워크 로드 밸런서 사용 설명서의 Network Load Balancer 를 참조하십시오. 게이트웨이 로드 밸런서에 가용 영역을 추가하려면 게이트웨이 로드 밸런서 사용 설명서의 게이트웨이 로드 밸런서 생성을 참조하십시오.

[ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21), NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 데이터 보호 > 데이터 무결성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: `clb-desync-mode-check`

스케줄 유형: 변경이 트리거됨

파라미터:

- `desyncMode`: `defensive, strictest`(사용자 지정할 수 없음)

이 제어는 Classic Load Balancer가 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어 있는지 확인합니다. Classic Load Balancer가 방어 모드 또는 가장 엄격한 비동기 완화 모드로 구성되지 않은 경우 제어가 실패합니다.

HTTP 비동기화 문제로 인해 요청 밀수가 발생하고 애플리케이션이 요청 대기열이나 캐시 중독에 취약해질 수 있습니다. 결과적으로 이러한 취약성으로 인해 보안 인증이 도용되거나 승인되지 않은 명령이 실행될 수 있습니다. 방어적이거나 가장 엄격한 비동기화 완화 모드로 구성된 Classic Load Balancer는 HTTP 비동기화로 인해 발생할 수 있는 보안 문제로부터 애플리케이션을 보호합니다.

이제 Security Hub가 와 통합되었습니다

Classic Load Balancer에서 비동기화 완화 모드를 업데이트하려면 Classic Load Balancer 사용 설명서의 비동기화 완화 모드 수정을 참조하십시오.

[ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF

관련 요구 사항: NIST.800-53.r5 AC-4(21)

범주: 보호 > 보호 서비스

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: `alb-waf-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Application Load Balancer가 AWS WAF 클래식 또는 AWS WAF 웹 액세스 제어 목록 (웹 ACL) 과 연결되어 있는지 여부를 확인합니다. AWS WAF 구성에 대한 `Enabled` 필드가 `false`로 설정된 경우 제어가 실패합니다.

AWS WAF 웹 애플리케이션과 API를 공격으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 를 사용하여 AWS WAF정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 일련의 규칙인 웹 ACL을 구성할 수 있습니다. Application Load Balancer를 AWS WAF 웹 ACL과 연결하여 악의적인 공격으로부터 보호하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

Application Load Balancer를 웹 ACL과 연결하려면 개발자 안내서의 리소스에 웹 ACL 연결 또는 연결 해제를 참조하십시오. AWS AWS WAF

Amazon EMR 제어

이러한 제어는 Amazon EMR 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::EMR::Cluster`

AWS Config 규칙: `emr-master-no-public-ip`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon EMR 클러스터의 프라이머리 노드에 퍼블릭 IP 주소가 있는지 확인합니다. 퍼블릭 IP 주소가 프라이머리 노드 인스턴스 중 하나와 연결되어 있는 경우 제어가 실패합니다.

퍼블릭 IP 주소는 인스턴스에 대한 `NetworkInterfaces` 구성의 `PublicIp` 필드에 지정됩니다. 이 제어는 `RUNNING` 또는 `WAITING` 상태에 있는 Amazon EMR 클러스터만 검사합니다.

이제 Security Hub가 와 통합되었습니다

시작하는 동안 기본 또는 기본이 아닌 서브넷의 인스턴스에 퍼블릭 IPv4 주소를 할당할지 여부를 제어할 수 있습니다. 기본적으로 기본 서브넷의 속성 값은 `true`로 설정되어 있습니다. 기본이 아닌 서브넷은 Amazon EC2 시작 인스턴스 마법사로 생성되지 않은 한 IPv4 퍼블릭 주소 지정 속성이 `false`로 설정되어 있습니다. 이 경우 속성이 `true`로 설정됩니다.

시작 후에는 인스턴스에서 퍼블릭 IPv4 주소를 수동으로 연결 해제할 수 없습니다.

실패한 결과를 수정하려면 IPv4 퍼블릭 주소 지정 속성이 `false`으로 설정된 프라이빗 서브넷이 있는 VPC에서 새 클러스터를 시작해야 합니다. 지침은 Amazon EMR 관리 안내서의 VPC로 클러스터 시작을 참조하세요.

[EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: `emr-block-public-access`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 계정이 Amazon EMR 퍼블릭 액세스 차단을 사용하여 구성되어 있는지 확인합니다. 퍼블릭 액세스 차단 설정이 활성화되지 않았거나 포트 22가 아닌 다른 포트가 허용되면 제어가 실패합니다.

Amazon EMR 퍼블릭 액세스 차단을 사용하면 클러스터에 포트의 퍼블릭 IP 주소로부터 들어오는 인바운드 트래픽을 허용하는 보안 구성이 있는 경우 퍼블릭 서브넷에서 클러스터를 시작할 수 없습니다.

AWS 계정 의 사용자가 클러스터를 시작하면 Amazon EMR은 클러스터의 보안 그룹에서 포트 규칙을 확인하고 이를 인바운드 트래픽 규칙과 비교합니다. 보안 그룹에 퍼블릭 IP 주소 IPv4 0.0.0.0/0 또는 IPv6: :/0에 대해 포트를 여는 인바운드 규칙이 있고 해당 포트가 계정에 대한 예외로 지정되지 않은 경우 Amazon EMR은 사용자의 클러스터 생성을 허용하지 않습니다.

> **Note**
>
> 퍼블릭 액세스 차단은 기본적으로 활성화되어 있습니다. 계정 보호를 강화하려면 이 기능을 활성화된 상태로 유지하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

Amazon EMR에 대한 퍼블릭 액세스 차단을 구성하려면 Amazon EMR 관리 가이드의 Amazon EMR 블록 퍼블릭 액세스 사용을 참조하세요.

Elasticsearch 제어

이러한 제어는 Elasticsearch 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다. AWS 리전자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/3.4, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-encrypted-at-rest`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Elasticsearch 도메인에 저장 시 암호화 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우 이 확인이 실패합니다.

민감한 데이터의 보안을 강화하려면 저장 시 암호화되도록 OpenSearch 구성해야 합니다. OpenSearch Elasticsearch 도메인은 저장 데이터 암호화를 제공합니다. 이 기능은 암호화 AWS KMS 키를 저장하고 관리하는 데 사용됩니다. 암호화를 수행하기 위해 256비트 키(AES-256)가 있는 고급 암호화 표준 알고리즘을 사용합니다.

저장 중 OpenSearch 암호화에 대해 자세히 알아보려면 Amazon OpenSearch OpenSearch Service 개발자 안내서의 Amazon Service용 미사용 데이터 암호화를 참조하십시오.

`t.small` 및 `t.medium` 등의 특정 인스턴스 유형은 저장 데이터의 암호화를 지원하지 않습니다. 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 지원되는 인스턴스 유형을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

신규 및 기존 Elasticsearch 도메인에 대해 저장 중 암호화를 활성화하려면 Amazon OpenSearch Service 개발자 안내서의 저장 데이터 암호화 활성화를 참조하십시오.

[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 심각

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-in-vpc-only`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Elasticsearch 도메인이 VPC에 있는지 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다. Elasticsearch 도메인이 퍼블릭 서브넷에 연결되어 있지 않은지 확인해야 합니다. Amazon OpenSearch 서비스 개발자 안내서의 리소스 기반 정책을 참조하십시오.

또한 권장 모범 사례에 따라 VPC가 구성되었는지 확인해야 합니다. 또한 Amazon VPC 사용 설명서에서 VPC에 대한 보안 모범 사례를 참조하십시오.

VPC 내에 배포된 Elasticsearch 도메인은 공용 인터넷을 통과할 필요 없이 사설 AWS 네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPC는 네트워크 ACL 및 보안 그룹을 포함하여 Elasticsearch 도메인에 대한 액세스를 보호하기 위한 여러 네트워크 제어를 제공합니다. Security Hub는 퍼블릭 Elasticsearch 도메인을 VPC로 마이그레이션하여 이러한 제어를 활용할 것을 권장합니다.

이제 Security Hub가 와 통합되었습니다

퍼블릭 엔드포인트가 있는 도메인을 만들 경우 나중에 해당 도메인을 VPC 안에 배치할 수 없습니다. 대신에 새 도메인을 만들어 데이터를 마이그레이션해야 합니다. 반대의 경우도 마찬가지입니다. VPC 내에 도메인을 만들 경우 퍼블릭 엔드포인트를 가질 수 없습니다. 대신 다른 도메인을 만들거나 이 제어를 비활성화해야 합니다.

Amazon OpenSearch 서비스 개발자 안내서의 VPC 내에서 Amazon OpenSearch 서비스 도메인 시작을 참조하십시오.

[ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-node-to-node-encryption-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Elasticsearch 도메인에 node-to-node 암호화가 활성화되어 있는지 확인합니다. Elasticsearch 도메인에 암호화가 활성화되어 있지 않으면 제어가 실패합니다. node-to-node 이 컨트롤은 Elasticsearch 버전이 암호화 검사를 지원하지 않는 경우에도 실패한 결과를 생성합니다. node-to-node

HTTPS (TLS) 를 사용하면 잠재적 공격자가 또는 유사한 공격을 사용하여 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다. person-in-the-middle 암호화된 HTTPS(TLS) 연결만 허용되어야 합니다. Elasticsearch node-to-node 도메인의 암호화를 활성화하면 전송 중에 클러스터 내 통신이 암호화됩니다.

이 구성과 관련하여 성능이 저하될 수 있습니다. 이 옵션을 활성화하기 전에 성능 균형을 파악하고 테스트해야 합니다.

이제 Security Hub가 와 통합되었습니다

신규 및 기존 도메인에서 node-to-node 암호화를 활성화하는 방법에 대한 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 node-to-node 암호화 활성화를 참조하십시오.

[ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 - 로깅

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-logs-to-cloudwatch`

스케줄 유형: 변경이 트리거됨

파라미터:

- `logtype = 'error'`(사용자 지정할 수 없음)

이 컨트롤은 Elasticsearch 도메인이 오류 로그를 로그로 전송하도록 구성되었는지 여부를 확인합니다. CloudWatch

Elasticsearch 도메인의 오류 로그를 활성화하고 보존 및 응답을 위해 해당 로그를 Logs로 보내야 CloudWatch 합니다. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

이제 Security Hub가 와 통합되었습니다

로그 게시를 활성화하는 방법에 대한 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 로그 게시 활성화 (콘솔) 를 참조하십시오.

[ES.5] Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-audit-logging-enabled` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

- `cloudWatchLogsLogGroupArnList`(사용자 지정할 수 없음). Security Hub는 이 파라미터를 채우지 않습니다. 감사 로그용으로 구성해야 하는 쉼표로 구분된 CloudWatch 로그 로그 그룹 목록입니다.

  이 규칙은 Elasticsearch 도메인의 CloudWatch 로그 로그 그룹이 이 파라미터 목록에 지정되지 않은 `NON_COMPLIANT` 경우에 적용됩니다.

이 제어는 Elasticsearch 도메인에 감사 로깅이 활성화되어 있는지 여부를 확인합니다. Elasticsearch 도메인에 감사 로깅이 활성화되어 있지 않으면 이 제어가 실패합니다.

감사 로그는 고도로 사용자 지정이 가능합니다. 이를 통해 인증 성공 및 실패, 요청, 색인 변경, 수신 검색 쿼리 등 Elasticsearch 클러스터에서의 사용자 활동을 추적할 수 OpenSearch 있습니다.

이제 Security Hub가 와 통합되었습니다

감사 로그 활성화에 대한 자세한 지침은 Amazon OpenSearch Service 개발자 안내서의 감사 로그 활성화를 참조하십시오.

[ES.6] Elasticsearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-data-node-fault-tolerance` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Elasticsearch 도메인이 최소 세 개의 데이터 노드로 구성되어 있고 `zoneAwarenessEnabled`이 `true`인지 확인합니다.

Elasticsearch 도메인에는 고가용성 및 내결함성을 위해 최소 3개의 데이터 노드가 필요합니다. 최소 3개의 데이터 노드가 있는 Elasticsearch 도메인을 배포하면 노드에 장애가 발생하더라도 클러스터 운영이 보장됩니다.

이제 Security Hub가 와 통합되었습니다

Elasticsearch 도메인의 데이터 노드 수를 수정하려면

1. https://console.aws.amazon.com/aos/ 에서 아마존 OpenSearch 서비스 콘솔을 엽니다.
2. 도메인에서 편집하려는 도메인의 이름을 선택합니다.
3. 도메인 편집을 선택합니다.
4. 데이터 노드에서 노드 수를 3 이상의 수로 설정합니다.

   3개의 가용 영역 배포의 경우 가용 영역 전체에 균등하게 배포되도록 3의 배수로 설정합니다.
5. 제출을 선택합니다.

[ES.7] Elasticsearch 도메인은 최소 3개의 전용 프라이머리 노드로 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config규칙: `elasticsearch-primary-node-fault-tolerance` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Elasticsearch 도메인이 3개 이상의 전용 기본 노드로 구성되어 있는지 확인합니다. 도메인이 전용 기본 노드를 사용하지 않으면 이 제어가 실패합니다. Elasticsearch 도메인에 5개의 전용 기본 노드가 있는 경우 이 제어는 통과됩니다. 하지만 가용성 위험을 줄이기 위해 기본 노드를 3개 이상 사용하는 것은 불필요할 수 있으며 추가 비용이 발생할 수 있습니다.

Elasticsearch 도메인에는 고가용성 및 내결함성을 위해 최소 3개의 전용 기본 노드가 필요합니다. 관리해야 할 추가 노드가 있기 때문에 데이터 노드 블루/그린 배포 중에는 전용 기본 노드 리소스에 부담을 줄 수 있습니다. 최소 3개의 전용 기본 노드와 함께 Elasticsearch 도메인을 배포하면 노드에 장애가 발생할 경우 충분한 기본 노드 리소스 용량과 클러스터 운영이 보장됩니다.

이제 Security Hub가 와 통합되었습니다

도메인의 전용 기본 노드 수를 수정하려면 OpenSearch

1. https://console.aws.amazon.com/aos/ 에서 아마존 OpenSearch 서비스 콘솔을 엽니다.
2. 도메인에서 편집하려는 도메인의 이름을 선택합니다.
3. 도메인 편집을 선택합니다.
4. 전용 프라이머리 노드에서 인스턴스 유형을 원하는 인스턴스 유형으로 설정합니다.
5. 프라이머리 노드 수를 3개 이상으로 설정합니다.
6. 제출을 선택합니다.

[ES.8] Elasticsearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3),

NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-https-required` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Elasticsearch 도메인 엔드포인트가 최신 TLS 보안 정책을 사용하도록 구성되었는지 여부를 확인합니다. Elasticsearch 도메인 엔드포인트가 지원되는 최신 정책을 사용하도록 구성되지 않았거나 HTTP가 활성화되지 않은 경우 제어가 실패합니다. 현재 지원되는 최신 TLS 보안 정책은 입니다. `Policy-Min-TLS-1-2-PFS-2023-10`

HTTPS (TLS) 는 잠재적 공격자가 네트워크 트래픽을 도청하거나 조작하기 위해 person-in-the-middle 또는 유사한 공격을 사용하는 것을 방지하는 데 사용할 수 있습니다. 암호화된 HTTPS(TLS) 연결만 허용되어야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 이해해야 합니다. TLS 1.2는 이전 버전의 TLS보다 몇 가지 향상된 보안 기능을 제공합니다.

이제 Security Hub가 와 통합되었습니다

TLS 암호화를 활성화하려면 API 작업을 사용하여 객체를 구성하십시오. UpdateDomainConfigDomainEndpointOptions 이렇게 하면 가 설정됩니다. `TLSSecurityPolicy`

[ES.9] Elasticsearch 도메인에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `tagged-elasticsearch-domain` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Elasticsearch 도메인에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다. `requiredTagKeys` 도메인에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 도메인에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Elasticsearch 도메인에 태그를 추가하려면 Amazon OpenSearch 서비스 개발자 안내서의 태그 사용을 참조하십시오.

아마존 EventBridge 컨트롤

이러한 컨트롤은 EventBridge 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Events::EventBus`

AWS Config 규칙: `tagged-events-eventbus` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon EventBridge 이벤트 버스에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 이벤트 버스에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 이벤트 버스에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를

추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

EventBridge 이벤트 버스에 태그를 추가하려면 Amazon EventBridge 사용 설명서의 Amazon EventBridge 태그를 참조하십시오.

[EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(3)

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 낮음

리소스 유형: `AWS::Events::EventBus`

AWS Config 규칙: `custom-schema-registry-policy-attached`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon EventBridge 사용자 지정 이벤트 버스에 리소스 기반 정책이 연결되어 있는지 확인합니다. 사용자 지정 이벤트 버스에 리소스 기반 정책이 없는 경우 이 제어가 실패합니다.

기본적으로 EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있지 않습니다. 이렇게 하면 계정의 보안 주체가 이벤트 버스에 액세스할 수 있습니다. 이벤트 버스에 리소스 기반 정책을 연결하면 이벤트 버스에 대한 액세스를 지정된 계정으로 제한할 수 있을 뿐만 아니라 의도적으로 다른 계정의 엔터티에 대한 액세스 권한을 부여할 수도 있습니다.

이제 Security Hub가 와 통합되었습니다

리소스 기반 정책을 EventBridge 사용자 지정 이벤트 버스에 연결하려면 Amazon EventBridge User Guide의 이벤트 버스 권한 관리를 참조하십시오.

[EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Events::Endpoint`

AWS Config 규칙: `global-endpoint-event-replication-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon EventBridge 글로벌 엔드포인트에 대한 이벤트 복제가 활성화되어 있는지 확인합니다. 글로벌 엔드포인트에서 이벤트 복제가 활성화되지 않은 경우 제어가 실패합니다.

글로벌 엔드포인트는 애플리케이션의 리전별 내결함성을 높이는 데 도움이 됩니다. 시작하려면 Amazon Route 53 상태 확인을 엔드포인트에 할당합니다. 장애 조치가 시작되면 상태 확인에서 "비정상" 상태를 보고합니다. 장애 조치가 시작된 후 몇 분 이내에 모든 사용자 지정 이벤트는 보조 리전의 이벤트 버스로 라우팅되고 해당 이벤트 버스에 의해 처리됩니다. 글로벌 엔드포인트를 사용하면 이벤트 복제를 활성화할 수 있습니다. 이벤트 복제는 관리형 규칙을 사용하여 모든 사용자 지정 이벤트를 기본 및 보조 리전의 이벤트 버스로 전송합니다. 글로벌 엔드포인트를 설정할 때는 이벤트 복제를 활성화하는 것이 좋습니다. 이벤트 복제를 통해 글로벌 엔드포인트가 올바르게 구성되었는지 확인할 수 있습니다. 장애 조치 이벤트에서 자동으로 복구하려면 이벤트 복제가 필요합니다. 이벤트 복제를 활성화하지 않은 경우 이벤트가 기본 리전으로 다시 라우팅되기 전에 Route 53 상태 확인을 "정상"으로 수동으로 재설정해야 합니다.

> **Note**
>
> 사용자 지정 이벤트 버스를 사용하는 경우 장애 조치가 제대로 작동하려면 각 리전에 동일한 이름과 동일한 계정을 가진 사용자 정의 짝수 버스가 필요합니다. 이벤트 복제를 활성화하면 월별 비용이 증가할 수 있습니다. 요금에 대한 자세한 내용은 Amazon EventBridge 요금을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

EventBridge 글로벌 엔드포인트에 대한 이벤트 복제를 활성화하려면 Amazon EventBridge 사용 설명서의 글로벌 엔드포인트 생성을 참조하십시오. 이벤트 복제의 경우 이벤트 복제 활성화를 선택합니다.

Amazon FSx 제어

이러한 제어는 Amazon FSx 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다. AWS 리전자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::FSx::FileSystem`

AWS Config 규칙: `fsx-openzfs-copy-tags-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있는지 확인합니다. OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되지 않은 경우 제어가 실패합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 태그를 사용하면 AWS 리소스를 다양한 방식 (예: 목적, 소유자 또는 환경) 으로 분류할 수 있습니다. 이 기능은 동일 유형의 리소스가 많을 때 유용합니다. 지정한 태그에 따라 특정 리소스를 빠르게 식별할 수 있기 때문입니다.

이제 Security Hub가 와 통합되었습니다

백업 및 볼륨에 태그를 복사하도록 OpenZFS용 FSX를 구성하려면 Amazon FSX OpenZFS 사용 설명서의 파일 시스템 업데이트를 참조하세요.

[FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.

관련 요구 사항: NIST.800-53.R5 CP-9, NIST.800-53.R5 CM-8

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::FSx::FileSystem`

AWS Config 규칙: `fsx-lustre-copy-tags-to-backups`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon FSx for Lustre 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있는지 여부를 확인합니다. Lustre 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되지 않은 경우 제어가 실패합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 태그를 사용하면 AWS 리소스를 다양한 방식 (예: 목적, 소유자 또는 환경) 으로 분류할 수 있습니다. 이 기능은 동일 유형의 리소스가 많을 때 유용합니다. 지정한 태그에 따라 특정 리소스를 빠르게 식별할 수 있기 때문입니다.

이제 Security Hub가 와 통합되었습니다

태그를 백업에 복사하도록 FSx for Lustre 파일 시스템을 구성하려면 Amazon FSX OpenZFS 사용 설명서의 파일 시스템 업데이트를 참조하십시오.

AWS Global Accelerator 컨트롤:

이러한 컨트롤은 글로벌 액셀러레이터 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::GlobalAccelerator::Accelerator`

AWS Config 규칙: `tagged-globalaccelerator-accelerator` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS Global Accelerator 액셀러레이터에 매개변수에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. 액셀러레이터에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 컨트롤이 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 가속기에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

글로벌 액셀러레이터 글로벌 액셀러레이터에 태그를 추가하려면 개발자 안내서의 태깅을 참조하십시오. AWS Global AcceleratorAWS Global Accelerator

AWS Glue 컨트롤

이러한 제어는 AWS Glue 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Glue::Job`

AWS Config 규칙: `tagged-glue-job` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 AWS Glue 작업에 매개변수에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredTagKeys. 작업에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 제어가 requiredTagKeys 실패합니다. 매개 변수를 requiredTagKeys 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 작업에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 aws: 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

AWS Glue 작업에 태그를 추가하려면 AWS Glue 사용 설명서의AWS 태그를 참조하십시오. AWS Glue

아마존 GuardDuty 컨트롤

이러한 컨트롤은 GuardDuty 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[GuardDuty.1] 을 GuardDuty 활성화해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/11.4, NIST.800-53.r5 AC-2(12), NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 CM-8(3), NIST.800-53.r5 RA-3(4), NIST.800-53.r5 SA-11(1), NIST.800-53.r5 SA-11(6), NIST.800-53.r5 SA-15(2), NIST.800-53.r5

SA-15(8), NIST.800-53.r5 SA-8(19), NIST.800-53.r5 SA-8(21), NIST.800-53.r5 SA-8(25), NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-5(1), NIST.800-53.r5 SC-5(3), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(1), NIST.800-53.r5 SI-4(13), NIST.800-53.r5 SI-4(2), NIST.800-53.r5 SI-4(22), NIST.800-53.r5 SI-4(25), NIST.800-53.r5 SI-4(4), NIST.800-53.r5 SI-4(5)

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `guardduty-enabled-centralized`

스케줄 유형: 주기적

파라미터: 없음

이 GuardDuty 컨트롤은 GuardDuty 계정 및 지역에서 Amazon이 활성화되어 있는지 확인합니다.

지원되는 모든 GuardDuty AWS 지역에서 활성화하는 것이 좋습니다. 이렇게 하면 GuardDuty 활발히 사용하지 않는 지역에서도 승인되지 않았거나 비정상적인 활동에 대한 결과를 얻을 수 있습니다. 또한 GuardDuty 이를 통해 AWS 서비스 IAM과 같은 글로벌 CloudTrail 이벤트를 모니터링할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

이 문제를 해결하려면 활성화하십시오. GuardDuty

여러 계정을 관리하는 방법을 GuardDuty 포함하여 활성화하는 방법에 대한 자세한 내용은 Amazon 사용 AWS Organizations GuardDuty 설명서의 GuardDuty시작하기를 참조하십시오.

[GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::GuardDuty::Filter`

AWS Config 규칙: `tagged-guardduty-filter` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon GuardDuty 필터에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 필터에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 필터에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

GuardDuty 필터에 태그를 추가하려면 Amazon GuardDuty API 참조를 참조하십시오 TagResource.

[GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::GuardDuty::IPSet`

AWS Config 규칙: `tagged-guardduty-ipset` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon GuardDuty IPSet에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. IPset에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 IPset에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

GuardDuty IPset에 태그를 추가하려면 Amazon GuardDuty API 참조를 참조하십시오 TagResource.

[GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config 규칙: `tagged-guardduty-detector` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon GuardDuty 감지기에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 탐지기에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 탐지기에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

GuardDuty 탐지기에 태그를 추가하려면 Amazon GuardDuty API 참조를 참조하십시오 TagResource.

AWS Identity and Access Management 컨트롤

이러한 제어는 IAM 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

관련 요구 사항: PCI DSS v3.2.1/7.2.1, CIS 재단 벤치마크 v1.2.0/1.22, CIS AWS 재단 벤치마크 v1.4.0/1.16, NIST.800-53.r5 AC-2, NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (15), AWS NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 .800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.R5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2), NIST.800-53.r5 AC-6 (3)

범주: 보호 > 보안 액세스 관리

심각도: 높음

리소스 유형: `AWS::IAM::Policy`

AWS Config 규칙: `iam-policy-no-statements-with-admin-access`

스케줄 유형: 변경이 트리거됨

파라미터:

- `excludePermissionBoundaryPolicy: true`(사용자 지정할 수 없음)

이 제어는 `"Resource": "*"`에 대해 `"Effect": "Allow"`과 `"Action": "*"`이 있는 문을 포함하여 기본 버전의 IAM 정책(고객 관리형 정책이라고도 함)에 관리자 액세스 권한이 있는지 확인합니다. 이러한 문이 포함된 IAM 정책이 있으면 제어가 실패합니다.

제어는 사용자가 생성한 고객 관리형 정책만 확인합니다. 인라인 및 AWS 관리형 정책은 확인하지 않습니다.

IAM 정책에서는 사용자, 그룹 또는 역할에 부여되는 권한 세트를 정의합니다. 표준 보안 AWS 권고에 따라 최소 권한, 즉 작업 수행에 필요한 권한만 부여하는 것이 좋습니다. 사용자에게 있어야 하는 최소한의 권한 집합으로 제한하지 않고 전체 관리 권한을 제공하면 리소스가 원치 않는 작업에 노출될 수 있습니다.

전체 관리 권한을 허용하는 대신 사용자가 해야 할 작업을 파악한 후 해당 작업만 수행하도록 정책을 작성합니다. 최소한의 권한 집합으로 시작하여 필요에 따라 추가 권한을 부여하는 것이 안전합니다. 처음부터 권한을 많이 부여하지 말고 나중에 강화하세요.

`"Resource": "*"`에 대해 `"Effect": "Allow"` 과 `"Action": "*"`이 있는 문이 있는 IAM 정책을 제거해야 합니다.

> **Note**
>
> AWS Config Security Hub를 사용하는 모든 지역에서 활성화되어야 합니다. 그러나 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

전체 “*” 관리 권한이 허용되지 않도록 IAM 정책을 수정하려면 IAM 사용 설명서의 IAM 정책 편집을 참조하십시오.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

관련 요구 사항: PCI DSS v3.2.1/7.2.1, CIS 재단 벤치마크 v3.0.0/1.15, CIS AWS 재단 벤치마크 v1.2.0/1.16, NIST.800-53.R5 AC-2, NIST.800-53.R5 AC-2 (1), NIST.800-53.r5 AC-3 (15), AWS NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5

AC-3 (15), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC800-53.r5 AC-3 (7), NIST.800-53.R5 AC-6, NIST.800-53.R5 AC-6 (3)

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `iam-user-no-policies-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 IAM 사용자에게 정책이 연결되어 있는지 확인합니다. IAM 사용자에게 정책이 연결되어 있는 경우 제어가 실패합니다. 대신 IAM 사용자는 IAM 그룹에서 권한을 상속하거나 역할을 맡아야 합니다.

기본적으로 IAM 사용자, 그룹, 역할은 AWS 리소스에 액세스할 수 없습니다. IAM 정책은 사용자, 그룹 또는 역할에 권한을 부여하는 방법입니다. IAM 정책을 사용자가 아닌 그룹 및 역할에 직접 적용하는 것이 좋습니다. 그룹 또는 역할 수준에서 권한을 지정하면 사용자 수가 증가할 때 액세스 관리 복잡성이 줄어듭니다. 액세스 관리 복잡성을 줄이면 보안 주체가 부주의로 과도한 권한을 받거나 보유할 기회가 줄어듭니다.

> **Note**
>
> Amazon Simple Email Service에서 생성된 IAM 사용자는 인라인 정책을 사용하여 자동으로 생성됩니다. Security Hub는 이러한 사용자를 이 제어에서 자동으로 제외합니다.
> AWS Config Security Hub를 사용하는 모든 지역에서 활성화되어야 합니다. 그러나 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

이 문제를 해결하려면 IAM 그룹을 생성하고 정책을 그룹에 연결하십시오. 그런 다음 사용자를 그룹에 추가합니다. 정책은 그룹 내 각 사용자에게 적용됩니다. 사용자에게 직접 연결된 정책을 제거하려면 IAM 사용 설명서의 IAM 자격 증명 권한 추가 및 제거를 참조하십시오.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/1.14, CIS 재단 벤치마크 v1.4.0/1.14, CIS AWS AWS 재단 벤치마크 v1.2.0/1.4, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `access-keys-rotated`

스케줄 유형: 주기적

파라미터:

- `maxAccessKeyAge`: `90`(사용자 지정할 수 없음)

이 제어는 활성 액세스 키가 90일마다 교체되는지 여부를 확인합니다.

사용자 계정에서 모든 액세스 키를 생성 및 제거하지 않는 것이 좋습니다. 대신 하나 이상의 IAM 역할을 생성하거나 페더레이션을 사용하는 것이 가장 좋습니다 AWS IAM Identity Center. 이러한 방법을 사용하여 사용자가 AWS Management Console 및 AWS CLI에 액세스하도록 허용할 수 있습니다.

각 접근법에는 사용 사례가 있습니다. 페더레이션은 일반적으로 기존 중앙 디렉터리가 있거나 IAM 사용자에 대한 현재 제한보다 더 많은 것이 필요할 것으로 예상되는 기업에 더 좋습니다. AWS 환경 외부에서 실행되는 애플리케이션에는 프로그래밍 방식으로 AWS 리소스에 액세스하기 위한 액세스 키가 필요합니다.

하지만 프로그래밍 방식 액세스가 필요한 리소스가 내부에서 AWS실행되는 경우 IAM 역할을 사용하는 것이 가장 좋습니다. 역할을 사용하면 액세스 키 ID 및 보안 액세스 키를 구성에 하드 코딩하지 않고도 리소스 액세스 권한을 부여할 수 있습니다.

액세스 키와 계정을 보호하는 방법에 대한 자세한 내용은 의 액세스 키 관리 AWS 모범 사례를 참조하십시오. AWS 일반 참조 프로그래밍 방식 액세스를 사용하는 AWS 계정 동안 사용자를 보호하기 위한 블로그 게시물 지침도 참조하십시오.

이미 액세스 키가 있는 경우, Security Hub는 사용자가 90일마다 액세스 키를 교체하는 것을 권장합니다. 액세스 키를 교체하면 손상되거나 종료된 계정에 연결된 액세스 키가 사용될 가능성이 줄어듭니다.

또한 분실, 해킹 또는 도용된 기존 키로 데이터에 액세스할 수 없도록 합니다. 액세스 키를 교체한 후에는 항상 애플리케이션을 업데이트하세요.

액세스 키는 액세스 키 ID와 보안 액세스 키로 구성되어 있습니다. 이 키들은 AWS에 보내는 프로그래밍 방식의 요청에 서명하는 데 사용됩니다. 사용자는 PowerShell Windows용 도구 AWS CLI, AWS AWS SDK에서 프로그래밍 방식으로 호출하거나 개인용 API 작업을 사용하여 직접 HTTP 호출을 하려면 고유한 액세스 키가 필요합니다. AWS 서비스

조직에서 AWS IAM Identity Center (IAM ID 센터) 를 사용하는 경우 사용자는 Active Directory, 내장된 IAM ID 센터 디렉터리 또는 IAM ID 센터에 연결된 다른 ID 공급자 (IdP) 에 로그인할 수 있습니다. 그런 다음 액세스 키 없이도 AWS CLI 명령을 실행하거나 AWS API 작업을 호출할 수 있는 IAM 역할에 매핑할 수 있습니다. 자세히 알아보려면 사용 AWS Command Line Interface 설명서의 사용을 AWS CLIAWS IAM Identity Center위한 구성을 참조하십시오.

> **Note**
>
> AWS Config Security Hub를 사용하는 모든 지역에서 활성화되어야 합니다. 그러나 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

90일이 지난 액세스 키를 교체하려면 IAM 사용 설명서의 액세스 키 교체를 참조하십시오. 액세스 키 사용 기간이 90일 이상인 모든 사용자의 지침을 따르십시오.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/1.4, CIS 재단 벤치마크 v1.4.0/1.4, CIS AWS 재단 벤치마크 v1.2.0/1.12, PCI DSS v3.2.1/2.1, PCI DSS AWS v3.2.1/2.2, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (7), NIST.800-53.R5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.R5 AC-6 (2)

범주: 보호 > 보안 액세스 관리

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-root-access-key-check`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 루트 사용자 액세스 키가 존재하는지 확인합니다.

루트 사용자는 에서 가장 권한이 있는 AWS 계정사용자입니다. AWS 액세스 키는 지정된 계정에 프로그래밍 방식으로 액세스할 수 있도록 합니다.

Security Hub에서는 루트 사용자와 연결된 모든 액세스 키를 제거할 것을 권장합니다. 이렇게 하면 계정을 손상시킬 수 있는 벡터가 제한됩니다. 권한이 가장 적은 역할 기반 계정을 만들고 사용할 수도 있습니다.

이제 Security Hub가 와 통합되었습니다

루트 사용자 액세스 키를 삭제하려면 IAM 사용 설명서의 루트 사용자의 액세스 키 삭제를 참조하십시오. in에서 루트 사용자 액세스 키를 삭제하려면 사용 설명서의 내 AWS GovCloud (US) 계정 루트 사용자 액세스 키 삭제를 참조하십시오. AWS 계정 AWS GovCloud (US)AWS GovCloud (US)

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/1.10, CIS 재단 벤치마크 v1.4.0/1.10, CIS AWS AWS 재단 벤치마크 v1.2.0/1.2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (1) A-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 (8)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `mfa-enabled-for-iam-console-access`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 콘솔 비밀번호를 사용하는 모든 IAM 사용자에 대해 AWS 멀티 팩터 인증 (MFA) 이 활성화되어 있는지 확인합니다.

다중 인증(MFA)을 통해 사용자 이름 및 비밀번호 외에 보호 계층이 한 단계 더 추가됩니다. MFA를 활성화하면 사용자가 AWS 웹 사이트에 로그인할 때 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다. 또한 AWS MFA 디바이스에서 인증 코드를 입력하라는 메시지가 표시됩니다.

콘솔 암호가 있는 모든 계정에 대해 MFA를 활성화하는 것이 좋습니다. MFA는 콘솔 액세스의 보안을 강화하도록 설계되었습니다. 인증 주체는 시간에 민감한 키를 내보내는 디바이스를 가지고 있어야 하며 보안 인증에 대한 지식이 있어야 합니다.

> **Note**
>
> AWS Config Security Hub를 사용하는 모든 지역에서 활성화되어야 합니다. 그러나 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

IAM 사용자를 위한 MFA를 추가하려면 IAM 사용 설명서의 AWS에서의 다중 인증(MFA) 사용을 참조하십시오.

MFA 보안 키는 자격을 갖춘 고객에게 무료로 제공됩니다. 자격이 되는지 확인하고 무료 키를 주문하십시오.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/1.6, CIS 재단 벤치마크 v1.4.0/1.6, CIS AWS 재단 벤치마크 v1.2.0/1.14, PCI DSS v3.2.1/8.3.1, AWS NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 (8)

범주: 보호 > 보안 액세스 관리

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: `root-account-hardware-mfa-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 AWS 계정 컨트롤은 하드웨어 멀티 팩터 인증 (MFA) 디바이스를 사용하여 루트 사용자 자격 증명으로 로그인할 수 있는지 여부를 확인합니다. MFA가 활성화되지 않았거나 가상 MFA 디바이스가 루트 사용자 보안 인증 정보로 로그인하도록 허용된 경우 제어가 실패합니다.

가상 MFA는 하드웨어 MFA 디바이스와 동일한 수준의 보안을 제공하지 않을 수 있습니다. 하드웨어 구매 승인 또는 하드웨어 도착을 기다리는 동안 가상 MFA 디바이스만 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 가상 다중 인증(MFA) 디바이스 활성화(콘솔)를 참조하십시오.

시간 기반 일회용 암호(TOTP) 및 유니버설 세컨드 팩터(U2F) 토큰 모두 하드웨어 MFA 옵션으로 사용 가능합니다.

이제 Security Hub가 와 통합되었습니다

루트 사용자를 위한 하드웨어 MFA 디바이스를 추가하려면 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔) 용 하드웨어 MFA 디바이스 활성화를 참조하십시오.

MFA 보안 키는 자격을 갖춘 고객에게 무료로 제공됩니다. 자격이 되는지 확인하고 무료 키를 주문하세요.

[IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-2(3), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 IA-5(1)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`RequireUppercaseCharacters`	암호에 대문자가 한 개 이상 있어야 합니다.	불	`true` 또는 `false`	`true`
`RequireLowercaseCharacters`	암호에 소문자가 한 개 이상 있어야 합니다.	불	`true` 또는 `false`	`true`

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
RequireSymbols	암호에 기호가 한 개 이상 있어야 합니다.	불	true 또는 false	true
RequireNumbers	암호에 숫자가 한 개 이상 있어야 합니다.	불	true 또는 false	true
MinimumPasswordLength	암호의 최소 특수 문자 수	Integer	8~128	8
PasswordReusePrevention	이전 암호를 다시 사용할 수 있을 때까지의 암호 순환 횟수	Integer	12~24	기본값 없음
MaxPasswordAge	암호 만료까지 남은 일수	Integer	1~90	기본값 없음

이 제어는 IAM 사용자에 대한 계정 암호 정책이 강력한 구성을 사용하는지 확인합니다. 암호 정책에서 강력한 구성을 사용하지 않으면 제어가 실패합니다. 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 위 표에 나와 있는 기본값을 사용합니다. PasswordReusePrevention 및 MaxPasswordAge 파라미터에는 기본값이 없으므로 이러한 파라미터를 제외하면 Security Hub는 이 제어를 평가할 때 암호 순환 횟수와 암호 사용 기간을 무시합니다.

IAM 사용자에게 액세스하려면 AWS Management Console암호가 필요합니다. 모범 사례로서 Security Hub에서는 IAM 사용자를 생성하는 대신 페더레이션을 사용할 것을 적극 권장합니다. 페더레이션을 통해 사용자는 기존 기업 보안 인증을 사용하여 AWS Management Console에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 를 사용하여 사용자를 생성하거나 페더레이션한 다음 계정에 IAM 역할을 맡기십시오.

ID 공급자 및 페더레이션에 대해 자세히 알아보려면 IAM 사용 설명서의 ID 공급자 및 페더레이션을 참조하십시오. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서를 참조하십시오.

IAM 사용자를 사용해야 하는 경우 Security Hub는 강력한 사용자 비밀번호를 강제로 생성할 것을 권장합니다. 에 암호 정책을 AWS 계정 설정하여 암호의 복잡성 요구 사항 및 필수 교체 기간을 지정할 수

있습니다. 비밀번호 정책을 생성 또는 변경하더라도 대부분의 비밀번호 정책 설정은 사용자가 다음에 자신의 비밀번호를 변경할 때 적용됩니다. 일부 설정은 바로 적용됩니다.

이제 Security Hub가 와 통합되었습니다

암호 정책을 업데이트하려면 IAM 사용 설명서의 IAM 사용자를 위한 계정 암호 정책 설정을 참조하세요.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/8.1.4, CIS AWS 파운데이션 벤치마크 v1.2.0/1.3, NIST.800-53.R5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.R5 AC-3 (15), NIST.800-53.R5 AC-3 (15), Nist.800-53.r5 AC-3 (15), Nist.800-53.R5 AC-3 (15), Nist.ST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `iam-user-unused-credentials-check`

스케줄 유형: 주기적

파라미터:

- `maxCredentialUsageAge`: `90`(사용자 지정할 수 없음)

이 제어는 IAM 사용자에게 90일 동안 사용되지 않은 암호 또는 활성 액세스 키가 있는지 확인합니다.

IAM 사용자는 암호 또는 액세스 키와 같은 다양한 유형의 자격 증명을 사용하여 AWS 리소스에 액세스할 수 있습니다.

Security Hub에서는 90일 이상 사용되지 않은 모든 보안 인증을 제거하거나 비활성화할 것을 권장합니다. 불필요한 보안 인증을 비활성화하거나 제거하면 침해되거나 버려진 계정과 연결된 보안 인증이 사용될 가능성이 줄어듭니다.

> **Note**
>
> AWS Config Security Hub를 사용하는 모든 지역에서 활성화되어야 합니다. 그러나 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하

는 경우 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

IAM 콘솔에서 사용자 정보를 보면 액세스 키 사용 기간, 비밀번호 사용 기간, 마지막 활동 열이 표시됩니다. 이 열 중 어느 하나라도 값이 90일보다 큰 경우 해당 사용자의 보안 인증을 비활성화하십시오.

또한 보안 인증 보고서를 사용해 사용자를 모니터링하고 90일 이상 활동이 없는 사용자를 식별할 수 있습니다. IAM 콘솔에서 `.csv` 형식으로 된 보안 인증 정보 보고서를 다운로드할 수 있습니다.

비활성 계정이나 사용하지 않는 보안 인증 정보를 식별한 후에는 비활성화하십시오. 자세한 지침은 IAM 사용 설명서의 IAM 사용자 암호 생성, 변경 또는 삭제(콘솔)를 참조하십시오.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/8.3.1, CIS 재단 벤치마크 v3.0.0/1.5, CIS AWS 재단 벤치마크 v1.4.0/1.5, CIS AWS 재단 벤치마크 v1.2.0/1.13, NIST.800-53.R5 AC-2 (1), AWS NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 (8)

범주: 보호 > 보안 액세스 관리

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: `root-account-mfa-enabled`

스케줄 유형: 주기적

파라미터: 없음

루트 사용자에게는 AWS 계정의 모든 서비스 및 리소스에 대한 완전한 액세스 권한을 갖습니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. MFA를 활성화하면 사용자가 에 로그인할 때 사용자 이름과 암호 AWS Management Console, 그리고 MFA AWS 디바이스의 인증 코드를 입력하라는 메시지가 표시됩니다.

루트 사용자에 대해 가상 MFA를 사용하는 경우 CIS에서는 개인용 디바이스를 사용하지 않는 것을 권장합니다. 대신에 모든 개인용 개별 디바이스에서 독립적으로 충전 및 보안 상태를 유지하도록 관리할 수 있는 전용 모바일 디바이스(태블릿 또는 전화)를 사용하세요. 이렇게 하면 디바이스 분실, 디바이스

거래로 인해 또는 디바이스를 소유한 개인이 회사를 그만둠으로 인해 MFA에 대한 액세스 권한을 상실할 위험이 줄어듭니다.

이제 Security Hub가 와 통합되었습니다

루트 사용자에 대해 MFA를 활성화하려면 AWS 계정 관리 참조 가이드의 AWS 계정 루트 사용자에 대한 MFA 활성화를 참조하십시오.

[IAM.10] IAM 사용자를 위한 암호 정책은 엄격한 기준을 적용해야 합니다. AWS Config

관련 요구 사항: PCI DSS v3.2.1/8.1.4, PCI DSS v3.2.1/8.2.3, PCI DSS v3.2.1/8.2.4, PCI DSS v3.2.1/8.2.5

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 IAM 사용자에 대한 계정 비밀번호 정책이 다음 최소 PCI DSS 구성을 사용하는지 확인합니다.

- `RequireUppercaseCharacters` – 암호에 대문자가 한 개 이상이어야 합니다. (기본값은 `true`)
- `RequireLowercaseCharacters` – 암호에 소문자가 한 개 이상이어야 합니다. (기본값은 `true`)
- `RequireNumbers` – 암호에 숫자가 한 개 이상이어야 합니다. (기본값은 `true`)
- `MinimumPasswordLength` – 암호 최소 길이입니다. (기본값은 7 이상)
- `PasswordReusePrevention` – 재사용을 허가받기까지 사용할 수 있는 암호 개수입니다. (기본값은 4)
- MaxPasswordAge — 비밀번호가 만료되기 전 남은 일수. (기본값은 90)

이제 Security Hub가 와 통합되었습니다

권장 구성을 사용하도록 암호 정책을 업데이트하려면 IAM 사용 설명서의 IAM 사용자에 대한 계정 비밀번호 정책 설정을 참조하십시오.

[IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/1.5

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호에 다양한 문자 집합이 사용되도록 합니다.

CIS는 비밀번호 정책에 하나 이상의 대문자를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

이제 Security Hub가 와 통합되었습니다

비밀번호 정책을 변경하려면 IAM 사용 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하십시오. 비밀번호 강도에서 라틴 알파벳(A~Z) 중 하나 이상의 대문자 요구를 선택합니다.

[IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS 재단 벤치마크 v1.2.0/1.6 AWS

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호에 다양한 문자 집합이 사용되도록 합니다. CIS에서는 비밀번호 정책에 하나 이상의 소문자를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

이제 Security Hub가 와 통합되었습니다

비밀번호 정책을 변경하려면 IAM 사용 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하십시오. 비밀번호 강도에서 라틴 알파벳(A~Z) 중 하나 이상의 소문자 요구를 선택합니다.

[IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS 재단 벤치마크 v1.2.0/1.7 AWS

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호에 다양한 문자 집합이 사용되도록 합니다.

CIS에서는 비밀번호 정책에 하나 이상의 기호를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

이제 Security Hub가 와 통합되었습니다

비밀번호 정책을 변경하려면 IAM 사용 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하십시오. 비밀번호 강도에서 하나 이상의 영숫자가 아닌 문자 요구를 선택합니다.

[IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS 재단 벤치마크 v1.2.0/1.8 AWS

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호에 다양한 문자 집합이 사용되도록 합니다.

CIS에서는 비밀번호 정책에 하나 이상의 숫자를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

이제 Security Hub가 와 통합되었습니다

비밀번호 정책을 변경하려면 IAM 사용 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하십시오. 비밀번호 강도에서 하나 이상의 숫자 요구를 선택합니다.

[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/1.8, CIS 재단 벤치마크 v1.4.0/1.8, CIS 재단 벤치마크 v1.2.0/1.9 AWS AWS

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호가 지정된 길이 이상이 되도록 합니다.

CIS에서는 비밀번호 정책에 최소 14자의 비밀번호 길이를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

이제 Security Hub가 와 통합되었습니다

비밀번호 정책을 변경하려면 IAM 사용 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하십시오. 비밀번호의 최소 길이에 **14** 또는 더 큰 숫자를 입력합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/1.9, CIS AWS 재단 벤치마크 v1.4.0/1.9, CIS AWS 재단 벤치마크 v1.2.0/1.10

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 기억할 암호 수가 24개로 설정되어 있는지 확인합니다. 값이 24가 아니면 제어가 실패합니다.

IAM 비밀번호 정책은 동일한 사용자가 특정 비밀번호를 재사용하는 것을 방지할 수 있습니다.

CIS에서는 비밀번호 정책을 통해 비밀번호 재사용을 방지할 것을 권장합니다. 암호 재사용을 방지하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

이제 Security Hub가 와 통합되었습니다

비밀번호 정책을 변경하려면 IAM 사용 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하십시오. 비밀번호 재사용 방지에 **24**를 입력합니다.

[IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/1.11

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

IAM 암호 정책에서는 지정된 일수 후에 암호를 교체하거나 만료하도록 요구할 수 있습니다.

CIS는 비밀번호 정책에서 비밀번호가 90일 이내에 만료되도록 권장합니다. 비밀번호 수명을 줄이면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다. 또한 정기적으로 비밀번호를 변경하도록 하면 다음과 같은 시나리오에 도움이 됩니다.

- 비밀번호는 지식이 없어도 도용하거나 침해할 수 있습니다. 이러한 일은 시스템 침해, 소프트웨어 취약점 또는 인터넷 위협을 통해 발생합니다.
- 암호화된 트래픽이라도 특정 기업 및 정부 웹 필터 또는 프록시 서버가 가로채 기록할 수 있습니다.
- 많은 사람들은 업무, 이메일, 개인 용도로 여러 시스템에 동일한 비밀번호를 사용합니다.
- 침해된 최종 사용자 워크스테이션에는 키 입력 로거가 있을 수 있습니다.

이제 Security Hub가 와 통합되었습니다

비밀번호 정책을 변경하려면 IAM 사용 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하십시오. 비밀번호 만료 활성화에 **`90`** 또는 더 작은 숫자를 입력하십시오.

[IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/1.17, CIS 재단 벤치마크 v1.4.0/1.17, CIS 재단 벤치마크 v1.2.0/1.20 AWS AWS

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-policy-in-use`

스케줄 유형: 주기적

파라미터:

- `policyARN`: `arn:partition:iam::aws:policy/AWSSupportAccess`(사용자 지정할 수 없음)
- `policyUsageType`: `ANY`(사용자 지정할 수 없음)

AWS 사고 알림 및 대응은 물론 기술 지원 및 고객 서비스에 사용할 수 있는 지원 센터를 제공합니다.

AWS 지원을 통해 권한 있는 사용자가 인시던트를 관리할 수 있도록 IAM 역할을 생성합니다. 액세스 제어를 위한 최소 권한을 구현함으로써 IAM 역할에는 인시던트를 관리하기 위한 지원 센터 액세스를 허용하는 적절한 IAM 정책이 필요합니다. AWS Support

> **Note**
>
> AWS Config Security Hub를 사용하는 모든 지역에서 활성화되어야 합니다. 그러나 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

이 문제를 해결하려면 권한이 있는 사용자가 AWS Support 인시던트를 관리할 수 있도록 허용하는 역할을 생성합니다.

AWS Support 액세스에 사용할 역할을 만들려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. 역할 유형에서 다른 AWS 계정을 선택합니다.
4. 계정 ID에는 리소스에 대한 액세스 권한을 AWS 계정 부여하려는 AWS 계정 ID를 입력합니다.

   이 역할을 수임할 사용자 또는 그룹이 동일한 계정에 있는 경우 로컬 계정 번호를 입력합니다.

   > **Note**
   >
   > 지정된 계정의 관리자는 해당 계정의 모든 사용자에게 이 역할을 맡을 수 있는 권한을 부여할 수 있습니다. 이를 위해 관리자는 `sts:AssumeRole` 작업에 대한 권한을 부여하는 정책을 사용자나 그룹에 연결합니다. 이 정책에서 리소스는 역할 ARN이어야 합니다.

5. 다음: 권한을 선택합니다.
6. 관리형 정책 `AWSSupportAccess`를 검색합니다.
7. `AWSSupportAccess` 관리형 정책의 확인란을 선택합니다.
8. 다음: 태그를 선택합니다.
9. (선택 사항) 역할에 메타데이터를 추가하려면 태그를 키-값 쌍으로 연결합니다.

   IAM에서 태그 사용에 대한 자세한 내용을 알아보려면 IAM 사용 설명서의 IAM 사용자 및 역할 태그 지정을 참조하십시오.
10. 다음: 검토를 선택합니다.
11. 역할 이름에 역할의 이름을 입력합니다.

    역할 이름은 사용자 내에서 고유해야 합니다 AWS 계정. 이메일은 대소문자를 구분하지 않습니다.
12. (선택 사항) 역할 설명에 새 역할에 대한 설명을 입력합니다.
13. 역할을 검토한 후 역할 생성을 선택합니다.

[IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/8.3.1, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 IA-2(1), NIST.800-53.r5 IA-2(2), NIST.800-53.r5 IA-2(6), NIST.800-53.r5 IA-2(8)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `iam-user-mfa-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 IAM 사용자가 다중 인증(MFA)을 활성화했는지 여부를 확인합니다.

> **Note**
>
> AWS Config Security Hub를 사용하는 모든 지역에서 활성화되어야 합니다. 그러나 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하

는 경우 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

IAM 사용자를 위한 MFA를 추가하려면 IAM 사용 설명서의 AWS사용자를 위한 MFA 디바이스 활성화를 참조하십시오.

[IAM.20] 루트 사용자의 사용을 피합니다.

Important

Security Hub는 2024년 4월에 이 제어를 폐기했습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: CIS AWS 재단 벤치마크 v1.2.0/1.1

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `use-of-root-account-test` (사용자 지정 Security Hub 규칙)

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 루트 사용자의 사용에 AWS 계정 제한이 있는지 여부를 확인합니다. 이 제어는 다음 리소스를 평가합니다.

- Amazon Simple Notification Service(SNS) 주제
- AWS CloudTrail 트레일
- 트레일과 관련된 메트릭 필터 CloudTrail
- 필터 기반 Amazon CloudWatch 알람

다음 문 중 하나 이상이 참인 경우 이 검사는 FAILED 결과가 됩니다.

- 계정에는 CloudTrail 트레일이 없습니다.
- CloudTrail 트레일이 활성화되었지만 읽기 및 쓰기 관리 이벤트가 포함된 멀티 리전 트레일이 하나 이상 포함되도록 구성되지는 않았습니다.
- CloudTrail 트레일은 활성화되지만 로그 CloudWatch 로그 그룹과 연결되지는 않습니다.
- CIS(인터넷 보안 센터)에서 규정한 정확한 지표 필터는 사용되지 않습니다. 규정된 지표 필터는 `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`입니다.
- 계정에는 지표 필터를 기반으로 하는 CloudWatch 경보가 없습니다.
- CloudWatch 관련 SNS 주제에 알림을 보내도록 구성된 경보는 경보 조건에 따라 트리거되지 않습니다.
- SNS 주제는 SNS 주제에 메시지를 전송하기 위한 제약 조건을 준수하지 않습니다.
- SNS 주제에 구독자가 한 명 이상 없습니다.

다음 문 중 하나 이상이 참인 경우 이 검사를 통해 제어 상태는 NO_DATA이 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub는 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub는 추적을 소유한 계정에 대한 조사 결과만 생성할 수 있습니다.

다음 문 중 하나 이상이 참인 경우 이 검사를 통해 제어 상태는 WARNING이 됩니다.

- 현재 계정은 경보에서 참조된 SNS 주제를 소유하지 않습니다. CloudWatch
- 현재 계정은 `ListSubscriptionsByTopic` SNS API 호출 시 해당 SNS 주제에 접근할 수 없습니다.

> **Note**
>
> 조직 추적을 사용하여 조직 내 여러 계정의 이벤트를 기록하는 것이 좋습니다. 조직 트레일은 기본적으로 다중 지역 트레일이며 AWS Organizations 관리 계정 또는 위임된 관리자 계정으로만 관리할 수 있습니다. CloudTrail 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 제어 상태가 NO_DATA가 됩니다. 구성원 계정에서 Security Hub는 구성원 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성

됩니다. 크로스 리전 집계 활성화를 통해 Security Hub 위임 관리자 계정에서 이러한 조사 결과를 확인할 수 있습니다.

계정 및 서비스 관리 작업 수행에 필요한 경우에만 루트 사용자 보안 인증 정보를 사용하는 것이 가장 좋습니다. IAM 정책을 사용자가 아닌 그룹 및 역할에 직접 적용하십시오. 일상적인 사용을 위해 관리자를 설정하는 방법에 대한 지침은 IAM 사용 설명서의 첫 번째 IAM 관리자 및 그룹 생성을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

이 문제를 해결하는 단계에는 Amazon SNS 주제, CloudTrail 트레일, 지표 필터 및 지표 필터에 대한 경보 설정이 포함됩니다.

Amazon SNS 토픽을 생성하려면

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 모든 CIS 경보를 수신하는 Amazon SNS 주제를 생성합니다.

   이 주제에 대해 하나 이상의 구독자를 생성합니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하십시오.

다음으로, 모든 지역에 CloudTrail 적용되는 액티브를 설정합니다. 이렇게 하려면 the section called "[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다."의 문제 해결 절차를 따르세요.

CloudTrail 트레일에 연결하는 로그 CloudWatch 로그 그룹의 이름을 기록해 둡니다. 로그 그룹에 대한 지표 필터를 생성합니다.

마지막으로 지표 필터와 경보를 생성합니다.

지표 필터 및 경보를 생성하려면

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 로그 그룹을 선택합니다.
3. 생성한 CloudTrail 트레일과 연결된 CloudWatch 로그 로그 그룹의 확인란을 선택합니다.
4. 작업에서 지표 필터 생성을 선택합니다.
5. 패턴 정의에 대해 다음을 수행합니다.

   a. 다음 패턴을 복사하여 필터 패턴 필드에 붙여 넣습니다.

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
 $.eventType !="AwsServiceEvent"}
```

b. 다음을 선택합니다.

6. 지표 할당에서 다음 작업을 수행합니다.

   a. 필터 이름에 지표 필터의 이름을 입력합니다.

   b. 지표 네임스페이스에 **LogMetrics**를 입력합니다.

      모든 CIS 로그 지표 필터에 동일한 네임스페이스를 사용하는 경우 모든 CIS 벤치마크 지표가 함께 그룹화됩니다.

   c. 지표 이름에 지표의 이름을 입력합니다. 지표의 이름을 기억하십시오. 경보를 만들 때 지표를 선택해야 합니다.

   d. 지표 값에 **1**를 입력합니다.

   e. 다음을 선택합니다.

7. 검토 및 생성에서 새 지표 필터에 대해 제공한 정보를 확인합니다. 그런 다음 지표 필터 생성을 선택합니다.

8. 탐색 창에서 로그 그룹을 선택한 다음 지표 필터에서 생성한 필터를 선택합니다.

9. 필터 확인란을 선택합니다. 경보 생성을 선택하십시오.

10. 지표 및 조건 지정에서 다음을 수행합니다.

    a. 조건의 임계값에서 정적을 선택합니다.

    b. 경보 조건 정의에서 크거나/같음을 선택합니다.

    c. 임계값 정의에는 **1**을 입력합니다.

    d. 다음을 선택합니다.

11. 작업 구성에서 다음 작업을 수행합니다.

    a. 경보 상태 트리거에서 경보를 선택합니다.

    b. SNS 주제 선택에서 기존 SNS 주제 선택을 선택합니다.

    c. 알림 보내기에 이전 절차에서 생성한 SNS 주제의 이름을 입력합니다.

    d. 다음을 선택합니다.

12. 이름 및 설명 추가에서 경보에 대한 이름 및 설명을 입력합니다(예: **CIS-1.1-RootAccountUsage**). 다음을 선택합니다.

13. 미리 보기 및 생성에서 경보 구성을 검토하십시오. 그런 다음 경보 생성을 선택합니다.

[IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(10), NIST.800-53.r5 AC-6(2), NIST.800-53.r5 AC-6(3)

범주: 감지 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::IAM::Policy`

AWS Config 규칙: `iam-policy-no-statements-with-full-access`

스케줄 유형: 변경이 트리거됨

파라미터:

- `excludePermissionBoundaryPolicy`: `True`(사용자 지정할 수 없음)

이 제어는 생성한 IAM 자격 증명 기반 정책에 * 와일드카드를 사용하여 모든 서비스의 모든 작업에 대한 권한을 부여하는 Allow 문이 있는지 확인합니다. 정책 문에 `"Effect": "Allow"`과 `"Action": "Service:*"`가 포함된 경우 제어가 실패합니다.

예를 들어 정책의 다음 문으로 인해 결과가 실패합니다.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

`"Effect": "Allow"`와 `"NotAction": "service:*"`를 함께 사용하는 경우에도 제어가 실패합니다. 이 경우 `NotAction` 요소는 에서 지정한 작업을 제외한 모든 작업에 대한 액세스를 제공합니다`NotAction`. AWS 서비스

이 제어는 고객 관리형 IAM 정책에만 적용됩니다. AWS에서 관리하는 IAM 정책에는 적용되지 않습니다.

에 권한을 할당할 AWS 서비스때는 IAM 정책에서 허용된 IAM 작업의 범위를 정하는 것이 중요합니다. IAM 작업은 필요한 작업으로만 제한해야 합니다. 이렇게 하면 최소 권한 권한을 프로비저닝할 수 있습니다. 권한이 과도하게 부여된 정책은 권한이 필요하지 않은 IAM 보안 주체에 정책이 연결된 경우 권한 상승으로 이어질 수 있습니다.

경우에 따라 `DescribeFlowLogs` 및 `DescribeAvailabilityZones`와 같이 접두사가 비슷한 IAM 작업을 허용할 수 있습니다. 이러한 승인된 경우에는 접미사가 붙은 와일드카드를 일반 접두사에 추가할 수 있습니다. 예를 들어 `ec2:Describe*`입니다.

접두사가 붙은 와일드카드와 함께 접두사가 붙은 IAM 작업을 사용하면 이 제어가 통과됩니다. 예를 들어, 정책의 다음 문은 결과 통과로 이어집니다.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

이러한 방식으로 관련 IAM 작업을 그룹화하면 IAM 정책 크기 제한을 초과하는 것을 방지할 수도 있습니다.

> **Note**
>
> AWS Config Security Hub를 사용하는 모든 지역에서 활성화되어야 합니다. 그러나 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

이 문제를 해결하려면 전체 “*” 관리 권한을 허용하지 않도록 IAM 정책을 업데이트하십시오. IAM 정책 편집에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 편집을 참조하십시오.

[IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/1.12, CIS 재단 벤치마크 v1.4.0/1.12 AWS

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: **`iam-user-unused-credentials-check`**

스케줄 유형: 주기적

파라미터: 없음

이 제어는 IAM 사용자가 45일 이상 사용하지 않은 암호 또는 활성 액세스 키를 가지고 있는지 확인합니다. 이를 위해 AWS Config 규칙의 `maxCredentialUsageAge` 매개변수가 45 이상인지 확인합니다.

사용자는 암호 또는 액세스 키와 같은 다양한 유형의 자격 증명을 사용하여 AWS 리소스에 액세스할 수 있습니다.

CIS에서는 45일 이상 사용되지 않은 모든 자격 증명을 제거하거나 비활성화할 것을 권장합니다. 불필요한 보안 인증을 비활성화하거나 제거하면 침해되거나 버려진 계정과 연결된 보안 인증이 사용될 가능성이 줄어듭니다.

이 컨트롤의 AWS Config 규칙은 4시간마다만 업데이트되는 `GetCredentialReport`및 `GenerateCredentialReport`API 작업을 사용합니다. IAM 사용자 변경 내용이 이 제어에 표시되는 데 최대 4시간이 걸릴 수 있습니다.

> **Note**
>
> AWS Config Security Hub를 사용하는 모든 지역에서 활성화되어야 합니다. 그러나 단일 리전에서 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

IAM 콘솔에서 사용자 정보를 보면 액세스 키 사용 기간, 비밀번호 사용 기간, 마지막 활동 열이 표시됩니다. 이 열 중 어느 하나라도 값이 45일보다 큰 경우 해당 사용자의 보안 인증을 비활성화하십시오.

또한 보안 인증 보고서를 사용해 사용자를 모니터링하고 45일 이상 활동이 없는 사용자를 식별할 수 있습니다. IAM 콘솔에서 `.csv` 형식으로 된 보안 인증 정보 보고서를 다운로드할 수 있습니다.

비활성 계정이나 사용하지 않는 보안 인증 정보를 식별한 후에는 비활성화하십시오. 자세한 지침은 IAM 사용 설명서의 IAM 사용자 암호 생성, 변경 또는 삭제(콘솔)를 참조하십시오.

[IAM.23] IAM 액세스 분석기 분석기는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AccessAnalyzer::Analyzer`

AWS Config 규칙: `tagged-accessanalyzer-analyzer` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer)에서 관리하는 분석기에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 분석기에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 분석기에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를

추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

분석기에 태그를 추가하려면 AWS IAM 액세스 분석기 TagResourceAPI 참조를 참조하십시오.

[IAM.24] IAM 역할에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IAM::Role`

AWS Config 규칙: `tagged-iam-role` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS Identity and Access Management (IAM) 역할에 `requiredTagKeys` 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 역할에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 역할에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

IAM 역할에 태그를 추가하려면 IAM 사용 설명서의 IAM 리소스 태그 지정을 참조하십시오.

[IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `tagged-iam-user` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS Identity and Access Management (IAM) 사용자가 `requiredTagKeys` 파라미터에 정의된 특정 키가 포함된 태그를 가지고 있는지 확인합니다. 사용자에게 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 사용자에게 키 태그가 지정되지 않은 경우 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

IAM 사용자에게 태그를 추가하려면 IAM 사용 설명서의 IAM 리소스 태그 지정을 참조하십시오.

[IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.

관련 요구 사항: AWS CIS 재단 벤치마크 v3.0.0/1.19

카테고리: 식별 > 규정 준수

심각도: 중간

리소스 유형: `AWS::IAM::ServerCertificate`

AWS Config 규칙: **`iam-server-certificate-expiration-check`**

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 IAM에서 관리되는 활성 SSL/TLS 서버 인증서가 만료되었는지 여부를 확인합니다. 만료된 SSL/TLS 서버 인증서를 제거하지 않으면 제어가 실패합니다.

에서 웹 사이트 또는 애플리케이션에 대한 HTTPS 연결을 활성화하려면 SSL/TLS 서버 인증서가 AWS 필요합니다. IAM 또는 AWS Certificate Manager (ACM) 을 사용하여 서버 인증서를 저장하고 배포할 수 있습니다. ACM에서 지원하지 않는 환경에서 HTTPS 연결을 지원해야 AWS 리전 하는 경우에만 IAM을 인증서 관리자로 사용하십시오. IAM은 프라이빗 키를 안전하게 암호화하고 암호화된 버전을 IAM SSL 인증서 스토리지에 저장합니다. IAM은 모든 지역에 서버 인증서를 배포하는 것을 지원하지만 함께 사용하려면 외부 공급자로부터 인증서를 받아야 합니다. AWS ACM 인증서를 IAM에 업로드할 수 없습니다. 또한 IAM 콘솔에서는 인증서를 관리할 수 없습니다. 만료된 SSL/TLS 인증서를 제거하면 잘못된 인증서가 실수로 리소스에 배포되어 기본 애플리케이션 또는 웹 사이트의 신뢰성이 손상될 위험이 없어집니다.

이제 Security Hub가 와 통합되었습니다

IAM에서 서버 인증서를 제거하려면 IAM 사용 설명서의 IAM에서 서버 인증서 관리를 참조하십시오.

[IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess

관련 요구 사항: CIS 재단 벤치마크 v3.0.0/1.22 AWS

카테고리: 보호 > 보안 액세스 관리 > 보안 IAM 정책

심각도: 중간

리소스 유형:`AWS::IAM::Role`,, `AWS::IAM::User` `AWS::IAM::Group`

AWS Config 규칙: **`iam-policy-blacklisted-check`**

스케줄 유형: 변경이 트리거됨

파라미터:

- “Policyarns”: “arn:aws:iam: :aws:policy/, arn:aws-cn:iam: :aws:policy/, arn :iam: :aws:policy/” AWSCloudShellFullAccess AWSCloudShellFullAccess aws-us-gov AWSCloudShellFullAccess

이 컨트롤은 IAM ID (사용자, 역할 또는 그룹) 에 관리형 정책이 연결되어 있는지 확인합니다. AWS `AWSCloudShellFullAccess` IAM ID에 `AWSCloudShellFullAccess` 정책이 연결된 경우 제어가 실패합니다.

AWS CloudShell CLI 명령을 실행할 수 있는 편리한 방법을 제공합니다. AWS 서비스 AWS 관리형 정책은 사용자의 로컬 시스템과 CloudShell 환경 간에 파일 업로드 및 다운로드 기능을 허용하는 전체 액세스를 `AWSCloudShellFullAccess` CloudShell 제공합니다. CloudShell 환경 내에서 사용자는 sudo 권한을 가지며 인터넷에 액세스할 수 있습니다. 따라서 이 관리형 정책을 IAM ID에 연결하면 파일 전송 소프트웨어를 설치하고 데이터를 외부 인터넷 서버로 이동할 수 있습니다. CloudShell 최소 권한 원칙을 따르고 IAM ID에 더 좁은 권한을 추가하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

`AWSCloudShellFullAccess`정책을 IAM ID에서 분리하려면 IAM 사용 설명서의 IAM 자격 증명 권한 추가 및 제거를 참조하십시오.

[IAM.28] IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.

관련 요구 사항: CIS 재단 벤치마크 v3.0.0/1.20 AWS

카테고리: 탐지 > 탐지 서비스 > 권한 있는 사용 모니터링

심각도: 높음

리소스 유형: `AWS::AccessAnalyzer::Analzyer`

AWS Config 규칙: **`iam-external-access-analyzer-enabled`**

스케줄 유형: 주기적

파라미터: 없음

이 AWS 계정 컨트롤은 IAM 액세스 분석기 외부 액세스 분석기가 활성화되어 있는지 확인합니다. 현재 선택한 계정에 외부 액세스 분석기가 활성화되어 있지 않으면 제어가 실패합니다. AWS 리전

IAM 액세스 분석기 외부 액세스 분석기는 Amazon Simple Storage Service (Amazon S3) 버킷 또는 IAM 역할과 같이 외부 엔티티와 공유되는 조직 및 계정의 리소스를 식별하는 데 도움이 됩니다. 이렇게 하면 리소스 및 데이터에 의도하지 않은 액세스를 방지할 수 있습니다. IAM 액세스 분석기는 지역적이므로 각 지역에서 활성화해야 합니다. 외부 보안 주체와 공유되는 리소스를 식별하기 위해 액세스 분석기는 로직 기반 추론을 사용하여 사용자 환경의 리소스 기반 정책을 분석합니다. AWS 외부 액세스 분석기를 활성화하면 전체 조직 또는 계정에 대한 분석기가 만들어집니다.

이제 Security Hub가 와 통합되었습니다

특정 지역에서 외부 액세스 분석기를 활성화하려면 IAM 사용 설명서의 IAM 액세스 분석기 활성화를 참조하십시오. 리소스에 대한 액세스를 모니터링하려는 각 지역에서 분석기를 활성화해야 합니다.

AWS IoT 제어:

이러한 제어는 AWS IoT 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::SecurityProfile`

AWS Config 규칙: `tagged-iot-securityprofile` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS IoT Core 보안 프로필에 매개변수에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 보안 프로필에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 보안 프로필에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

AWS IoT Core 보안 프로필에 태그를 추가하려면 개발자 안내서의 AWS IoT 리소스 태그 지정을 참조하십시오.AWS IoT

[IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::MitigationAction`

AWS Config 규칙: `tagged-iot-mitigationaction` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS IoT Core 완화 작업에 `requiredTagKeys` 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. 완화 작업에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 완화 작업에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

AWS IoT Core 완화 조치에 태그를 추가하려면 개발자 안내서의 AWS IoT 리소스 태그 지정을 참조하십시오.AWS IoT

[IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::Dimension`

AWS Config 규칙: `tagged-iot-dimension` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS IoT Core 차원에 매개변수에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 차원에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 컨트롤이 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 차원에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

AWS IoT Core 차원에 태그를 추가하려면 개발자 안내서의 AWS IoT 리소스 태그 지정을 참조하십시오.AWS IoT

[IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::Authorizer`

AWS Config 규칙: `tagged-iot-authorizer` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS IoT Core 권한 부여자가 `requiredTagKeys` 파라미터에 정의된 특정 키를 가진 태그를 가지고 있는지 확인합니다. 권한 부여자에 태그 키가 없거나 매개변수에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 권한 부여자에게 키 태그가 지정되지 않은 경우 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

AWS IoT Core 권한 부여자에 태그를 추가하려면 개발자 안내서의 AWS IoT 리소스 태그 지정을 참조하십시오.AWS IoT

[IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::RoleAlias`

AWS Config 규칙: `tagged-iot-rolealias` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS IoT Core 역할 별칭에 매개 변수에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. 역할 별칭에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 제어

가 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 역할 별칭에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

AWS IoT Core 역할 별칭에 태그를 추가하려면 개발자 안내서의 AWS IoT 리소스 태그 지정을 참조하십시오.AWS IoT

[IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::Policy`

AWS Config 규칙: `tagged-iot-policy` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS IoT Core 정책에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 정책에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 정책에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

AWS IoT Core 정책에 태그를 추가하려면 개발자 안내서의 AWS IoT 리소스 태그 지정을 참조하십시오.AWS IoT

Amazon Kinesis 제어

이러한 제어는 Kinesis 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::Kinesis::Stream`

AWS Config 규칙: `kinesis-stream-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Kinesis Data Streams가 서버 측 암호화를 통해 저장 시 암호화되는지 확인합니다. Kinesis 스트림이 서버 측 암호화를 통해 저장 시 암호화되지 않으면 이 제어가 실패합니다.

서버 측 암호화는 Amazon Kinesis Data Streams의 기능으로, 데이터를 저장하기 전에 AWS KMS key를 사용하여 자동으로 암호화합니다. 데이터는 Kinesis 스트림 스토리지 계층에 기록되기 전에 암호화되고, 스토리지에서 검색된 후에는 해독됩니다. 결과적으로 데이터는 Amazon Kinesis Data Streams 서비스 내에서 암호화됩니다.

이제 Security Hub가 와 통합되었습니다

Kinesis 스트림의 서버 측 암호화를 활성화에 대한 자세한 내용은 Amazon Kinesis 개발자 안내서의 서버 측 암호화를 시작하려면 어떻게 해야 합니까?를 참조하십시오.

[Kinesis.2] Kinesis 스트림에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Kinesis::Stream`

AWS Config규칙: `tagged-kinesis-stream` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon Kinesis 데이터 스트림에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 데이터 스트림에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 데이터 스트림에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Kinesis 데이터 스트림에 태그를 추가하려면 Amazon Kinesis 개발자 안내서의 Amazon Kinesis 데이터 스트림에서 스트림에 태그 지정을 참조하십시오.

AWS Key Management Service 컨트롤:

이러한 컨트롤은 AWS KMS 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(3)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::Policy`

AWS Config 규칙: `iam-customer-policy-blocked-kms-actions`

스케줄 유형: 변경이 트리거됨

파라미터:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(사용자 지정할 수 없음)
- `excludePermissionBoundaryPolicy`: `True`(사용자 지정할 수 없음)

IAM 고객 관리형 정책의 기본 버전에서 보안 주체가 모든 리소스에 대한 AWS KMS 암호 해독 작업을 사용할 수 있도록 허용하는지 확인합니다. 모든 KMS 키에 대해 `kms:Decrypt` 또는 `kms:ReEncryptFrom` 작업을 허용할 만큼 정책이 공개되어 있으면 제어가 실패합니다.

제어는 리소스 요소의 KMS 키만 검사하고 정책의 조건 요소에 있는 조건은 고려하지 않습니다. 또한 제어는 연결된 고객 관리형 정책과 연결되지 않은 고객 관리형 정책을 모두 평가합니다. 인라인 정책이나 관리형 정책은 확인하지 않습니다. AWS

를 사용하면 KMS 키를 사용하고 암호화된 데이터에 액세스할 수 있는 사용자를 제어할 수 있습니다. AWS KMS IAM 정책은 자격 증명(사용자, 그룹 또는 역할)이 어떤 리소스에 대해 어떤 작업을 수행할 수 있는지 정의합니다. 보안 모범 사례에 따라 최소 권한을 허용할 AWS 것을 권장합니다. 즉, ID에

kms:Decrypt 또는 kms:ReEncryptFrom 권한만 부여하고 작업을 수행하는 데 필요한 키에 대해서만 부여해야 합니다. 그렇지 않으면 사용자가 데이터에 적합하지 않은 키를 사용할 수 있습니다.

모든 키에 대한 권한을 부여하는 대신 사용자가 암호화된 데이터에 액세스하는 데 필요한 최소 키 세트를 결정합니다. 그런 다음 사용자가 해당 키만 사용하도록 허용하는 정책을 설계합니다. 예를 들어 모든 KMS 키에 대한 kms:Decrypt 권한을 허용하지 마십시오. 대신 계정의 특정 리전에 있는 키에만 kms:Decrypt를 허용하십시오. 최소 권한 원칙을 채택하면 데이터가 의도하지 않게 공개될 위험을 줄일 수 있습니다.

이제 Security Hub가 와 통합되었습니다

IAM 고객 관리형 정책을 수정하려면 IAM 사용 설명서의 고객 관리형 정책 편집을 참조하십시오. 정책을 편집할 때 암호 해독 작업을 허용하려는 특정 키의 Amazon 리소스 이름(ARN)을 Resource 필드에 제공합니다.

[KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(3)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형:

- AWS::IAM::Group
- AWS::IAM::Role
- AWS::IAM::User

AWS Config 규칙: iam-inline-policy-blocked-kms-actions

스케줄 유형: 변경이 트리거됨

파라미터:

- blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt(사용자 지정할 수 없음)

이 컨트롤은 IAM ID (역할, 사용자 또는 그룹) 에 내장된 인라인 정책이 모든 KMS 키에 대한 AWS KMS 암호 해독 및 재암호화 작업을 허용하는지 여부를 확인합니다. 모든 KMS 키에 대해 `kms:Decrypt` 또는 `kms:ReEncryptFrom` 작업을 허용할 만큼 정책이 공개되어 있으면 제어가 실패합니다.

제어는 리소스 요소의 KMS 키만 검사하고 정책의 조건 요소에 있는 조건은 고려하지 않습니다.

를 AWS KMS사용하면 KMS 키를 사용하고 암호화된 데이터에 액세스할 수 있는 사용자를 제어할 수 있습니다. IAM 정책은 자격 증명(사용자, 그룹 또는 역할)이 어떤 리소스에 대해 어떤 작업을 수행할 수 있는지 정의합니다. 보안 모범 사례에 따라 최소 권한을 허용할 AWS 것을 권장합니다. 즉, 필요한 권한과 작업을 수행하는 데 필요한 키만 ID에 부여해야 합니다. 그렇지 않으면 사용자가 데이터에 적합하지 않은 키를 사용할 수 있습니다.

모든 키에 권한을 부여하는 대신 사용자가 암호화된 데이터에 액세스하는 데 필요한 최소 키 세트를 결정하십시오. 그런 다음 사용자가 해당 키만 사용하도록 허용하는 정책을 설계합니다. 예를 들어 모든 KMS 키에 대한 `kms:Decrypt` 권한을 허용하지 마십시오. 대신 계정에 대한 특정 리전의 특정 키에 대해서만 권한을 허용하십시오. 최소 권한 원칙을 채택하면 데이터가 의도하지 않게 공개될 위험을 줄일 수 있습니다.

이제 Security Hub가 와 통합되었습니다

IAM 인라인 정책을 수정하려면 IAM 사용 설명서의 인라인 정책 편집을 참조하십시오. 정책을 편집할 때 암호 해독 작업을 허용하려는 특정 키의 Amazon 리소스 이름(ARN)을 `Resource` 필드에 제공합니다.

[KMS.3] 을 (를) 실수로 AWS KMS keys 삭제해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12(2)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 심각

리소스 유형: `AWS::KMS::Key`

AWS Config 규칙: `kms-cmk-not-scheduled-for-deletion-2` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 KMS 키가 삭제되도록 예약되어 있는지 여부를 확인합니다. KMS 키 삭제가 예약된 경우 제어가 실패합니다.

KMS 키는 일단 삭제되면 복구할 수 없습니다. KMS 키를 삭제하면 KMS 키로 암호화된 데이터도 영구적으로 복구할 수 없습니다. 삭제될 예정인 KMS 키로 의미 있는 데이터를 암호화한 경우, 의도적으로 암호화 삭제를 수행하지 않는 한 데이터를 해독하거나 새 KMS 키로 데이터를 다시 암호화하는 것을 고려해 보십시오.

KMS 키 삭제가 예약되면 오류로 예약된 경우 삭제를 되돌릴 수 있는 시간을 확보하기 위해 필수 대기 기간이 적용됩니다. 기본 대기 기간은 30일이지만 KMS 키 삭제가 예정된 경우 짧게는 7일로 줄일 수 있습니다. 대기 기간 동안에는 예약된 삭제를 취소할 수 있으며 KMS 키는 삭제되지 않습니다.

KMS 키 삭제에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 KMS 키 삭제를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

예약된 KMS 키 삭제를 취소하려면 AWS Key Management Service 개발자 안내서의 키 삭제 예약 및 취소(콘솔) 아래의 키 삭제를 취소하려면을 참조하십시오.

[KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS

관련 요구 사항: PCI DSS v3.2.1/3.6.4, CIS 재단 벤치마크 v3.0.0/3.6, CIS AWS 재단 벤치마크 v1.4.0/3.8, CIS AWS 재단 벤치마크 v1.2.0/2.8, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2), AWS NIST.800-53.r5 SC-28 (3)

범주: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::KMS::Key`

AWS Config 규칙: `cmk-backing-key-rotation-enabled`

스케줄 유형: 주기적

파라미터: 없음

AWS KMS 고객이 KMS 키의 키 ID에 저장되고 KMS 키의 키 ID에 AWS KMS 연결되는 키 자료인 백킹 키를 교체할 수 있습니다. 이 백업 키는 암호화, 해독 등 암호화 작업을 수행하는 데 사용됩니다. 자동화

된 키 교체는 암호화된 데이터의 해독이 투명하게 이루어질 수 있도록 하기 위해 현재 모든 이전 버전의 백업 키를 유지합니다.

CIS에서는 KMS 키 순환을 활성화할 것을 권장합니다. 암호화 키를 교체하면 노출되었을 수 있는 이전 키로 새로운 키로는 암호화된 데이터에 액세스할 수 없으므로 침해된 키가 영향을 미칠 가능성을 줄일 수 있습니다.

이제 Security Hub가 와 통합되었습니다

KMS 키 교체를 활성화하려면 AWS Key Management Service 개발자 안내서의 자동 키 교체를 활성화 및 비활성화하는 방법을 참조하십시오.

AWS Lambda 제어:

이러한 제어는 Lambda 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다. AWS 리전자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: `lambda-function-public-access-prohibited`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Lambda 함수 리소스 기반 정책이 계정 외부의 퍼블릭 액세스를 금지하는지 여부를 확인합니다. 퍼블릭 액세스가 허용되면 제어가 실패합니다. Amazon S3에서 Lambda 함수를 호출하고 정책

에 AWS:SourceAccount와 같이 퍼블릭 액세스를 제한하는 조건이 포함되어 있지 않은 경우에도 제어가 실패합니다. 액세스를 더 세분화하려면 버킷 정책에 AWS:SourceAccount와 다른 S3 조건을 함께 사용하는 것이 좋습니다.

Lambda 함수는 의도하지 않은 함수 코드에 접근할 수 있으므로 공개적으로 액세스할 수 없어야 합니다.

이제 Security Hub가 와 통합되었습니다

이 문제를 해결하려면 함수의 리소스 기반 정책을 업데이트하여 권한을 제거하거나 AWS:SourceAccount 조건을 추가해야 합니다. Lambda API 또는 에서만 리소스 기반 정책을 업데이트할 수 있습니다. AWS CLI

시작하려면 Lambda 콘솔에서 리소스 기반 정책을 검토하십시오. 정책을 공개하는 Principal 필드 값(예: "*" 또는 { "AWS": "*" })이 포함된 정책문을 식별하십시오.

콘솔에서는 정책을 편집할 수 없습니다. 함수에서 권한을 제거하려면 AWS CLI에서 remove-permission 명령을 실행합니다.

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

*<function-name>*을 Lambda 함수 이름으로 바꾸고, *<statement-id>*을 제거하려는 문의 문 ID(Sid)로 대체하십시오.

[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

범주: 보호 > 보안 개발

심각도: 중간

리소스 유형: AWS::Lambda::Function

AWS Config 규칙: lambda-function-settings-check

스케줄 유형: 변경이 트리거됨

파라미터:

- `runtime: dotnet8, dotnet6, java21, java17, java11, java8.al2, nodejs20.x, nodejs18.x, nodejs16.x, python3.12, python3.11, python3.10, python3.9, python3.8, ruby3.3, ruby3.2`(사용자 지정할 수 없음)

이 컨트롤은 AWS Lambda 함수 런타임 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. Lambda 함수가 이전 파라미터에서 언급한 지원되는 런타임을 사용하지 않으면 제어가 실패합니다. Security Hub는 패키지 유형이 `Image` 인 함수를 무시합니다.

Lambda 런타임은 유지 관리 및 보안 업데이트가 적용되는 운영 체제, 프로그래밍 언어, 소프트웨어 라이브러리의 조합을 기반으로 구축됩니다. 보안 업데이트를 위해 런타임 구성 요소가 더 이상 지원되지 않으면 Lambda는 런타임을 더 이상 사용하지 않습니다. 더 이상 사용되지 않는 런타임을 사용하는 함수를 만들 수는 없지만 함수를 사용하여 호출 이벤트를 처리할 수는 있습니다. Lambda 함수를 최신으로 유지하고 더 이상 사용되지 않는 런타임 환경을 사용하지 않는 것이 좋습니다. 지원되는 런타임 목록은 개발자 안내서의 Lambda 런타임을 참조하십시오.AWS Lambda

이제 Security Hub가 와 통합되었습니다

지원되는 런타임 및 지원 중단 일정에 대한 자세한 내용은 AWS Lambda 개발자 안내서의 런타임 지원 중단 정책을 참조하십시오. 런타임을 최신 버전으로 마이그레이션할 때는 해당 언어 게시자의 구문과 지침을 따르세요. 또한 런타임 버전 비호환성이 드물게 발생하는 경우 워크로드에 영향을 미칠 위험을 줄일 수 있도록 런타임 업데이트를 적용하는 것이 좋습니다.

[Lambda.3] Lambda 함수는 VPC에 있어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: **`lambda-inside-vpc`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Lambda 함수가 가상 사설 클라우드 (VPC) 에 배포되었는지 여부를 확인합니다. Lambda 함수가 VPC에 배포되지 않은 경우 제어가 실패합니다. Security Hub는 VPC 서브넷 라우팅 구성을 평가하여 퍼블릭 연결 가능성을 결정하지 않습니다. Lambda@Edge 리소스에 대해 실패한 조사 결과가 표시될 수 있습니다.

VPC에 리소스를 배포하면 네트워크 구성에 대한 보안 및 제어가 강화됩니다. 또한 이러한 배포는 여러 가용 영역에 걸쳐 확장성과 높은 내결함성을 제공합니다. 다양한 애플리케이션 요구 사항을 충족하도록 VPC 배포를 사용자 지정할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

VPC의 프라이빗 서브넷에 연결하도록 기존 함수를 구성하려면 AWS Lambda 개발자 안내서의 VPC 액세스 구성을 참조하십시오. 고가용성을 위해 최소 두 개의 프라이빗 서브넷을 선택하고 함수의 연결 요구 사항을 충족하는 보안 그룹을 하나 이상 선택하는 것이 좋습니다.

[Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: `lambda-vpc-multi-az-check`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`availabilityZones`	최소 가용 영역의 수	Enum	`2, 3, 4, 5, 6`	`2`

이 컨트롤은 가상 사설 클라우드 (VPC) 에 연결하는 AWS Lambda 함수가 최소한 지정된 수의 가용 영역 (AZ) 에서 작동하는지 확인합니다. 함수가 최소한 지정된 수의 AZ에서 작동하지 않으면 제어가 실

패합니다. 최소 AZ 수에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 두 AZ를 사용합니다.

아키텍처 내에서 고가용성을 보장하기 위한 AWS 모범 사례는 여러 AZ에 리소스를 배포하는 것입니다. 가용성은 기밀성, 무결성, 가용성 3중 보안 모델의 핵심 요소입니다. VPC에 연결하는 모든 Lambda 함수는 단일 장애 영역으로 인해 운영이 완전히 중단되지 않도록 다중 AZ 배포를 포함해야 합니다.

이제 Security Hub가 와 통합되었습니다

계정의 VPC에 연결하도록 함수를 구성하는 경우 고가용성을 보장하기 위해 여러 AZ에 서브넷을 지정합니다. 지침은 AWS Lambda 개발자 안내서의 VPC 액세스 구성을 참조하십시오.

Lambda는 단일 영역에서 서비스 중단이 발생할 경우 이벤트를 처리할 수 있도록 여러 AZ에서 다른 함수를 자동으로 실행합니다.

[Lambda.6] Lambda 함수는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: `tagged-lambda-function` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS Lambda 함수에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 함수에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 컨트롤이

requiredTagKeys 실패합니다. 매개 변수를 requiredTagKeys 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 함수에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 aws: 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Lambda 함수에 태그를 추가하려면 개발자 안내서의 Lambda 함수에서 태그 사용을 참조하십시오.AWS Lambda

Amazon Macie 제어

이러한 제어는 Macie 리소스와 관련이 있습니다.

이러한 제어 기능을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Macie.1] Amazon Macie를 활성화해야 합니다

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8(19), NIST.800-53.r5 SI-4

범주: 감지 > 감지 서비스

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `macie-status-check`

스케줄 유형: 주기적

이 제어는 계정에 Amazon Macie가 활성화되어 있는지 확인합니다. 계정에 Macie가 활성화되어 있지 않으면 제어가 실패합니다.

Amazon Macie는 기계 학습과 패턴 일치를 사용하여 민감한 데이터를 검색하고, 데이터 보안 위험에 대한 가시성을 제공하며, 이러한 위험에 대한 자동 보호를 지원합니다. Macie는 Amazon Simple Storage Service(S3) 버킷의 보안 및 액세스 제어를 자동으로 지속적으로 평가하고, 결과를 생성하여 Amazon S3 데이터의 보안 또는 프라이버시와 관련된 잠재적인 문제를 알려줍니다. 또한 Macie는 개인 식별 정보(PII)와 같은 민감한 데이터의 검색 및 보고를 자동화하여 Amazon S3에 저장하는 데이터를 더 잘 이해할 수 있도록 합니다. 자세한 내용은 Amazon Macie 사용 설명서를 참조하세요.

이제 Security Hub가 와 통합되었습니다

Macie를 활성화하려면 Amazon Macie 사용 설명서의 Macie 활성화를 참조하세요.

[Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8(19), NIST.800-53.r5 SI-4

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `macie-auto-sensitive-data-discovery-check`

스케줄 유형: 주기적

이 컨트롤은 Amazon Macie 관리자 계정에 대해 민감한 데이터 자동 검색이 활성화되어 있는지 여부를 확인합니다. Macie 관리자 계정에서 민감한 데이터 자동 검색을 활성화하지 않으면 제어가 실패합니다. 이 제어는 관리자 계정에만 적용됩니다.

Macie는 Amazon Simple Storage Service (Amazon S3) 버킷에서 개인 식별 정보 (PII) 와 같은 민감한 데이터를 자동으로 검색하고 보고합니다. Macie는 자동화된 민감한 데이터 검색을 통해 버킷 인벤토리를 지속적으로 평가하고 샘플링 기법을 사용하여 버킷에서 대표적인 S3 객체를 식별하고 선택합니다.

그런 다음 Macie는 선택한 객체를 분석하여 민감한 데이터가 있는지 검사합니다. 분석이 진행됨에 따라 Macie는 S3 데이터에 대해 제공하는 통계, 인벤토리 데이터 및 기타 정보를 업데이트합니다. 또한 Macie는 발견한 민감한 데이터를 보고하기 위해 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

S3 버킷의 객체를 분석하기 위한 자동 민감 데이터 검색 작업을 생성 및 구성하려면 Amazon Macie 사용 설명서의 계정에 대한 자동 민감 데이터 검색 구성을 참조하십시오.

Amazon MSK 제어

이러한 제어는 Amazon Managed Streaming for Apache Kafka(Amazon MSK) 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::MSK::Cluster`

AWS Config 규칙: `msk-in-cluster-node-require-tls`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MSK 클러스터가 클러스터의 브로커 노드 간에 전송 중에 HTTPS (TLS) 로 암호화되었는지 여부를 확인합니다. 클러스터 브로커 노드 연결에 일반 텍스트 통신이 활성화된 경우 제어가 실패합니다.

HTTPS는 TLS를 사용하여 데이터를 이동하므로 추가 보안 계층을 제공하며, 이를 통해 잠재적 공격자가 네트워크 트래픽을 도청하거나 조작하기 위한 공격 person-in-the-middle 또는 이와 유사한 공격을

사용하지 못하도록 방지할 수 있습니다. 기본적으로 Amazon MSK는 TLS를 사용하여 전송 중 데이터를 암호화합니다. 그러나 클러스터를 생성할 때 이 기본값을 재정의할 수 있습니다. 브로커 노드 연결에는 HTTPS(TLS)를 통한 암호화된 연결을 사용하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

MSK 클러스터의 암호화 설정을 업데이트하려면 Amazon Managed Streaming for Apache Kafka(Amazon MSK) 개발자 안내서의 클러스터 보안 설정 업데이트를 참조하세요.

[MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::MSK::Cluster`

AWS Config 규칙: `msk-enhanced-monitoring-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MSK 클러스터에 `PER_TOPIC_PER_BROKER` 이상의 모니터링 수준으로 지정된 향상된 모니터링이 구성되어 있는지 확인합니다. 클러스터의 모니터링 수준이 `DEFAULT` 또는 `PER_BROKER`로 설정된 경우 제어가 실패합니다.

`PER_TOPIC_PER_BROKER` 모니터링 수준은 MSK 클러스터의 성능에 대한 보다 세밀한 통찰력을 제공하고 CPU 및 메모리 사용량 등 리소스 사용률과 관련된 지표도 제공합니다. 이를 통해 개별 주제 및 브로커의 성능 병목 현상과 리소스 사용 패턴을 식별할 수 있습니다. 이러한 가시성을 통해 결국 Kafka 브로커의 성능을 최적화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

MSK 클러스터에 대한 향상된 모니터링을 구성하려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/msk/home?region=us-east-1#/home/에서 Amazon MSK 콘솔을 엽니다.

2. 탐색 창에서 클러스터를 선택합니다. 그런 다음 클러스터를 선택합니다.
3. 작업에서 모니터링 편집을 선택합니다.
4. 향상된 주제 수준 모니터링 옵션을 선택합니다.
5. 변경 사항 저장을 선택합니다.

모니터링 수준에 대한 자세한 내용은 Amazon Managed Streaming for Apache Kafka 개발자 안내서에서 클러스터의 보안 설정 업데이트를 참조하세요.

Amazon MQ 제어

이러한 제어는 Amazon MQ 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch

관련 요구 사항: NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.r5 AU-12, NIST.800-53.R5 SI-4

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::AmazonMQ::Broker`

AWS Config 규칙: `mq-cloudwatch-audit-log-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon MQ ActiveMQ 브로커가 감사 로그를 Amazon Logs로 스트리밍하는지 여부를 확인합니다. CloudWatch 브로커가 감사 로그를 Logs로 스트리밍하지 않으면 제어가 실패합니다. CloudWatch

ActiveMQ 브로커 로그를 CloudWatch Logs에 게시하면 보안 관련 정보의 가시성을 높이는 경보 및 지표를 CloudWatch 생성할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

ActiveMQ 브로커 로그를 CloudWatch 로그로 스트리밍하려면 Amazon MQ 개발자 안내서의 ActiveMQ 로그를 위한 Amazon MQ 구성을 참조하십시오.

[MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.

관련 요구 사항: NIST.800-53.R5 CM-3, NIST.800-53.R5 SI-2

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 낮음

리소스 유형: `AWS::AmazonMQ::Broker`

AWS Config 규칙: `mq-auto-minor-version-upgrade-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon MQ 브로커에 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. 브로커가 자동 마이너 버전 업그레이드를 활성화하지 않은 경우 제어가 실패합니다.

Amazon MQ는 새 브로커 엔진 버전을 릴리스하고 지원하기 때문에 변경 사항은 기존 애플리케이션과 이전 버전과 호환되며 기존 기능을 더 이상 사용하지 않습니다. 자동 브로커 엔진 버전 업데이트는 보안 위험으로부터 보호하고, 버그를 수정하고, 기능을 개선하는 데 도움이 됩니다.

> **Note**
>
> 자동 마이너 버전 업그레이드와 관련된 브로커가 최신 패치를 사용하고 있는데 지원되지 않게 되면 수동 조치를 취하여 업그레이드해야 합니다.

이제 Security Hub가 와 통합되었습니다

MQ 브로커의 자동 마이너 버전 업그레이드를 활성화하려면 Amazon MQ 개발자 안내서의 마이너 엔진 버전 자동 업그레이드를 참조하십시오.

[MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AmazonMQ::Broker`

AWS Config 규칙: `tagged-amazonmq-broker` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon MQ 브로커에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 브로커에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 브로커에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Amazon MQ 브로커에 태그를 추가하려면 Amazon MQ 개발자 안내서의 리소스 태그 지정을 참조하십시오.

[MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 낮음

리소스 유형: `AWS::AmazonMQ::Broker`

AWS Config 규칙: `mq-active-deployment-mode`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MQ ActiveMQ 브로커의 배포 모드가 활성/대기로 설정되어 있는지 확인합니다. 단일 인스턴스 브로커(기본적으로 활성화됨)를 배포 모드로 설정하면 제어가 실패합니다.

활성/대기 배포는 AWS 리전에서 Amazon MQ ActiveMQ 브로커에 대한 고가용성을 제공합니다. 활성/대기 배포 모드에는 중복 쌍으로 구성된 두 개의 서로 다른 가용 영역에 있는 두 개의 브로커 인스턴스가 포함됩니다. 이러한 브로커는 애플리케이션과 동기적으로 통신하므로 장애 발생 시 가동 중지 시간과 데이터 손실을 줄일 수 있습니다.

이제 Security Hub가 와 통합되었습니다

활성/대기 배포 모드로 새 ActiveMQ 브로커를 생성하려면 Amazon MQ 개발자 안내서의 ActiveMQ 브로커 생성 및 구성을 참조하십시오. 배포 모드에서 활성/대기 브로커를 선택합니다. 기존 브로커의 배포 모드는 변경할 수 없습니다. 대신 새 브로커를 생성하고 이전 브로커의 설정을 복사해야 합니다.

[MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5

범주: 복구 > 복원력 > 고가용성

심각도: 낮음

리소스 유형: `AWS::AmazonMQ::Broker`

AWS Config 규칙: `mq-rabbit-deployment-mode`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MQ RabbitMQ 브로커의 배포 모드가 클러스터 배포로 설정되었는지 여부를 확인합니다. 단일 인스턴스 브로커(기본적으로 활성화됨)를 배포 모드로 설정하면 제어가 실패합니다.

클러스터 배포는 AWS 리전에서 Amazon MQ RabbitMQ 브로커에 대한 고가용성을 제공합니다. 클러스터 배포는 각각 자체 Amazon Elastic Block Store(Amazon EBS) 볼륨과 공유 상태를 갖는 세 개의 RabbitMQ 브로커 노드로 구성된 논리적 그룹입니다. 클러스터 배포를 통해 데이터가 클러스터의 모든 노드에 복제되므로 장애 발생 시 가동 중지 시간과 데이터 손실을 줄일 수 있습니다.

이제 Security Hub가 와 통합되었습니다

클러스터 배포 모드를 사용하여 새 RabbitMQ 브로커를 생성하려면 Amazon MQ 개발자 안내서의 RabbitMQ 브로커 생성 및 연결을 참조하십시오. 배포 모드에서는 클러스터 배포를 선택합니다. 기존 브로커의 배포 모드는 변경할 수 없습니다. 대신 새 브로커를 생성하고 이전 브로커의 설정을 복사해야 합니다.

Amazon Neptune 제어

이러한 제어는은 Neptune 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다. AWS 리전자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune DB 클러스터가 저장 시 암호화되어 있는지 여부를 확인합니다. Neptune DB 클러스터가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 해당 데이터의 기밀성을 보호하여 권한 없는 사용자가 해당 데이터에 액세스할 수 있는 위험을 줄일 수 있습니다. Neptune DB 클러스터를 암호화하면 데이터와 메타데이터를 무단 액세스로부터 보호할 수 있습니다. 또한 프로덕션 파일 시스템의 data-at-rest 암호화에 대한 규정 준수 요구 사항도 충족합니다.

이제 Security Hub가 와 통합되었습니다

Neptune DB 클러스터를 만들 때 저장 시 암호화를 활성화할 수 있습니다. 클러스터를 생성한 후에는 암호화 설정을 변경할 수 없습니다. 자세한 내용은 Neptune 사용 설명서의 저장 중 Neptune 리소스 암호화를 참조하십시오.

[Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 AU-7(1), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-4(5), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-cloudwatch-log-export-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Neptune DB 클러스터가 Amazon Logs에 감사 로그를 게시하는지 여부를 확인합니다. CloudWatch Neptune DB 클러스터가 감사 로그를 Logs에 게시하지 않으면 제어가 실패합니다. CloudWatch `EnableCloudWatchLogsExport`로 설정해야 합니다. `Audit`

Amazon Neptune과 CloudWatch Amazon이 통합되어 성능 지표를 수집하고 분석할 수 있습니다. Neptune은 자동으로 CloudWatch 메트릭을 전송하고 알람도 지원합니다. CloudWatch 감사 로그는 고도로 사용자 지정이 가능합니다. 데이터베이스를 감사할 때 어떤 데이터베이스 클러스터에 액세스하고 어떻게 액세스하는지에 대한 정보를 포함하여 데이터에 대한 각 작업을 모니터링하고 감사 추적에 기록할 수 있습니다. Neptune DB 클러스터를 모니터링하는 CloudWatch 데 도움이 되도록 이러한 로그를 전송하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

Neptune 감사 로그를 Logs에 CloudWatch 게시하려면 Neptune 사용 설명서의 CloudWatch Amazon Logs에 Neptune 로그 게시를 참조하십시오. 로그 내보내기 섹션에서 감사를 선택합니다.

[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::RDS::DBClusterSnapshot`

AWS Config 규칙: `neptune-cluster-snapshot-public-prohibited`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune 수동 DB 클러스터 스냅샷이 퍼블릭인지 여부를 확인합니다. Neptune 수동 DB 클러스터 스냅샷이 퍼블릭인 경우 제어가 실패합니다.

Neptune DB 클러스터 수동 스냅샷은 의도하지 않는 한 공개해서는 안 됩니다. 암호화되지 않은 수동 스냅샷을 공개로 공유하면 모든 AWS 계정에서 해당 스냅샷을 사용할 수 있습니다. 퍼블릭 스냅샷은 의도하지 않은 데이터 노출을 초래할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Neptune 수동 DB 클러스터 스냅샷에 대한 퍼블릭 액세스를 제거하려면 Neptune 사용 설명서의 DB 클러스터 스냅샷 공유를 참조하십시오.

[Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune DB 클러스터의 삭제 방지 기능 활성화 여부를 확인합니다. Neptune DB 클러스터에 삭제 방지 기능이 활성화되지 않은 경우 제어가 실패합니다.

클러스터 삭제 방지를 활성화하면 우발적인 데이터베이스 삭제 또는 권한 없는 사용자에 의한 삭제에 대한 추가 보호 계층이 제공됩니다. 삭제 방지가 활성화된 동안에는 Neptune DB 클러스터를 삭제할 수 없습니다. 삭제 요청이 성공하려면 먼저 삭제 방지를 비활성화해야 합니다.

이제 Security Hub가 와 통합되었습니다

기존 Neptune DB 클러스터에 대한 삭제 방지를 활성화하려면 Amazon Aurora 사용 설명서의 콘솔, CLI 및 API를 사용하여 DB 클러스터 수정을 참조하십시오.

[Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-12

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-backup-retention-check`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
`minimumBackupRetentionPeriod`	백업 보존 기간(일수)	Integer	7~35	7	

이 제어는 Neptune DB 클러스터에 자동 백업이 활성화되어 있고 백업 보존 기간이 지정된 기간 이상인지 확인합니다. Neptune DB 클러스터에 대한 백업이 활성화되지 않았거나 보존 기간이 지정된 기간 미만인 경우 제어가 실패합니다. 백업 보존 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 7일을 사용합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구하고 시스템의 복원력을 강화할 수 있습니다. Neptune DB 클러스터의 백업을 자동화하면 시스템을 특정 시점으로 복원하고 가동 중지 시간과 데이터 손실을 최소화할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

자동 백업을 활성화하고 Neptune DB 클러스터의 백업 보존 기간을 설정하려면 Amazon RDS 사용 설명서의 자동 백업 활성화를 참조하세요. 백업 보존 기간의 경우 7 이상의 값을 선택합니다.

[Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SC-7(18)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::RDS::DBClusterSnapshot`

AWS Config 규칙: `neptune-cluster-snapshot-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune DB 클러스터 스냅샷이 저장 시 암호화되었는지 여부를 확인합니다. Neptune DB 클러스터가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 이러한 데이터의 기밀을 보호하여 권한이 없는 사용자가 데이터에 액세스할 위험을 줄일 수 있습니다. Neptune DB 클러스터 스냅샷의 데이터는 추가 보안 계층을 위해 저장 시 암호화되어야 합니다.

이제 Security Hub가 와 통합되었습니다

기존 Neptune DB 클러스터 스냅샷은 암호화할 수 없습니다. 대신 스냅샷을 새 DB 클러스터에 복원하고 클러스터에서 암호화를 활성화해야 합니다. 암호화된 클러스터에서 암호화된 스냅샷을 생성할 수 있습니다. 지침은 Neptune 사용 설명서의 DB 클러스터 스냅샷에서 복원 및 Neptune에서 DB 클러스터 스냅샷 생성을 참조하십시오.

[Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-iam-database-authentication`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune DB 클러스터에 IAM 데이터베이스 인증이 활성화되어 있는지 확인합니다. Neptune DB 클러스터에 대해 IAM 데이터베이스 인증이 활성화되지 않은 경우 제어가 실패합니다.

Amazon Neptune 데이터베이스 클러스터에 대한 IAM 데이터베이스 인증을 사용하면 인증을 IAM을 사용해 외부에서 관리하기 때문에 데이터베이스 구성 내에 사용자 보안 인증을 저장할 필요가 없습니다. IAM 데이터베이스 인증이 활성화되면 AWS 서명 버전 4를 사용하여 각 요청에 서명해야 합니다.

이제 Security Hub가 와 통합되었습니다

기본적으로 Neptune DB 클러스터를 생성하면 IAM 데이터베이스 인증이 비활성화됩니다. 이를 활성화하려면 Neptune 사용 설명서의 Neptune에서 IAM 데이터베이스 인증 활성화를 참조하십시오.

[Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-copy-tags-to-snapshot-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 스냅샷이 생성될 때 Neptune DB 클러스터가 모든 태그를 스냅샷에 복사하도록 구성되어 있는지 확인합니다. Neptune DB 클러스터가 태그를 스냅샷에 복사하도록 구성되지 않은 경우 제어가 실패합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 상위 Amazon RDS 데이터베이스 클러스터와 동일한 방식으로 스냅샷에 태그를 지정해야 합니다. 태그를 복사하면 DB 스냅샷의 메타데이터가 상위 데이터베이스 클러스터의 메타데이터와 일치하고, DB 스냅샷의 액세스 정책도 상위 DB 인스턴스의 액세스 정책과 일치하게 됩니다.

이제 Security Hub가 와 통합되었습니다

Neptune DB 클러스터의 스냅샷에 태그를 복사하려면 Neptune 사용 설명서의 Neptune에서 태그 복사를 참조하세요.

[Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-multi-az-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Neptune DB 클러스터의 여러 가용 영역(AZ)에 읽기 전용 복제본 인스턴스가 있는지 확인합니다. 클러스터를 하나의 AZ에만 배포하면 제어가 실패합니다.

AZ를 사용할 수 없고 정기적인 유지 관리 이벤트가 발생하는 경우 읽기 전용 복제본은 기본 인스턴스의 장애 조치 대상 역할을 합니다. 즉, 기본 인스턴스에 장애가 발생하면 Neptune은 읽기 전용 복제본 인스턴스를 기본 인스턴스로 승격합니다. 반대로 DB 클러스터에 읽기 전용 복제본 인스턴스가 포함되어 있지 않으면 기본 인스턴스에 장애가 발생해도 DB 클러스터를 다시 만들 때까지 사용할 수 없습니다. 기본 인스턴스를 다시 만드는 것은 읽기 전용 복제본을 승격하는 것보다 훨씬 더 오래 걸립니다. 고가용성을 보장하려면 기본 인스턴스와 동일한 DB 인스턴스 클래스를 갖고 기본 인스턴스와는 다른 AZ에 위치한 하나 이상의 읽기 전용 복제본 인스턴스를 생성하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

여러 AZ에 Neptune DB 클러스터를 배포하려면 Neptune 사용 설명서의 Neptune DB 클러스터의 읽기 전용 복제본 DB 인스턴스를 참조하세요.

AWS Network Firewall 제어:

이러한 제어는 네트워크 방화벽 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::Firewall`

AWS Config 규칙: `netfw-multi-az-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 AWS Network Firewall 제어는 통해 관리되는 방화벽이 여러 가용 영역 (AZ) 에 배포되었는지 여부를 평가합니다. 방화벽을 하나의 AZ에만 배포하면 제어가 실패합니다.

AWS 글로벌 인프라에는 여러 개가 포함됩니다. AWS 리전 AZ는 각 리전 내에서 물리적으로 분리되고 격리된 위치로, 이러한 위치는 짧은 지연 시간, 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 여러 AZ에 Network Firewall 방화벽을 배포하면 AZ 간에 트래픽을 분산하고 이동할 수 있으므로 고가용성 솔루션을 설계하는 데 도움이 됩니다.

이제 Security Hub가 와 통합되었습니다

여러 AZ에 Network Firewall 방화벽 배포

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창의 Network Firewall에서 방화벽을 선택합니다.
3. 방화벽 페이지에서 편집하려는 방화벽을 선택합니다.
4. 방화벽 세부 정보 페이지에서 방화벽 세부 정보 탭을 선택합니다.
5. 관련 정책 및 VPC 섹션에서 편집을 선택합니다.
6. 새 AZ를 추가하려면 새 서브넷 추가를 선택합니다. 사용할 AZ와 서브넷을 선택합니다. 두 개 이상의 AZ를 선택해야 합니다.
7. 저장을 선택합니다.

[NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(12), NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::LoggingConfiguration`

AWS Config 규칙: `netfw-logging-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 AWS Network Firewall 방화벽에 대한 로깅이 활성화되었는지 여부를 확인합니다. 하나 이상의 로그 유형에 대해 로깅이 활성화되지 않았거나 로깅 대상이 존재하지 않는 경우 제어가 실패합니다.

로깅은 방화벽의 안정성, 가용성 및 성능을 유지하는 데 도움이 됩니다. Network Firewall에서 로깅은 상태 저장 엔진이 패킷 흐름을 받은 시간, 패킷 흐름에 대한 상세 정보, 패킷 흐름에 대해 수행된 상태 저장 규칙 동작을 비롯해 네트워크 트래픽에 대한 자세한 정보를 제공합니다.

이제 Security Hub가 와 통합되었습니다

방화벽 로깅을 활성화하려면 AWS Network Firewall 개발자 안내서의 방화벽 로깅 구성 업데이트를 참조하세요.

[NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config 규칙: `netfw-policy-rule-group-associated`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 네트워크 방화벽 정책에 상태 저장 또는 상태 비저장 규칙 그룹이 연결되어 있는지 확인합니다. 상태 비저장 또는 상태 저장 규칙 그룹이 할당되지 않으면 제어가 실패합니다.

방화벽 정책은 Amazon Virtual Private Cloud(Amazon VPC)에서 방화벽이 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하면 패킷과 트래픽 흐름을 필터링하는 데 도움이 되며 기본 트래픽 처리를 정의합니다.

이제 Security Hub가 와 통합되었습니다

네트워크 방화벽 정책에 규칙 그룹을 추가하려면 AWS Network Firewall 개발자 가이드에서 방화벽 정책 업데이트를 참조하십시오. 규칙 그룹을 만들고 관리하는 방법에 대한 자세한 내용은 AWS Network Firewall의 규칙 그룹을 참조하십시오.

[NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config 규칙: `netfw-policy-default-action-full-packets`

스케줄 유형: 변경이 트리거됨

파라미터:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`(사용자 지정할 수 없음)

이 제어는 네트워크 방화벽 정책의 전체 패킷에 대한 기본 상태 비저장 작업이 삭제인지 전달인지 확인합니다. `Drop` 또는 `Forward`를 선택하면 제어가 통과하고, `Pass`를 선택하면 제어가 실패합니다.

방화벽 정책은 방화벽이 Amazon VPC의 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링합니다. Pass를 기본값으로 설정하면 의도하지 않은 트래픽이 허용될 수 있습니다.

이제 Security Hub가 와 통합되었습니다

방화벽 정책을 변경하려면 AWS Network Firewall 개발자 안내서의 방화벽 정책 업데이트를 참조하십시오. 상태 비저장 기본 작업에서 편집을 선택합니다. 그런 다음 작업으로 삭제 또는 상태 저장 규칙 그룹으로 전달을 선택합니다.

[NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config 규칙: `netfw-policy-default-action-fragment-packets`

스케줄 유형: 변경이 트리거됨

파라미터:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe`(사용자 지정할 수 없음)

이 제어는 네트워크 방화벽 정책의 조각화된 패킷에 대한 기본 상태 비저장 작업이 삭제인지 전달인지 확인합니다. Drop 또는 Forward를 선택하면 제어가 통과하고, Pass를 선택하면 제어가 실패합니다.

방화벽 정책은 방화벽이 Amazon VPC의 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링합니다. Pass를 기본값으로 설정하면 의도하지 않은 트래픽이 허용될 수 있습니다.

이제 Security Hub가 와 통합되었습니다

방화벽 정책을 변경하려면 AWS Network Firewall 개발자 안내서의 방화벽 정책 업데이트를 참조하십시오. 상태 비저장 기본 작업에서 편집을 선택합니다. 그런 다음 작업으로 삭제 또는 상태 저장 규칙 그룹으로 전달을 선택합니다.

[NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(5)

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::RuleGroup`

AWS Config 규칙: `netfw-stateless-rule-group-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 의 상태 비저장 규칙 그룹에 규칙이 포함되어 있는지 확인합니다. AWS Network Firewall 규칙 그룹에 규칙이 없으면 제어가 실패합니다.

규칙 그룹에는 방화벽이 VPC의 트래픽을 처리하는 방법을 정의하는 규칙이 포함되어 있습니다. 빈 상태 비저장 규칙 그룹이 방화벽 정책에 존재하면 규칙 그룹이 트래픽을 처리할 것 같은 인상을 줄 수 있습니다. 하지만 상태 비저장 규칙 그룹이 비어 있으면 트래픽을 처리하지 않습니다.

이제 Security Hub가 와 통합되었습니다

Network Firewall 규칙 그룹에 규칙을 추가하려면 AWS Network Firewall 개발자 안내서의 상태 저장 규칙 그룹 업데이트를 참조하십시오. 방화벽 세부 정보 페이지에서 상태 비저장 규칙 그룹에 대해 편집을 선택하여 규칙을 추가합니다.

[NetworkFirewall.7] Network Firewall 방화벽에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::NetworkFirewall::Firewall`

AWS Config 규칙: `tagged-networkfirewall-firewall` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS Network Firewall 방화벽에 매개변수에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 방화벽에 태그 키가 없거나 매개변수에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 방화벽에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Network Firewall 방화벽에 태그를 추가하려면 AWS Network Firewall 개발자 안내서의 AWS Network Firewall 리소스 태깅을 참조하십시오.

[NetworkFirewall.8] Network Firewall 방화벽 정책에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config 규칙: `tagged-networkfirewall-firewallpolicy` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS Network Firewall 방화벽 정책에 매개변수에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 방화벽 정책에 태그 키가 없거나 매개변수에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 방화벽 정책에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Network Firewall 정책에 태그를 추가하려면 AWS Network Firewall 개발자 안내서의 AWS Network Firewall 리소스 태깅을 참조하십시오.

[NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2)

범주: 보호 > 네트워크 보안

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::Firewall`

AWS Config 규칙: `netfw-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS Network Firewall 방화벽에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 방화벽에 삭제 방지가 활성화되어 있지 않으면 제어가 실패합니다.

AWS Network Firewall VPC (Virtual Private Cloud) 에서 들어오거나 가상 사설 클라우드 (VPC) 간에 들어오는 트래픽을 검사하고 필터링할 수 있는 상태 저장 관리형 네트워크 방화벽 및 침입 탐지 서비스입니다. 삭제 방지 설정은 실수로 방화벽을 삭제하는 것을 방지합니다.

이제 Security Hub가 와 통합되었습니다

기존 Network Firewall 방화벽에서 삭제 방지를 활성화하려면 AWS Network Firewall 개발자 안내서의 방화벽 업데이트를 참조하십시오. 변경 방지에 대해서는 활성화를 선택합니다. UpdateFirewallDeleteProtectionAPI를 호출하고 필드를 로 설정하여 삭제 보호를 활성화할 수도 있습니다. `DeleteProtection` `true`

아마존 OpenSearch 서비스 컨트롤

이러한 컨트롤은 OpenSearch 서비스 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-encrypted-at-rest`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 OpenSearch 도메인에 encryption-at-rest 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우 이 확인이 실패합니다.

민감한 데이터에 대한 보안을 강화하려면 OpenSearch 서비스 도메인이 유휴 상태에서 암호화되도록 구성해야 합니다. 저장된 데이터의 암호화를 구성하면 암호화 키를 AWS KMS 저장하고 관리합니다. 암호화를 수행하려면 256비트 키가 포함된 고급 암호화 표준 알고리즘 (AES-256) 을 AWS KMS 사용합니다.

서비스 저장 중 암호화에 대해 자세히 알아보려면 Amazon OpenSearch OpenSearch Service개발자 안내서의 Amazon OpenSearch Service의 유휴 데이터 암호화를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

신규 및 기존 OpenSearch 도메인에 대해 저장 중 암호화를 활성화하려면 Amazon OpenSearch Service 개발자 안내서의 저장 데이터 암호화 활성화를 참조하십시오.

[Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 심각

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-in-vpc-only`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 OpenSearch 도메인이 VPC에 있는지 여부를 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다.

OpenSearch 도메인이 퍼블릭 서브넷에 연결되지 않았는지 확인해야 합니다. Amazon OpenSearch 서비스 개발자 안내서의 리소스 기반 정책을 참조하십시오. 또한 권장 모범 사례에 따라 VPC가 구성되었는지 확인해야 합니다. 또한 Amazon VPC 사용 설명서에서 VPC에 대한 보안 모범 사례를 참조하십시오.

OpenSearch VPC 내에 배포된 도메인은 퍼블릭 인터넷을 통과할 필요 없이 프라이빗 AWS 네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPC는 네트워크 ACL 및 보안 그룹을 포함하여 OpenSearch 도메인에 대한 액세스를 보호하기 위한 다양한 네트워크 제어를 제공합니다. Security Hub는 퍼블릭 OpenSearch 도메인을 VPC로 마이그레이션하여 이러한 제어를 활용할 것을 권장합니다.

이제 Security Hub가 와 통합되었습니다

퍼블릭 엔드포인트가 있는 도메인을 만들 경우 나중에 해당 도메인을 VPC 안에 배치할 수 없습니다. 대신에 새 도메인을 만들어 데이터를 마이그레이션해야 합니다. 반대의 경우도 마찬가지입니다. VPC 내에 도메인을 만들 경우 퍼블릭 엔드포인트를 가질 수 없습니다. 대신 다른 도메인을 만들거나 이 제어를 비활성화해야 합니다.

지침은 Amazon OpenSearch 서비스 개발자 안내서의 VPC 내에서 Amazon OpenSearch 서비스 도메인 시작을 참조하십시오.

[Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-node-to-node-encryption-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 OpenSearch 도메인에 node-to-node 암호화가 활성화되어 있는지 확인합니다. 도메인에서 node-to-node 암호화를 사용하지 않도록 설정하면 이 제어가 실패합니다.

HTTPS (TLS) 는 잠재적 공격자가 또는 유사한 공격을 사용하여 네트워크 트래픽을 도청하거나 조작하는 것을 방지하는 데 사용할 수 있습니다. person-in-the-middle 암호화된 HTTPS(TLS) 연결만 허용되어야 합니다. OpenSearch 도메인 node-to-node 암호화를 활성화하면 전송 중에 클러스터 내 통신이 암호화됩니다.

이 구성과 관련하여 성능이 저하될 수 있습니다. 이 옵션을 활성화하기 전에 성능 균형을 파악하고 테스트해야 합니다.

이제 Security Hub가 와 통합되었습니다

OpenSearch 도메인에서 node-to-node 암호화를 활성화하려면 Amazon OpenSearch Service 개발자 안내서의 node-to-node 암호화 활성화를 참조하십시오.

[Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-logs-to-cloudwatch`

스케줄 유형: 변경이 트리거됨

파라미터:

- `logtype = 'error'`(사용자 지정할 수 없음)

이 컨트롤은 오류 로그를 Logs로 보내도록 OpenSearch 도메인이 구성되어 있는지 확인합니다. CloudWatch 도메인에 대한 오류 로깅이 활성화되지 않은 경우 이 CloudWatch 제어는 실패합니다.

OpenSearch 도메인에 대한 오류 로그를 활성화하고 해당 로그를 Logs로 전송하여 CloudWatch 보존 및 응답을 받아야 합니다. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

이제 Security Hub가 와 통합되었습니다

로그 게시를 활성화하려면 Amazon OpenSearch Service 개발자 안내서의 로그 게시 활성화 (콘솔) 를 참조하십시오.

[Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-audit-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

- `cloudWatchLogsLogGroupArnList`(사용자 지정할 수 없음) – Security Hub는 이 파라미터를 채우지 않습니다. 감사 로그용으로 구성해야 하는 쉼표로 구분된 CloudWatch 로그 로그 그룹 목록입니다.

이 규칙은 OpenSearch 도메인의 로그 CloudWatch 로그 그룹이 이 매개 변수 목록에 지정되지 않은 `NON_COMPLIANT` 경우에 적용됩니다.

이 컨트롤은 OpenSearch 도메인에 감사 로깅이 활성화되어 있는지 확인합니다. OpenSearch 도메인에 감사 로깅이 활성화되어 있지 않으면 이 제어가 실패합니다.

감사 로그는 고도로 사용자 지정이 가능합니다. 이를 통해 인증 성공 및 실패, 요청, 색인 변경, 수신 검색 쿼리 등 OpenSearch 클러스터에서의 사용자 활동을 추적할 OpenSearch 수 있습니다.

이제 Security Hub가 와 통합되었습니다

감사 로그 활성화에 대한 지침은 Amazon OpenSearch Service 개발자 안내서의 감사 로그 활성화를 참조하십시오.

[Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-data-node-fault-tolerance`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 OpenSearch 도메인이 최소 세 개의 데이터 노드로 구성되어 있는지, 구성되었는지 여부를 확인합니다. `zoneAwarenessEnabled` `true` 이 `instanceCount` 제어는 OpenSearch 도메인이 3개 미만이거나 `zoneAwarenessEnabled` %인 경우 해당 도메인에 대해 `false` 실패합니다.

OpenSearch 도메인에는 고가용성 및 내결함성을 위해 최소 3개의 데이터 노드가 필요합니다. 3개 이상의 데이터 노드가 있는 OpenSearch 도메인을 배포하면 노드에 장애가 발생해도 클러스터 작동이 보장됩니다.

이제 Security Hub가 와 통합되었습니다

도메인의 데이터 노드 수 수정하기 OpenSearch

1. AWS 콘솔에 로그인하고 https://console.aws.amazon.com/aos/ 에서 아마존 OpenSearch 서비스 콘솔을 엽니다.

2. 내 도메인에서 편집할 도메인의 이름을 선택하고 편집을 선택합니다.
3. 데이터 노드에서 노드 수를 3보다 큰 수로 설정합니다. 세 개의 가용 영역에 배포하는 경우 가용 영역 간에 균등하게 분배되도록 수를 3의 배수로 설정하십시오.
4. 제출을 선택합니다.

[Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리 > 민감한 API 작업 제한

심각도: 높음

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-access-control-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 도메인에 세분화된 액세스 제어가 활성화되어 있는지 OpenSearch 확인합니다. 세분화된 액세스 제어가 비활성화된 경우 제어에 실패합니다. 세분화된 액세스 제어를 사용하려면 매개변수가 활성화되어야 합니다`advanced-security-options`. OpenSearch `update-domain-config`

세분화된 액세스 제어는 Amazon Service의 데이터에 대한 액세스를 제어하는 추가 방법을 제공합니다. OpenSearch

이제 Security Hub가 와 통합되었습니다

세분화된 액세스 제어를 활성화하려면 Amazon OpenSearch Service 개발자 안내서의 Amazon Service의 세분화된 액세스 제어를 참조하십시오. OpenSearch

[Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .

관련 요구 사항: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3),

NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-https-required`

스케줄 유형: 변경이 트리거됨

파라미터:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`(사용자 지정할 수 없음)

이 제어는 Amazon OpenSearch Service 도메인 엔드포인트가 최신 TLS 보안 정책을 사용하도록 구성되었는지 여부를 확인합니다. OpenSearch 도메인 엔드포인트가 지원되는 최신 정책을 사용하도록 구성되지 않았거나 HTTPS가 활성화되지 않은 경우 제어가 실패합니다.

HTTPS (TLS) 는 잠재적 공격자가 네트워크 트래픽을 도청하거나 조작하기 위한 person-in-the-middle 또는 유사한 공격을 사용하는 것을 방지하는 데 사용할 수 있습니다. 암호화된 HTTPS(TLS) 연결만 허용되어야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 이해해야 합니다. TLS 1.2는 이전 버전의 TLS보다 몇 가지 향상된 보안 기능을 제공합니다.

이제 Security Hub가 와 통합되었습니다

TLS 암호화를 활성화하려면 API 작업을 사용하십시오. UpdateDomainConfig 값을 지정하도록 DomainEndpointOptions필드를 구성합니다. `TLSSecurityPolicy` 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 N ode-to-node 암호화를 참조하십시오.

[Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `tagged-opensearch-domain` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon OpenSearch Service 도메인에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 도메인에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 도메인에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

OpenSearch 서비스 도메인에 태그를 추가하려면 Amazon OpenSearch Service 개발자 안내서의 태그 사용을 참조하십시오.

[Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 낮음

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-update-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon OpenSearch Service 도메인에 최신 소프트웨어 업데이트가 설치되어 있는지 확인합니다. 소프트웨어 업데이트가 제공되지만 도메인에 설치되지 않은 경우 제어가 실패합니다.

OpenSearch 서비스 소프트웨어 업데이트는 환경에 사용할 수 있는 최신 플랫폼 수정, 업데이트 및 기능을 제공합니다. 패치 설치를 up-to-date 유지하면 도메인 보안 및 가용성을 유지하는 데 도움이 됩니다. 필수 업데이트에 대해 아무 작업도 수행하지 않으면 (보통 2주 후) 서비스 소프트웨어가 자동으로 업데이트됩니다. 서비스 중단을 최소화하려면 도메인 트래픽이 적은 시간대에 업데이트를 예약하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

OpenSearch 도메인에 대한 소프트웨어 업데이트를 설치하려면 Amazon OpenSearch Service 개발자 안내서의 업데이트 시작을 참조하십시오.

[Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.

관련 요구 사항: NIST.800-53.R5 CP-10, NIST.800-53.R5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-primary-node-fault-tolerance`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon OpenSearch Service 도메인이 3개 이상의 전용 기본 노드로 구성되어 있는지 확인합니다. 도메인의 전용 기본 노드가 3개 미만이면 제어가 실패합니다.

OpenSearch 서비스는 전용 기본 노드를 사용하여 클러스터 안정성을 높입니다. 전용 기본 노드는 클러스터 관리 작업을 수행하지만 데이터를 보관하거나 데이터 업로드 요청에 응답하지는 않습니다. 예비 버전과 함께 다중 AZ를 사용하는 것이 좋습니다. 그러면 각 프로덕션 OpenSearch 도메인에 전용 기본 노드 3개가 추가됩니다.

이제 Security Hub가 와 통합되었습니다

OpenSearch 도메인의 기본 노드 수를 변경하려면 Amazon 서비스 개발자 안내서의 Amazon OpenSearch Service 도메인 생성 및 관리를 참조하십시오. OpenSearch

AWS Private Certificate Authority 규제:

이러한 컨트롤은 AWS Private CA 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[PCA.1] AWS Private CA 루트 인증 기관을 비활성화해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::ACMPCA::CertificateAuthority`

AWS Config 규칙: `acm-pca-root-ca-disabled`

스케줄 유형: 주기적

파라미터: 없음

이 AWS Private CA 컨트롤은 비활성화된 루트 CA (인증 기관) 가 있는지 확인합니다. 루트 CA가 활성화되면 제어가 실패합니다.

를 사용하여 루트 CA와 AWS Private CA하위 CA를 포함하는 CA 계층 구조를 만들 수 있습니다. 특히 프로덕션 환경에서는 일상적인 작업에 루트 CA를 사용하는 것을 최소화해야 합니다. 루트 CA는 중간 CA에 대한 인증서를 발급하기 위한 용도로만 사용해야 합니다. 이렇게 하면 중간 CA가 최종 엔터티 인증서를 발급하는 일상적인 작업을 수행하는 동안 루트 CA를 손상 없이 저장할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

루트 CA를 비활성화하려면 AWS Private Certificate Authority 사용 설명서의 CA 상태 업데이트를 참조하세요.

Amazon Relational Database Service 제어

이러한 제어는 Amazon RDS 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[RDS.1] RDS 스냅샷은 비공개여야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config 규칙: `rds-snapshots-public-prohibited`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS 스냅샷이 퍼블릭인지 여부를 확인합니다. RDS 스냅샷이 퍼블릭인 경우 제어가 실패합니다. 이 제어는 RDS 인스턴스, Aurora DB 인스턴스, Neptune DB 인스턴스 및 Amazon DocumentDB 클러스터를 평가합니다.

RDS 스냅샷은 특정 시점에 RDS 인스턴스의 데이터를 백업하는 데 사용됩니다. RDS 인스턴스의 이전 상태를 복원하는 데 사용할 수 있습니다.

RDS 스냅샷은 의도하지 않은 경우 공개 상태가 아니어야 합니다. 암호화되지 않은 수동 스냅샷을 공개로 공유하면 모든 AWS 계정에서 해당 스냅샷을 사용할 수 있습니다. 이로 인해 의도하지 않은 RDS 인스턴스 데이터가 노출될 수 있습니다.

공용 액세스를 허용하도록 구성을 변경한 경우 AWS Config 규칙이 최대 12시간 동안 변경 사항을 감지하지 못할 수 있습니다. AWS Config 규칙이 변경을 감지할 때까지는 구성이 규칙을 위반하더라도 확인이 통과됩니다.

DB 스냅샷 공유에 대한 자세한 내용은 Amazon RDS 사용 설명서의 DB 스냅샷 공유를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

RDS 스냅샷에서 퍼블릭 액세스를 제거하려면 Amazon RDS 사용 설명서의 스냅샷 공유를 참조하십시오. DB 스냅샷 가시성에서 비공개를 선택합니다.

[RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v3.0.0/2.3.3, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (4), NIST.800-ST.800-53.r5 SC-7 (5)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-public-access-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 인스턴스 구성 항목의 `PubliclyAccessible` 필드를 평가하여 Amazon RDS 인스턴스에 퍼블릭 액세스가 가능한지 여부를 확인합니다.

Neptune DB 인스턴스와 Amazon DocumentDB 클러스터에는 `PubliclyAccessible` 플래그가 없으므로 평가할 수 없습니다. 그러나 이 제어는 여전히 이러한 리소스에 대한 조사 결과를 생성할 수 있습니다. 이러한 조사 결과를 숨길 수 있습니다.

RDS 인스턴스 구성의 `PubliclyAccessible` 값은 DB 인스턴스에 퍼블릭 액세스가 가능한지 여부를 나타냅니다. DB 인스턴스가 `PubliclyAccessible`로 구성된 경우, 퍼블릭 IP 주소로 확인되는 공개적으로 확인 가능한 DNS 이름을 가진 인터넷 경계 인스턴스입니다. DB 인스턴스에 퍼블릭 액세스가 불가한 경우 프라이빗 IP 주소로 확인되는 DNS 이름을 가진 내부 인스턴스인 것입니다.

RDS 인스턴스를 공개적으로 액세스할 수 있도록 의도하지 않는 한 RDS 인스턴스를 `PubliclyAccessible` 값으로 구성하면 안 됩니다. 이렇게 하면 데이터베이스 인스턴스에 불필요한 트래픽이 발생할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

RDS DB 인스턴스에서 퍼블릭 액세스를 제거하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하십시오. 퍼블릭 액세스에서 아니오를 선택합니다.

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/2.3.1, CIS AWS 재단 벤치마크 v1.4.0/2.3.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-28, NIST.800-53.R5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6) SC-13

범주: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-storage-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS DB 인스턴스에 스토리지 암호화가 활성화되어 있는지 확인합니다.

이 제어는 RDS DB 인스턴스용입니다. 하지만 Aurora DB 인스턴스, Neptune DB 인스턴스 및 Amazon DocumentDB 클러스터에 대한 조사 결과를 생성할 수도 있습니다. 이러한 조사 결과가 유용하지 않으면 숨길 수 있습니다.

RDS DB 인스턴스의 중요 데이터에 대한 보안을 강화하려면 RDS DB 인스턴스가 유휴 상태에서 암호화되도록 구성해야 합니다. 유휴 시 RDS DB 인스턴스 및 스냅샷을 암호화하려면 RDS DB 인스턴스에 대해 암호화 옵션을 활성화합니다. 유휴 시 암호화된 데이터에는 DB 인스턴스에 대한 기본 스토리지, 자동 백업, 읽기 전용 복제본 및 스냅샷이 포함됩니다.

RDS 암호화된 DB 인스턴스는 RDS DB 인스턴스를 호스팅하는 서버의 데이터를 개방형 표준 AES-256 암호화 알고리즘을 사용하여 암호화합니다. 데이터가 암호화되면 Amazon RDS는 성능에 최소한의 영향을 미치면서 투명하게 데이터 액세스 인증 및 암호 해독을 처리합니다. 암호화를 사용하도록 데이터베이스 클라이언트 애플리케이션을 수정하지 않아도 됩니다.

Amazon RDS 암호화는 현재 모든 데이터베이스 엔진과 스토리지 유형에 사용할 수 있습니다. Amazon RDS 암호화는 대부분의 DB 인스턴스 클래스에서 사용 가능합니다. Amazon RDS 암호화를 지원하지 않는 DB 인스턴스 클래스에 대해 알아보려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 암호화를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Amazon RDS의 DB 인스턴스 암호화에 대한 자세한 내용은 Amazon RDS 사용 설명서의 Amazon RDS 리소스 암호화를 참조하십시오.

[RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

범주: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config 규칙: `rds-snapshot-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS DB 스냅샷의 암호화 여부를 확인합니다. RDS DB 스냅샷이 암호화되지 않으면 제어가 실패합니다.

이 제어는 RDS DB 인스턴스용입니다. 하지만 Aurora DB 인스턴스, Neptune DB 인스턴스 및 Amazon DocumentDB 클러스터의 스냅샷에 대한 조사 결과를 생성할 수도 있습니다. 이러한 조사 결과가 유용하지 않으면 숨길 수 있습니다.

데이터를 저장 시 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. RDS 스냅샷의 데이터는 추가 보안 계층을 위해 저장 시 암호화되어야 합니다.

이제 Security Hub가 와 통합되었습니다

RDS 스냅샷을 암호화하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 암호화를 참조하십시오. RDS DB 인스턴스를 암호화하면 암호화된 데이터에는 인스턴스의 기본 스토리지, 자동 백업, 읽기 전용 복제본 및 스냅샷이 포함됩니다.

RDS DB 인스턴스를 생성할 때만 암호화할 수 있으며, DB 인스턴스가 생성된 후에는 암호화할 수 없습니다. 다만 암호화되지 않은 스냅샷의 사본을 암호화할 수 있기 때문에 암호화되지 않은 DB 인스턴스에 실질적으로 암호화를 추가할 수 있습니다. 즉, DB 인스턴스의 스냅샷을 만든 다음 해당 스냅샷의 암호화된 사본을 만들 수 있습니다. 그런 다음 암호화된 스냅샷에서 DB 인스턴스를 복구할 수 있고, 원본 DB 인스턴스의 암호화된 사본이 생깁니다.

[RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-multi-az-support`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 RDS DB 인스턴스에 대해 고가용성이 활성화되었는지 여부를 확인합니다.

RDS DB 인스턴스는 여러 가용 영역(AZ)에 대해 구성되어야 합니다. 이렇게 하면 저장된 데이터의 가용성이 보장됩니다. 다중 AZ 배포를 사용하면 AZ 가용성에 문제가 있거나 정기적인 RDS 유지 관리 중에 문제가 있는 경우 자동 장애 조치가 가능합니다.

이제 Security Hub가 와 통합되었습니다

다중 AZ에 DB 인스턴스를 배포하려면 Amazon RDS 사용 설명서의 DB 인스턴스를 다중 AZ DB 인스턴스 배포로 수정을 참조하십시오.

[RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-enhanced-monitoring-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
`monitoringInterval`	모니터링 지표 수집 간격(초)	Enum	`1`, `5`, `10`, `15`, `30`, `60`	기본값 없음	

이 제어는 Amazon Relational Database Service(RDS) DB 인스턴스에 확장 모니터링이 활성화되었는지 확인합니다. 인스턴스에 대해 향상된 모니터링이 활성화되지 않은 경우 제어가 실패합니다. `monitoringInterval` 파라미터에 사용자 지정 값을 제공하는 경우, 인스턴스에 대해 지정된 간격으로 향상된 모니터링 지표가 수집되는 경우에만 제어가 통과합니다.

Amazon RDS에서는 Enhanced Monitoring을 통해 기본 인프라의 성능 변화에 더욱 신속하게 대응할 수 있습니다. 이러한 성능 변화로 인해 데이터 가용성이 부족해질 수 있습니다. Enhanced Monitoring은 RDS DB 인스턴스가 실행되는 운영 체제에 대한 실시간 지표를 제공합니다. 에이전트가 인스턴스에 설치되어 있습니다. 에이전트는 하이퍼바이저 계층에서 가능한 것보다 더 정확하게 지표를 얻을 수 있습니다.

Enhanced Monitoring 지표는 DB 인스턴스의 다양한 프로세스나 스레드가 CPU를 어떻게 사용하는지 확인하려는 경우에 유용합니다. 자세한 내용을 알아보려면 Amazon RDS 사용 설명서의 Enhanced Monitoring을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

DB 인스턴스의 Enhanced Monitoring을 활성화하는 방법에 대한 자세한 지침은 Amazon RDS 사용 설명서의 Enhanced Monitoring 설정 및 활성화를 참조하세요.

[RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS DB 클러스터에 삭제 보호가 활성화되어 있는지 확인합니다. RDS DB 클러스터에 삭제 방지 기능이 활성화되지 않은 경우 제어가 실패합니다.

이 제어는 RDS DB 인스턴스용입니다. 하지만 Aurora DB 인스턴스, Neptune DB 인스턴스 및 Amazon DocumentDB 클러스터에 대한 조사 결과를 생성할 수도 있습니다. 이러한 조사 결과가 유용하지 않으면 숨길 수 있습니다.

클러스터 삭제 보호를 활성화하면 우발적인 데이터베이스 삭제 또는 승인되지 않은 개체에 의한 삭제에 대한 추가 보호 계층이 제공됩니다.

삭제 방지 기능이 활성화되면 RDS 클러스터가 삭제될 수 없습니다. 삭제 요청이 성공하려면 먼저 삭제 보호를 비활성화해야 합니다.

이제 Security Hub가 와 통합되었습니다

RDS DB 클러스터에 대한 삭제 보호를 활성화하려면 Amazon RDS 사용 설명서의 콘솔, CLI 및 API를 사용하여 DB 클러스터 수정을 참조하십시오. 삭제 방지에서 삭제 방지 활성화를 선택합니다.

[RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web`(사용자 지정할 수 없음)

이 제어는 나열된 데이터베이스 엔진 중 하나를 사용하는 RDS DB 인스턴스에 삭제 보호가 활성화되어 있는지 확인합니다. RDS DB 인스턴스에 삭제 방지 기능이 활성화되지 않은 경우 제어가 실패합니다.

인스턴스 삭제 보호를 활성화하면 우발적인 데이터베이스 삭제 또는 승인되지 않은 개체에 의한 삭제에 대한 추가 보호 계층이 제공됩니다.

삭제 보호가 활성화되어 있는 동안에는 RDS DB 인스턴스를 삭제할 수 없습니다. 삭제 요청이 성공하려면 먼저 삭제 보호를 비활성화해야 합니다.

이제 Security Hub가 와 통합되었습니다

RDS DB 인스턴스에 대한 삭제 보호를 활성화하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하십시오. 삭제 방지에서 삭제 방지 활성화를 선택합니다.

[RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon RDS DB 인스턴스가 Amazon CloudWatch Logs에 다음 로그를 게시하도록 구성되어 있는지 여부를 확인합니다. 인스턴스가 다음 로그를 Logs에 게시하도록 구성되지 않은 경우 제어가 실패합니다 CloudWatch .

- Oracle: (Alert, Audit, Trace, Listener)
- PostgreSQL: (Postgresql, Upgrade)
- MySQL: (감사, 오류, 일반,) SlowQuery
- MariaDB: (감사, 오류, 일반,) SlowQuery
- SQL Server: (Error, Agent)
- Aurora: (감사, 오류, 일반,) SlowQuery
- 오로라-MySQL: (감사, 오류, 일반,) SlowQuery
- Aurora-PostgreSQL: (Postgresql, Upgrade).

RDS 데이터베이스에는 관련 로그가 활성화되어 있어야 합니다. 데이터베이스 로깅은 RDS에 대한 요청에 대한 자세한 기록을 제공합니다. 데이터베이스 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

이제 Security Hub가 와 통합되었습니다

RDS 데이터베이스 로그를 로그에 게시하려면 CloudWatch Amazon RDS 사용 설명서의 CloudWatch 로그에 게시할 로그 지정을 참조하십시오.

[RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-iam-authentication-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS DB 인스턴스에 IAM 데이터베이스 인증이 활성화되어 있는지 확인합니다. RDS DB 인스턴스에 대해 IAM 인증이 구성되지 않은 경우 제어가 실패합니다. 이 제어는 엔진 유형이 `mysql`, `postgres`, `aurora`, `aurora-mysql`, `aurora-postgresql` 및 `mariadb`인 RDS 인스턴스만 평가합니다. 또한 검색 결과가 생성되려면 RDS 인스턴스가 `available`,`backing-up`, `storage-optimization` 또는 `storage-full` 상태 중 하나여야 합니다.

IAM 데이터베이스 인증을 사용하면 암호 대신 인증 토큰을 사용하여 데이터베이스 인스턴스를 인증할 수 있습니다. 데이터베이스를 오가는 네트워크 트래픽은 SSL을 통해 암호화됩니다. 자세한 내용을 알아보려면 Amazon Aurora 사용 설명서의 IAM 데이터베이스 인증을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

RDS DB 인스턴스에서 IAM 데이터베이스 인증을 활성화하려면 Amazon RDS 사용 설명서의 IAM 데이터베이스 인증 활성화 및 비활성화를 참조하십시오.

[RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `db-instance-backup-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
`backupRetentionMinimum`	백업 보존 기간(일수)	Integer	7~35	7	
`checkReadReplicas`	RDS DB 인스턴스에 읽기 전용 복제본 백업이 활성화되어 있는지 확인합니다.	불	사용자 지정할 수 없음	`false`	

이 제어는 Amazon Relational Database Service 인스턴스에 자동 백업이 활성화되어 있고 백업 보존 기간이 지정된 기간 이상인지 확인합니다. 읽기 전용 복제본은 평가에서 제외됩니다. 인스턴트에 대한 백업이 활성화되지 않았거나 보존 기간이 지정된 기간 미만인 경우 제어가 실패합니다. 백업 보존 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 7일을 사용합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구할 수 있고 시스템의 복원력을 강화할 수 있습니다. Amazon RDS를 사용하면 일일 전체 인스턴스 볼륨 스냅샷을 구성할 수 있습니다. Amazon RDS 자동 백업에 대한 자세한 내용은 Amazon RDS 사용 설명서의 백업 작업을 참조하세요.

이제 Security Hub가 와 통합되었습니다

RDS DB 인스턴스에서 자동 백업을 활성화하려면 Amazon RDS 사용 설명서의 자동 백업 활성화를 참조하십시오.

[RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-iam-authentication-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS DB 클러스터에 IAM 데이터베이스 인증이 활성화되어 있는지 확인합니다.

IAM 데이터베이스 인증을 사용하면 데이터베이스 인스턴스에 암호 없이 인증할 수 있습니다. 인증은 인증 토큰을 사용합니다. 데이터베이스를 오가는 네트워크 트래픽은 SSL을 통해 암호화됩니다. 자세한 내용을 알아보려면 Amazon Aurora 사용 설명서의 IAM 데이터베이스 인증을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

DB 클러스터에 대한 IAM 인증을 활성화하려면 Amazon Aurora 사용 설명서의 IAM 데이터베이스 인증 활성화 및 비활성화를 참조하십시오.

[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/2.3.2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-automatic-minor-version-upgrade-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS 데이터베이스 인스턴스에 대해 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다.

자동 마이너 버전 업그레이드를 활성화하면 관계형 데이터베이스 관리 시스템(RDBMS)에 대한 최신 마이너 버전 업데이트가 설치됩니다. 이러한 업그레이드에는 보안 패치 및 버그 수정이 포함될 수 있습니다. 패치 설치를 최신 상태로 유지하는 것은 시스템 보안의 중요한 단계입니다.

이제 Security Hub가 와 통합되었습니다

기존 DB 인스턴스의 자동 마이너 버전 업그레이드를 활성화하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하십시오. 자동 마이너 버전 업그레이드의 경우 예를 선택합니다.

[RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `aurora-mysql-backtracking-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
`BacktrackWindowInHours`	Aurora MySQL 클러스터를 역추적하는 데 걸리는 기간(시간)	Double	`0.1~72`	기본값 없음	

이 제어는 Amazon Aurora 클러스터에 역추적이 활성화되어 있는지 확인합니다. 클러스터에 역추적이 활성화되지 않은 경우 제어가 실패합니다. `BacktrackWindowInHours` 파라미터에 사용자 지정 값을 제공하는 경우 지정된 시간 동안 클러스터를 역추적하는 경우에만 제어가 통과합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구할 수 있습니다. 또한 시스템의 복원력을 강화합니다. Aurora 역추적은 데이터베이스를 특정 시점으로 복구하는 데 걸리는 시간을 줄여줍니다. 이를 위해 데이터베이스를 복원할 필요는 없습니다.

이제 Security Hub가 와 통합되었습니다

Aurora 역추적을 활성화하려면 Amazon Aurora 사용 설명서의 역추적 구성을 참조하세요.

기존 클러스터에서는 역추적을 활성화할 수 없다는 점에 유의하세요. 대신 역추적이 활성화된 복제본을 생성할 수 있습니다. Aurora 역추적 제한 사항에 대한 자세한 내용은 역추적 개요의 제한 사항 목록을 참조하세요.

[RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-multi-az-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 RDS DB 클러스터에 대해 고가용성이 활성화되었는지 여부를 확인합니다. RDS DB 클러스터가 여러 가용 영역(AZ)에 배포되지 않으면 제어가 실패합니다.

저장된 데이터의 가용성을 보장하려면 여러 AZ에 대해 RDS DB 클러스터를 구성해야 합니다. 여러 AZ에 배포하면 AZ 가용성 문제가 발생하는 경우 및 정기적인 RDS 유지 관리 이벤트 중에 자동 장애 조치가 가능합니다.

이제 Security Hub가 와 통합되었습니다

다중 AZ에 DB 클러스터를 배포하려면 Amazon RDS 사용 설명서의 DB 인스턴스를 다중 AZ DB 인스턴스 배포로 수정을 참조하십시오.

Aurora 글로벌 데이터베이스에 대한 수정 단계가 다릅니다. Aurora 글로벌 데이터베이스에 대해 여러 가용 영역을 구성하려면 DB 클러스터를 선택합니다. 그런 다음 작업과 리더 추가를 선택하고 여러 AZ를 지정합니다. 자세한 내용을 알아보려면 Amazon Aurora 사용 설명서의 DB 클러스터에 Aurora 복제본 추가를 참조하십시오.

[RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-copy-tags-to-snapshots-enabled` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 스냅샷이 생성될 때 RDS DB 클러스터가 모든 태그를 스냅샷에 복사하도록 구성되어 있는지 확인합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 보안 상태를 평가하고 잠재적인 약점 영역에 조치를 취할 수 있도록 모든 RDS DB 클러스터에 대한 가시성을 확보해야 합니다. 스냅샷에는 상위 RDS 데이터베이스 클러스터와 동일한 방식으로 태그를 지정해야 합니다. 이 설정을 활성화하면 스냅샷이 상위 데이터베이스 클러스터의 태그를 상속하게 됩니다.

이제 Security Hub가 와 통합되었습니다

RDS DB 클러스터의 스냅샷에 태그를 자동으로 복사하려면 Amazon Aurora 사용 설명서의 콘솔, CLI 및 API를 사용하여 DB 클러스터 수정을 참조하십시오. 스냅샷으로 태그 복사를 선택합니다.

[RDS.17] RDS DB 인스턴스는 태그를 스냅샷에 복사하도록 구성되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-copy-tags-to-snapshots-enabled` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 스냅샷이 생성될 때 RDS DB 인스턴스가 모든 태그를 스냅샷에 복사하도록 구성되어 있는지 확인합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 보안 상태를 평가하고 잠재적인 약점 영역에 조치를 취할 수 있도록 모든 RDS DB 인스턴스에 대한 가시성을 확보해야 합니다. 스냅샷에는 상위 RDS 데이터베이스 인스턴스와 같은 방식으로 태그를 지정해야 합니다. 이 설정을 활성화하면 스냅샷이 상위 데이터베이스 인스턴스의 태그를 상속하게 됩니다.

이제 Security Hub가 와 통합되었습니다

RDS DB 인스턴스의 스냅샷에 태그를 자동으로 복사하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하십시오. 스냅샷으로 태그 복사를 선택합니다.

[RDS.18] RDS 인스턴스는 VPC에 배포되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 높음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-deployed-in-vpc` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS 인스턴스가 EC2-VPC 상에 배포되었는지 여부를 확인합니다.

VPC는 RDS 리소스에 대한 액세스를 보호하기 위한 여러 네트워크 제어를 제공합니다. 이러한 제어에는 VPC 엔드포인트, 네트워크 ACL, 보안 그룹이 포함됩니다. 이러한 제어 기능을 활용하려면 EC2-VPC 상에 RDS 인스턴스를 생성하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

RDS 인스턴스를 VPC로 이동하는 방법에 대한 지침은 Amazon RDS 사용 설명서의 DB 인스턴스용 VPC 업데이트를 참조하십시오.

[RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::RDS::EventSubscription`

AWS Config 규칙: `rds-cluster-event-notifications-configured` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 데이터베이스 클러스터에 대한 기존 Amazon RDS 이벤트 구독에 다음 소스 유형 및 이벤트 범주 키-값 쌍에 대해 사용하도록 설정된 알림이 있는지 확인합니다.

```
DBCluster: ["maintenance","failure"]
```

계정에 기존 이벤트 구독이 없는 경우 제어가 통과됩니다.

RDS 이벤트 알림은 Amazon SNS를 사용하여 RDS 리소스의 가용성 또는 구성 변경 사항을 알려줍니다. 이러한 알림을 통해 신속하게 대응할 수 있습니다. RDS 이벤트 알림에 대한 추가 정보는 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 사용을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

RDS 클러스터 이벤트 알림을 구독하려면 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 구독을 참조하십시오. 다음 값을 사용합니다.

필드	값
소스 유형	클러스터
포함할 클러스터	모든 클러스터
포함할 이벤트 범주	특정 이벤트 범주 또는 모든 이벤트 범주를 선택합니다.

[RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::RDS::EventSubscription`

AWS Config 규칙: `rds-instance-event-notifications-configured` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 데이터베이스 인스턴스에 대한 기존 Amazon RDS 이벤트 구독에 다음 소스 유형 및 이벤트 범주 키-값 쌍에 대해 사용하도록 설정된 알림이 있는지 확인합니다.

```
DBInstance: ["maintenance","configuration change","failure"]
```

계정에 기존 이벤트 구독이 없는 경우 제어가 통과됩니다.

RDS 이벤트 알림은 Amazon SNS를 사용하여 RDS 리소스의 가용성 또는 구성 변경 사항을 알려줍니다. 이러한 알림을 통해 신속하게 대응할 수 있습니다. RDS 이벤트 알림에 대한 추가 정보는 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 사용을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

RDS 인스턴스 이벤트 알림을 구독하려면 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 구독을 참조하십시오. 다음 값을 사용합니다.

필드	값
소스 유형	인스턴스
포함할 인스턴스	모든 인스턴스
포함할 이벤트 범주	특정 이벤트 범주 또는 모든 이벤트 범주를 선택합니다.

[RDS.21] 중요한 데이터베이스 파라미터 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::RDS::EventSubscription`

AWS Config 규칙: `rds-pg-event-notifications-configured` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 다음과 같은 소스 유형, 이벤트 범주 키-값 쌍에 대해 알림이 활성화된 상태에서 Amazon RDS 이벤트 구독이 존재하는지 확인합니다. 계정에 기존 이벤트 구독이 없는 경우 제어가 통과됩니다.

```
DBParameterGroup: ["configuration change"]
```

RDS 이벤트 알림은 Amazon SNS를 사용하여 RDS 리소스의 가용성 또는 구성 변경 사항을 알려줍니다. 이러한 알림을 통해 신속하게 대응할 수 있습니다. RDS 이벤트 알림에 대한 추가 정보는 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 사용을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

RDS 데이터베이스 파라미터 그룹 이벤트 알림을 구독하려면 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 구독을 참조하십시오. 다음 값을 사용합니다.

필드	값
소스 유형	파라미터 그룹
포함할 파라미터 그룹	모든 파라미터 그룹
포함할 이벤트 범주	특정 이벤트 범주 또는 모든 이벤트 범주를 선택합니다.

[RDS.22] 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::RDS::EventSubscription`

AWS Config 규칙: `rds-sg-event-notifications-configured` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 다음과 같은 소스 유형, 이벤트 범주 키-값 쌍에 대해 알림이 활성화된 상태에서 Amazon RDS 이벤트 구독이 존재하는지 확인합니다. 계정에 기존 이벤트 구독이 없는 경우 제어가 통과됩니다.

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS 이벤트 알림은 Amazon SNS를 사용하여 RDS 리소스의 가용성 또는 구성 변경 사항을 알려줍니다. 이러한 알림을 통해 신속하게 대응할 수 있습니다. RDS 이벤트 알림에 대한 추가 정보는 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 사용을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

RDS 인스턴스 이벤트 알림을 구독하려면 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 구독을 참조하십시오. 다음 값을 사용합니다.

필드	값
소스 유형	보안 그룹
포함해야 할 보안 그룹	모든 보안 그룹
포함할 이벤트 범주	특정 이벤트 범주 또는 모든 이벤트 범주를 선택합니다.

[RDS.23] RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용하지 않아야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(5)

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-no-default-ports` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS 클러스터 또는 인스턴스가 데이터베이스 엔진의 기본 포트가 아닌 다른 포트를 사용하는지 여부를 확인합니다. RDS 클러스터 또는 인스턴스가 기본 포트를 사용하는 경우 제어가 실패합니다.

알려진 포트를 사용하여 RDS 클러스터 또는 인스턴스를 배포하면 공격자가 클러스터 또는 인스턴스에 대한 정보를 추측할 수 있습니다. 공격자는 이 정보를 다른 정보와 함께 사용하여 RDS 클러스터 또는 인스턴스에 연결하거나 애플리케이션에 대한 추가 정보를 얻을 수 있습니다.

포트를 변경할 때는 이전 포트에 연결하는 데 사용된 기존 연결 문자열도 업데이트해야 합니다. 또한 DB 인스턴스의 보안 그룹에 새 포트에서의 연결을 허용하는 인그레스 규칙이 포함되어 있는지 확인해야 합니다.

이제 Security Hub가 와 통합되었습니다

기존 RDS DB 인스턴스의 기본 포트를 수정하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하십시오. 기존 RDS DB 클러스터의 기본 포트를 수정하려면 Amazon Aurora 사용 설명서의 콘솔, CLI 및 API를 사용하여 DB 클러스터 수정을 참조하십시오. 데이터베이스 포트의 경우 포트 값을 기본값이 아닌 값으로 변경하십시오.

[RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-default-admin-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS 데이터베이스 클러스터가 관리자 사용자 이름을 기본값에서 변경했는지 여부를 확인합니다. 이 제어는 neptune(Neptune DB) 또는 docdb(DocumentDB) 유형의 엔진에는 적용되지 않습니다. 관리자 사용자 이름을 기본값으로 설정하면 이 규칙이 실패합니다.

Amazon RDS 데이터베이스를 생성할 때는 기본 관리자 사용자 이름을 고유한 값으로 변경해야 합니다. 기본 사용자 이름은 공개되어 있으므로 RDS 데이터베이스 생성 중에 변경해야 합니다. 기본 사용자 이름을 변경하면 의도하지 않은 액세스의 위험이 줄어듭니다.

이제 Security Hub가 와 통합되었습니다

Amazon RDS 데이터베이스 클러스터와 연결된 관리자 사용자 이름을 변경하려면 데이터베이스를 생성할 때 새 RDS 데이터베이스 클러스터를 생성하고 기본 관리자 사용자 이름을 변경하십시오.

[RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-default-admin-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Relational Database Service(RDS) 데이터베이스 인스턴스의 관리자 사용자 이름을 기본값에서 변경했는지 여부를 확인합니다. 이 제어는 neptune(Neptune DB) 또는 docdb(DocumentDB) 유형의 엔진에는 적용되지 않습니다. 관리자 사용자 이름이 기본값으로 설정된 경우 제어가 실패합니다.

Amazon RDS 데이터베이스의 기본 관리 사용자 이름은 공개된 정보입니다. Amazon RDS 데이터베이스를 생성할 때는 기본 관리자 사용자 이름을 고유한 값으로 변경하여 의도하지 않은 액세스의 위험을 줄여야 합니다.

이제 Security Hub가 와 통합되었습니다

RDS 데이터베이스 인스턴스와 관련된 관리 사용자 이름을 변경하려면 먼저 새 RDS 데이터베이스 인스턴스를 생성하십시오. 데이터베이스를 생성할 때 기본 관리 사용자 이름을 변경하십시오.

[RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.

범주: 복구 > 복원력 > 백업 활성화

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: **`rds-resources-protected-by-backup-plan`**

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
`backupVaultLockCheck`	컨트롤은 매개변수가 true로 설정되어 있고 리소스가 AWS Backup Vault Lock을 사용하는지 여부를 확인합니다. `PASSED`	불	`true` 또는 `false`	기본값 없음	

이 제어는 Amazon RDS DB 인스턴스에 백업 계획이 적용되는지 여부를 평가합니다. RDS DB 인스턴스에 백업 계획이 적용되지 않는 경우 이 제어가 실패합니다. `backupVaultLockCheck`매개 변수를 다음과 같이 설정하면 인스턴스가 AWS Backup 잠긴 저장소에 백업된 경우에만 제어가 통과합니다. `true`

AWS Backup 데이터 백업을 중앙 집중화하고 자동화하는 완전 관리형 백업 서비스입니다. AWS 서비스를 사용하여 AWS Backup백업 계획이라는 백업 정책을 만들 수 있습니다. 이러한 계획을 사용하여 데이터 백업 빈도 및 백업 보존 기간과 같은 백업 요구 사항을 정의할 수 있습니다. 백업 계획에 RDS DB 인스턴스를 포함하면 의도하지 않은 손실이나 삭제로부터 데이터를 보호하는 데 도움이 됩니다.

이제 Security Hub가 와 통합되었습니다

RDS DB 인스턴스를 AWS Backup 백업 계획에 추가하려면 AWS Backup 개발자 안내서의 백업 계획에 리소스 할당을 참조하십시오.

[RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: **`rds-cluster-encrypted-at-rest`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS DB 클러스터가 저장 시 암호화되어 있는지 확인합니다. RDS DB 클러스터가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 해당 데이터의 기밀성을 보호하여 권한 없는 사용자가 해당 데이터에 액세스할 수 있는 위험을 줄일 수 있습니다. RDS DB 클러스터를 암호화하면 데이터와 메타데이터를 무단 액세스로부터 보호할 수 있습니다. 또한 프로덕션 파일 시스템의 data-at-rest 암호화에 대한 규정 준수 요구 사항도 충족합니다.

이제 Security Hub가 와 통합되었습니다

RDS DB 클러스터를 만들 때 저장 시 암호화를 활성화할 수 있습니다. 클러스터를 생성한 후에는 암호화 설정을 변경할 수 없습니다. 자세한 내용을 알아보려면 Amazon Aurora 사용 설명서의 Amazon Aurora DB 클러스터 암호화를 참조하십시오.

[RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `tagged-rds-dbcluster` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon RDS DB 클러스터에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. DB 클러스터에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 DB 클러스터에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어

(ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

RDS DB 클러스터에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하십시오.

[RDS.29] RDS DB 클러스터 스냅샷에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBClusterSnapshot`

AWS Config 규칙: `tagged-rds-dbclustersnapshot` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon RDS DB 클러스터 스냅샷에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. DB 클러스터 스냅샷에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 DB 클러스터 스냅샷에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

RDS DB 클러스터 스냅샷에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하십시오.

[RDS.30] RDS DB 인스턴스에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `tagged-rds-dbinstance` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon RDS DB 인스턴스에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. DB 인스턴스에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 DB 인스턴스에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

RDS DB 인스턴스에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하십시오.

[RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBSecurityGroup`

AWS Config 규칙: `tagged-rds-dbsecuritygroup` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon RDS DB 보안 그룹에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. DB 보안 그룹에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 DB 보안 그룹에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

RDS DB 보안 그룹에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하십시오.

[RDS.32] RDS DB 스냅샷에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBSnapshot`

AWS Config 규칙: `tagged-rds-dbsnapshot` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon RDS DB 스냅샷에 파라미터에 `requiredTagKeys` 정의된 특정 키가 포함된 태그가 있는지 확인합니다. DB 스냅샷에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 DB 스냅샷에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

RDS DB 스냅샷에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하십시오.

[RDS.33] RDS DB 서브넷 그룹에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBSubnetGroup`

AWS Config 규칙: `tagged-rds-dbsubnetgroups` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon RDS DB 서브넷 그룹에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` DB 서브넷 그룹에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는

경우 제어가 실패합니다. `requiredTagKeys` 파라미터가 제공되지 `requiredTagKeys` 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 DB 서브넷 그룹에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

RDS DB 서브넷 그룹에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하십시오.

[RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: **`rds-aurora-mysql-audit-logging-enabled`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon Aurora MySQL DB 클러스터가 감사 로그를 Amazon Logs에 게시하도록 구성되어 있는지 여부를 확인합니다. CloudWatch 클러스터가 감사 로그를 Logs에 게시하도록 구성되지 않은 경우 제어가 실패합니다. CloudWatch 컨트롤은 Aurora 서버리스 v1 DB 클러스터에 대한 검색 결과를 생성하지 않습니다.

감사 로그는 로그인 시도, 데이터 수정, 스키마 변경 및 보안 및 규정 준수를 위해 감사할 수 있는 기타 이벤트를 포함한 데이터베이스 활동 기록을 캡처합니다. Amazon Logs의 로그 그룹에 감사 로그를 게시하도록 Aurora MySQL DB 클러스터를 구성하면 CloudWatch 로그 데이터를 실시간으로 분석할 수 있습니다. CloudWatch 로그는 내구성이 뛰어난 스토리지에 로그를 보관합니다. 에서 경보를 생성하고 지표를 볼 수도 있습니다. CloudWatch

> **Note**
>
> 감사 로그를 로그에 게시하는 또 다른 방법은 고급 감사를 활성화하고 클러스터 수준 DB 파라미터를 로 설정하는 것입니다. CloudWatch `server_audit_logs_upload` 1 `server_audit_logs_upload parameter`의 기본값은 `0`입니다. 그러나 이 제어를 통과하려면 대신 다음 수정 지침을 사용하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

Aurora MySQL DB 클러스터 감사 로그를 로그에 게시하려면 Amazon Aurora CloudWatch 사용 설명서의 Amazon Logs에 Amazon Aurora MySQL 로그 게시를 참조하십시오 CloudWatch .

[RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: **`rds-cluster-auto-minor-version-upgrade-enable`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon RDS 다중 AZ DB 클러스터에 대해 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. 다중 AZ DB 클러스터에 대해 자동 마이너 버전 업그레이드가 활성화되지 않은 경우 제어가 실패합니다.

RDS는 다중 AZ DB 클러스터를 최신 상태로 유지할 수 있도록 자동 마이너 버전 업그레이드를 제공합니다. 마이너 버전은 새로운 소프트웨어 기능, 버그 수정, 보안 패치 및 성능 개선을 도입할 수 있습니다. RDS 데이터베이스 클러스터에서 자동 마이너 버전 업그레이드를 활성화하면 클러스터는 새 버전이 출시될 때 클러스터의 인스턴스와 함께 마이너 버전에 대한 자동 업데이트를 받게 됩니다. 업데이트는 유지 관리 기간 동안 자동으로 적용됩니다.

이제 Security Hub가 와 통합되었습니다

다중 AZ DB 클러스터에서 자동 마이너 버전 업그레이드를 활성화하려면 Amazon RDS 사용 설명서의 다중 AZ DB 클러스터 수정을 참조하십시오.

Amazon Redshift 제어

이러한 제어는 Amazon Redshift 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `redshift-cluster-public-access-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터가 퍼블릭 액세스가 가능한지 여부를 확인합니다. 이는 클러스터 구성 항목의 `PubliclyAccessible` 필드를 평가합니다.

Amazon Redshift 클러스터 구성의 `PubliclyAccessible` 속성은 클러스터에 공개적으로 액세스할 수 있는지 여부를 나타냅니다. 클러스터가 `true`로 설정된 `PubliclyAccessible`로 구성된 경우, 이는 퍼블릭 IP 주소로 확인되는 공개적으로 확인 가능한 DNS 이름이 있는 인터넷 연결 인스턴스입니다.

클러스터에 퍼블릭 액세스가 불가능한 경우 이는 프라이빗 IP 주소로 확인되는 DNS 이름을 가진 내부 인스턴스입니다. 클러스터를 공개적으로 액세스할 수 있도록 하려는 경우가 아니라면 클러스터를 `true`로 설정된 `PubliclyAccessible`로 구성해서는 안 됩니다.

이제 Security Hub가 와 통합되었습니다

Amazon Redshift 클러스터를 업데이트하여 퍼블릭 액세스를 비활성화하려면 Amazon Redshift 관리 안내서의 클러스터 수정을 참조하십시오. 퍼블릭 액세스 가능을 아니오로 설정합니다.

[Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2)

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config 규칙: `redshift-require-tls-ssl`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 전송 중 암호화를 사용하기 위해 Amazon Redshift 클러스터에 대한 연결이 필요한지 여부를 확인합니다. Amazon Redshift 클러스터 파라미터 `require_SSL`가 `True`로 설정되지 않은 경우 확인이 실패합니다.

TLS는 잠재적 공격자가 person-in-the-middle 또는 유사한 공격을 사용하여 네트워크 트래픽을 도청하거나 조작하는 것을 방지하는 데 사용할 수 있습니다. TLS를 통한 암호화된 연결만 허용되어야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 이해해야 합니다.

이제 Security Hub가 와 통합되었습니다

암호화를 요구하도록 Amazon Redshift 파라미터 그룹을 업데이트하려면 Amazon Redshift 관리 안내서의 파라미터 그룹 수정을 참조하십시오. `require_ssl`를 true로 설정합니다.

[Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-13(5)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `redshift-backup-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값	
`MinRetentionPeriod`	최소 스냅샷 보존 기간(일 수)	Integer	`7~35`	7	

이 제어는 Amazon Redshift 클러스터에 자동 스냅샷이 활성화되어 있고 보존 기간이 지정된 기간 이상인지 확인합니다. 클러스터에서 자동 스냅샷을 사용할 수 없거나 보존 기간이 지정된 기간보다 짧으

면 제어가 실패합니다. 스냅샷 보존 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 7일을 사용합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구할 수 있습니다. 이는 시스템의 복원력을 강화합니다. Amazon Redshift는 기본적으로 주기적인 스냅샷을 찍습니다. 이 제어는 자동 스냅샷이 활성화되고 7일 이상 보관되는지 확인합니다. Amazon Redshift 자동 스냅샷에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 자동 스냅샷을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Amazon Redshift 클러스터의 스냅샷 보존 기간을 업데이트하려면 Amazon Redshift 관리 안내서의 클러스터 수정을 참조하십시오. 백업의 경우 스냅샷 보존 값을 7 이상으로 설정합니다.

[Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `redshift-cluster-audit-logging-enabled` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

- `loggingEnabled = true`(사용자 지정할 수 없음)

이 제어는 Amazon Redshift 클러스터에 감사 로깅이 활성화되어 있는지 여부를 확인합니다.

Amazon Redshift 감사 로깅은 클러스터 내 연결 및 사용자 작업에 대한 추가 정보를 제공합니다. 이 데이터는 Amazon S3에 저장 및 보호될 수 있으며 보안 감사 및 조사에 유용할 수 있습니다. 자세한 내용은 Amazon Redshift 관리 안내서의 데이터베이스 감사 로깅을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Amazon Redshift 클러스터에 대한 감사 로깅을 구성하려면 Amazon Redshift 관리 안내서의 콘솔을 사용하여 감사 구성을 참조하십시오.

[Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2(2), NIST.800-53.r5 SI-2(4), NIST.800-53.r5 SI-2(5)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `redshift-cluster-maintenancesettings-check`

스케줄 유형: 변경이 트리거됨

파라미터:

- `allowVersionUpgrade = true`(사용자 지정할 수 없음)

이 제어는 Amazon Redshift 클러스터에 자동 메이저 버전 업그레이드가 활성화되어 있는지 여부를 확인합니다.

자동 메이저 버전 업그레이드를 활성화하면 유지 관리 기간 중에 Amazon Redshift 클러스터에 대한 최신 메이저 버전 업데이트가 설치됩니다. 이러한 업데이트에는 보안 패치 및 버그 수정이 포함될 수 있습니다. 패치 설치를 최신 상태로 유지하는 것은 시스템 보안의 중요한 단계입니다.

이제 Security Hub가 와 통합되었습니다

에서 이 문제를 해결하려면 Amazon `modify-cluster` Redshift 명령을 사용하여 속성을 설정하십시오`--allow-version-upgrade`. AWS CLI

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

여기서 *`clustername`*은 Amazon Redshift 클러스터의 이름입니다.

[Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다

관련 요구 사항: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > API 프라이빗 액세스

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `redshift-enhanced-vpc-routing-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터에 `EnhancedVpcRouting`가 활성화되었는지 여부를 확인합니다.

향상된 VPC 라우팅은 클러스터와 데이터 저장소 사이의 모든 `COPY` 및 `UNLOAD` 트래픽이 VPC를 통과하도록 강제합니다. 그런 다음 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. 또한 VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

자세한 수정 지침은 Amazon Redshift 관리 안내서의 향상된 VPC 라우팅 활성화를 참조하십시오.

[Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `redshift-default-admin-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터가 관리자 사용자 이름을 기본값에서 변경했는지 여부를 확인합니다. Redshift 클러스터의 관리자 사용자 이름이 `awsuser`로 설정된 경우 이 제어가 실패합니다.

Redshift 클러스터를 만들 때는 기본 관리자 사용자 이름을 고유한 값으로 변경해야 합니다. 기본 사용자 이름은 공개되어 있으므로 구성 시 변경해야 합니다. 기본 사용자 이름을 변경하면 의도하지 않은 액세스의 위험이 줄어듭니다.

이제 Security Hub가 와 통합되었습니다

Amazon Redshift 클러스터가 생성된 후에는 해당 클러스터의 관리자 사용자 이름을 변경할 수 없습니다. 새 클러스터를 만들려면 여기 지침을 따르십시오.

[Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `redshift-default-db-name-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터가 데이터베이스 이름을 기본값에서 변경했는지 여부를 확인합니다. Redshift 클러스터의 데이터베이스 이름이 `dev`로 설정된 경우 제어가 실패합니다.

Redshift 클러스터를 만들 때는 기본 데이터베이스 이름을 고유한 값으로 변경해야 합니다. 기본 이름은 공개되어 있으므로 구성 시 변경해야 합니다. 예를 들어, 잘 알려진 이름이 IAM 정책 조건에 사용되면 의도하지 않은 액세스로 이어질 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Amazon Redshift 클러스터가 생성된 후에는 해당 클러스터의 데이터베이스 이름을 변경할 수 없습니다. 새 클러스터 생성에 대한 지침은 Amazon Redshift 시작 안내서의 Amazon Redshift 시작하기를 참조하십시오.

[Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `redshift-cluster-kms-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터가 저장 시 암호화되었는지 확인합니다. Redshift 클러스터가 저장 시 암호화되지 않거나 암호화 키가 규칙 파라미터에 제공된 키와 다른 경우 제어가 실패합니다.

Amazon Redshift에서는 클러스터의 데이터베이스 암호화를 통해 저장된 데이터를 보호할 수 있습니다. 클러스터에서 암호화를 활성화하면 해당 클러스터와 스냅샷의 데이터 블록 및 시스템 메타데이터가 암호화됩니다. 저장 데이터 암호화는 데이터에 액세스 관리 계층을 추가하므로 권장되는 모범 사례입니다. 저장된 Redshift 클러스터를 암호화하면 권한이 없는 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다.

이제 Security Hub가 와 통합되었습니다

KMS 암호화를 사용하도록 Redshift 클러스터를 수정하려면 Amazon Redshift 관리 안내서의 클러스터 암호화 변경을 참조하십시오.

[Redshift.11] Redshift 클러스터에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `tagged-redshift-cluster` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon Redshift 클러스터에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 클러스터에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 클러스터에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Redshift 클러스터에 태그를 추가하려면 Amazon Redshift 관리 안내서의 Amazon Redshift의 리소스 태그 지정을 참조하십시오.

[Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Redshift::EventSubscription`

AWS Config 규칙: `tagged-redshift-eventsubscription` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon Redshift 클러스터 스냅샷에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 클러스터 스냅샷에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 클러스터 스냅샷에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Redshift 이벤트 알림 구독에 태그를 추가하려면 Amazon Redshift 관리 안내서의 Amazon Redshift의 리소스 태그 지정을 참조하십시오.

[Redshift.13] Redshift 클러스터 스냅샷에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Redshift::ClusterSnapshot`

AWS Config 규칙: `tagged-redshift-clustersnapshot` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon Redshift 클러스터 스냅샷에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 클러스터 스냅샷에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 클러스터 스냅샷에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Redshift 클러스터 스냅샷에 태그를 추가하려면 Amazon Redshift 관리 안내서의 Amazon Redshift의 리소스 태그 지정을 참조하십시오.

[Redshift.14] Redshift 클러스터 서브넷 그룹은 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Redshift::ClusterSubnetGroup`

AWS Config 규칙: `tagged-redshift-clustersubnetgroup` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon Redshift 클러스터 서브넷 그룹에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 클러스터 서브넷 그룹에 태그 키가 없거나 파라미터에 지정된

모든 키가 없는 경우 제어가 실패합니다. `requiredTagKeys` 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 클러스터 서브넷 그룹에 키 태그가 지정되지 않으면 실패합니다. 로 `aws:` 시작하는 시스템 태그는 자동으로 적용되며 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Redshift 클러스터 서브넷 그룹에 태그를 추가하려면 Amazon Redshift 관리 안내서의 Amazon Redshift의 리소스 태그 지정을 참조하십시오.

[Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.

범주: 보호 > 보안 네트워크 구성 > 보안 그룹 구성

심각도: 높음

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: `redshift-unrestricted-port-access`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Redshift 클러스터와 연결된 보안 그룹에 인터넷에서의 클러스터 포트 액세스를 허용하는 수신 규칙 (0.0.0.0/0 또는: :/0) 이 있는지 확인합니다. 보안 그룹 인그레스 규칙이 인터넷을 통한 클러스터 포트 액세스를 허용하면 제어가 실패합니다.

Redshift 클러스터 포트 (/0 접미사가 있는 IP 주소) 에 대한 무제한 인바운드 액세스를 허용하면 무단 액세스 또는 보안 사고가 발생할 수 있습니다. 보안 그룹을 생성하고 인바운드 규칙을 구성할 때는 최소 권한 액세스 원칙을 적용하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

Redshift 클러스터 포트의 수신을 제한된 오리진으로 제한하려면 Amazon VPC 사용 설명서의 보안 그룹 규칙 사용을 참조하십시오. 포트 범위가 Redshift 클러스터 포트와 일치하고 IP 포트 범위가 0.0.0.0/0인 규칙을 업데이트합니다.

Amazon Route 53 제어

이러한 제어는 Route 53 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Route53::HealthCheck`

AWS Config 규칙: `tagged-route53-healthcheck` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon Route 53 상태 확인에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 상태 확인에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 상태 확인에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Route 53 상태 확인에 태그를 추가하려면 Amazon Route 53 개발자 안내서의 이름 지정 및 태그 지정 상태 확인을 참조하십시오.

[Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::Route53::HostedZone`

AWS Config 규칙: `route53-query-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Route 53 퍼블릭 호스팅 영역에 대해 DNS 쿼리 로깅이 활성화되어 있는지 확인합니다. Route 53 퍼블릭 호스팅 영역에 대해 DNS 쿼리 로깅을 활성화하지 않으면 제어가 실패합니다.

Route 53 호스팅 영역에 대한 DNS 쿼리를 로깅하면 DNS 보안 및 규정 준수 요구 사항을 해결하고 가시성을 확보할 수 있습니다. 로그에는 쿼리된 도메인 또는 하위 도메인, 쿼리 날짜 및 시간, DNS 레코드 유형(예: A 또는 AAAA), DNS 응답 코드(예: `NoError` 또는 `ServFail`) 등의 정보가 포함됩니다. DNS 쿼리 로깅이 활성화되면 Route 53은 로그 파일을 Amazon CloudWatch Logs에 게시합니다.

이제 Security Hub가 와 통합되었습니다

Route 53 퍼블릭 호스팅 영역에 대한 DNS 쿼리를 로깅하려면 Amazon Route 53 개발자 안내서의 DNS 쿼리에 대한 로깅 구성을 참조하십시오.

Amazon Simple Storage Service 제어

이러한 제어는 Amazon S3 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/2.1.4, AWS CIS 재단 벤치마크 v1.4.0/2.1.5, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.R5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (4) 7 (9))

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `s3-account-level-public-access-blocks-periodic`

스케줄 유형: 주기적

파라미터:

- `ignorePublicAcls`: `true`(사용자 지정할 수 없음)
- `blockPublicPolicy`: `true`(사용자 지정할 수 없음)
- `blockPublicAcls`: `true`(사용자 지정할 수 없음)
- `restrictPublicBuckets`: `true`(사용자 지정할 수 없음)

이 컨트롤은 이전 Amazon S3 블록 퍼블릭 액세스 설정이 S3 범용 버킷의 계정 수준에서 구성되었는지 여부를 확인합니다. 하나 이상의 블록 퍼블릭 액세스 설정이 로 `false` 설정된 경우 제어가 실패합니다.

설정 중 하나라도 `false`으로 설정되어 있거나 설정이 구성되지 않은 경우 제어가 실패합니다.

Amazon S3 퍼블릭 액세스 블록은 객체가 퍼블릭 액세스를 절대 갖지 않도록 전체 AWS 계정 또는 개별 S3 버킷 수준에서 제어를 제공하도록 설계되었습니다. 액세스 제어 목록(ACL), 버킷 정책 또는 둘 다를 통해 버킷 및 객체에 퍼블릭 액세스 권한이 부여됩니다.

S3 버킷에 대한 퍼블릭 액세스를 가능하도록 하려는 경우가 아니면 계정 수준의 Amazon S3 퍼블릭 액세스 차단 기능을 구성해야 합니다.

자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 퍼블릭 액세스 차단 사용을 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Amazon S3 퍼블릭 액세스 차단을 활성화하려면 Amazon 심플 스토리지 서비스 사용 설명서의 계정에 대한 블록 퍼블릭 액세스 설정 구성을 참조하십시오. AWS 계정

[S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-bucket-public-read-prohibited`

스케줄 유형: 주기적이며 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷이 공개 읽기 액세스를 허용하는지 여부를 확인합니다. 퍼블릭 액세스 차단 설정, 버킷 정책 및 버킷 ACL(액세스 제어 목록)을 평가합니다. 버킷이 공개 읽기 액세스를 허용하면 제어가 실패합니다.

일부 사용 사례에서는 인터넷의 모든 사용자가 S3 버킷에서 읽을 수 있어야 합니다. 그러나 이러한 상황은 드뭅니다. 데이터의 무결성과 보안을 보장하기 위해 S3 버킷은 공개적으로 읽을 수 없습니다.

이제 Security Hub가 와 통합되었습니다

Amazon S3 버킷에 대한 퍼블릭 읽기 액세스를 차단하려면 Amazon 심플 스토리지 서비스 사용 설명서의 S3 버킷에 대한 퍼블릭 액세스 차단 설정 구성을 참조하십시오.

[S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5

AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-bucket-public-write-prohibited`

스케줄 유형: 주기적이며 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷이 공개 쓰기 액세스를 허용하는지 여부를 확인합니다. 퍼블릭 액세스 차단 설정, 버킷 정책 및 버킷 ACL(액세스 제어 목록)을 평가합니다. 버킷이 공개 쓰기 액세스를 허용하면 제어가 실패합니다.

일부 사용 사례에서는 인터넷의 모든 사용자가 S3 버킷에 쓸 수 있어야 합니다. 그러나 이러한 상황은 드뭅니다. 데이터의 무결성과 보안을 보장하기 위해 S3 버킷은 공개적으로 쓸 수 없습니다.

이제 Security Hub가 와 통합되었습니다

Amazon S3 버킷에 대한 퍼블릭 쓰기 액세스를 차단하려면 Amazon 심플 스토리지 서비스 사용 설명서의 S3 버킷에 대한 퍼블릭 액세스 차단 설정 구성을 참조하세요.

[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/2.1.1, AWS CIS 재단 벤치마크 v1.4.0/2.1.2, PCI DSS v3.2.1/4.1, NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.R5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2)), NIST.800-53.r5 SI-7 (6)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-bucket-ssl-requests-only`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon S3 범용 버킷에 SSL 사용 요청을 요구하는 정책이 있는지 확인합니다. 버킷 정책에 SSL 사용 요청이 필요하지 않으면 제어가 실패합니다.

S3 버킷에는 S3 리소스 정책에 있는 HTTPS를 통한 데이터 전송만 허용하도록 모든 요청(`Action: S3:*`)을 요구하는 정책이 있어야 하며 조건 키 `aws:SecureTransport`으로 표시됩니다.

이제 Security Hub가 와 통합되었습니다

비보안 전송을 거부하도록 Amazon S3 버킷 정책을 업데이트하려면 Amazon 심플 스토리지 서비스 사용 설명서의 Amazon S3 콘솔을 사용하여 버킷 정책 추가를 참조하십시오.

다음 정책에 있는 것과 유사한 정책 설명을 추가하십시오. `DOC-EXAMPLE-BUCKET`를 수정하려는 버킷의 이름으로 바꿉니다.

```
{
    "Id": "ExamplePolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "Bool": {
                     "aws:SecureTransport": "false"
                }
            },
```

```
            "Principal": "*"
        }
    ]
}
```

자세한 내용은 AWS Config 규칙 s3- 를 준수하려면 어떤 S3 버킷 정책을 사용해야 합니까? 를 참조하십시오. bucket-ssl-requests-only AWS 공식 지식 센터에서.

[S3.6] S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 액세스 관리 > 민감한 API 작업 작업 제한

심각도: 높음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-bucket-blacklisted-actions-prohibited`

스케줄 유형: 변경이 트리거됨

파라미터:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl`(사용자 지정할 수 없음)

이 제어는 Amazon S3 범용 버킷 정책이 다른 AWS 계정 사람의 보안 주체가 S3 버킷의 리소스에 대해 거부된 작업을 수행하는 것을 방지하는지 확인합니다. 버킷 정책에서 다른 보안 주체의 이전 작업 중 하나 이상을 허용하는 경우 제어가 실패합니다. AWS 계정

최소 권한 액세스를 구현하는 것은 보안 위험과 오류 또는 악의적 의도의 영향을 줄이는 데 필수적입니다. S3 버킷 정책에서 외부 계정으로부터의 액세스를 허용하는 경우 내부자 위협이나 공격자에 의한 데이터 유출이 발생할 수 있습니다.

`blacklistedactionpatterns` 파라미터를 사용하면 S3 버킷의 규칙을 성공적으로 평가할 수 있습니다. 파라미터는 `blacklistedactionpatterns` 목록에 포함되지 않은 작업 패턴에 대해 외부 계정에 대한 액세스 권한을 부여합니다.

이제 Security Hub가 와 통합되었습니다

Amazon S3 버킷 정책을 업데이트하여 권한을 제거하려면 Amazon Simple Storage Service 사용 설명서의 Amazon S3 콘솔을 사용하여 버킷 정책 추가를 참조하십시오.

버킷 정책 편집 페이지의 정책 편집 텍스트 상자에서 다음 작업 중 하나를 수행하십시오.

- 거부된 작업에 대한 다른 AWS 계정 액세스 권한을 다른 사람에게 부여하는 문을 삭제하십시오.
- 명령문에서 허용된 거부된 작업을 제거합니다.

[S3.7] S3 범용 버킷은 지역 간 복제를 사용해야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: PCI DSS v3.2.1/2.2, NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-36(2), NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: **`s3-bucket-cross-region-replication-enabled`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon S3 범용 버킷에 지역 간 복제가 활성화되어 있는지 확인합니다. 버킷에 교차 리전 복제가 활성화되어 있지 않으면 제어가 실패합니다.

복제는 같거나 다른 버킷에 있는 객체를 비동기식으로 자동 복사하는 것입니다. AWS 리전복제는 새로 생성된 객체와 객체 업데이트를 소스 버킷에서 대상 버킷으로 복사합니다. AWS 모범 사례에서는 동일한 AWS 계정소유의 소스 및 대상 버킷에 대한 복제를 권장합니다. 가용성 외에도 다른 시스템 보안 강화 설정을 고려해야 합니다.

이제 Security Hub가 와 통합되었습니다

S3 버킷에서 크로스 리전 복제를 활성화하려면 Amazon Simple Storage Service 사용 설명서의 동일한 계정이 소유한 소스 및 대상 버킷에 대한 복제 구성을 참조하십시오. 소스 버킷의 경우 버킷의 모든 객체에 적용을 선택합니다.

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/2.1.4, CIS AWS 재단 벤치마크 v1.4.0/2.1.5, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.R5 AC-3 (7), NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 높음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-bucket-level-public-access-prohibited`

스케줄 유형: 변경이 트리거됨

파라미터:

- `excludedPublicBuckets`(사용자 지정할 수 없음) - 알려진 허용된 퍼블릭 S3 버킷 이름을 쉼표로 구분한 목록입니다.

이 제어는 Amazon S3 범용 버킷이 버킷 수준에서 퍼블릭 액세스를 차단하는지 여부를 확인합니다. 다음 설정 중 하나라도 로 설정된 경우 제어가 실패합니다`false`.

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`

- `restrictPublicBuckets`

S3 버킷 수준에서의 퍼블릭 액세스 차단은 객체에 퍼블릭 액세스가 없도록 제어하는 기능을 제공합니다. 액세스 제어 목록(ACL), 버킷 정책 또는 둘 다를 통해 버킷 및 객체에 퍼블릭 액세스 권한이 부여됩니다.

S3 버킷에 대한 퍼블릭 액세스를 가능하도록 하려는 경우가 아니면 버킷 수준의 Amazon S3 퍼블릭 액세스 차단 기능을 구성해야 합니다.

이제 Security Hub가 와 통합되었습니다

버킷 수준에서 퍼블릭 액세스를 제거하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 참조하십시오.

[S3.9] S3 범용 버킷은 서버 액세스 로깅을 활성화해야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-bucket-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷에 대해 서버 액세스 로깅이 활성화되었는지 여부를 확인합니다. 서버 액세스 로깅이 활성화되지 않은 경우 제어가 실패합니다. 로깅을 사용하도록 설정하면 Amazon S3는 소스 버킷에 대한 액세스 로그를 선택한 대상 버킷으로 전달합니다. 대상 버킷은 원본 버킷과 AWS 리

전 동일해야 하며 기본 보존 기간을 구성하지 않아야 합니다. 대상 로깅 버킷에는 서버 액세스 로깅을 활성화할 필요가 없으며 이 버킷에 대한 조사 결과를 표시하지 않아야 합니다.

서버 액세스 로깅은 버킷에 대한 요청에 대한 자세한 기록을 제공합니다. 서버 액세스 로그는 보안 및 액세스 감사에 도움이 될 수 있습니다. 자세한 내용은 Amazon S3 보안 모범 사례: Amazon S3 서버 액세스 로깅 활성화를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Amazon S3 서버 액세스 로깅을 활성화하려면 Amazon S3 사용 설명서의 Amazon S3 서버 액세스 로깅 활성화를 참조하십시오.

[S3.10] 버전 관리가 활성화된 S3 범용 버킷은 수명 주기 구성을 가져야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. Security Hub는 2024년 4월에 AWS 기본 보안 모범 사례 표준에서 이 제어 기능을 제거했지만 여전히 NIST SP 800-53 Rev. 5 표준에는 포함되어 있습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-version-lifecycle-policy-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon S3 범용 버전 관리 버킷에 수명 주기 구성이 있는지 여부를 확인합니다. 버킷에 수명 주기 구성이 없으면 제어가 실패합니다.

Amazon S3가 객체 수명 주기 동안 수행할 작업을 정의하는 데 도움이 되도록 S3 버킷의 수명 주기 구성을 생성하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

Amazon S3 버킷의 수명 주기 구성에 대한 자세한 내용은 버킷의 수명 주기 구성 설정 및 스토리지 수명 주기 관리를 참조하십시오.

[S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. Security Hub는 2024년 4월에 AWS 기본 보안 모범 사례 표준에서 이 제어 기능을 제거했지만 여전히 NIST SP 800-53 Rev. 5 표준에 포함되어 있습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(4)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-event-notifications-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`eventTypes`	선호하는 S3 이벤트 유형 목록	EnumList (최대 28개 항목)	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpira`	기본값 없음

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
			tion:Delete, s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:Object	

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
			Removed:Delete, s3:ObjectRemoved:DeleteMarkerCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replic	

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
			ation:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent	

이 컨트롤은 Amazon S3 범용 버킷에서 S3 이벤트 알림이 활성화되었는지 여부를 확인합니다. 버킷에서 S3 이벤트 알림을 활성화하지 않으면 제어가 실패합니다. eventTypes파라미터에 사용자 지정 값을 제공하는 경우 지정된 유형의 이벤트에 대해 이벤트 알림이 활성화된 경우에만 제어가 전달됩니다.

S3 이벤트 알림을 활성화하면 S3 버킷에 영향을 미치는 특정 이벤트가 발생할 때 알림을 받게 됩니다. 예를 들어 개체 생성, 개체 제거, 개체 복원에 대한 알림을 받을 수 있습니다. 이러한 알림은 무단 데이터 액세스로 이어질 수 있는 우발적이거나 의도적인 수정에 대해 관련 팀에 경고할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

S3 버킷 및 객체 변경 감지에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 이벤트 알림을 참조하십시오.

[S3.12] ACL은 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 됩니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-bucket-acl-prohibited`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷이 액세스 제어 목록 (ACL) 과 함께 사용자 권한을 제공하는지 여부를 확인합니다. 버킷에 대한 사용자 액세스를 관리하도록 ACL이 구성된 경우 제어가 실패합니다.

ACL은 IAM 이전의 레거시 액세스 제어 메커니즘입니다. ACL 대신 S3 버킷 정책 또는 AWS Identity and Access Management (IAM) 정책을 사용하여 S3 버킷에 대한 액세스를 관리하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

이 제어를 통과하려면 S3 버킷에 대한 ACL을 비활성화해야 합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 객체 소유권 제어 및 버킷에 대해 ACL 비활성화를 참조하십시오.

S3 버킷 정책을 생성하려면 Amazon S3 콘솔을 사용하여 버킷 정책 추가를 참조하십시오. S3 버킷에 IAM 사용자 정책을 생성하려면 사용자 정책을 사용한 버킷 액세스 제어를 참조하십시오.

[S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 보호 > 데이터 보호

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-lifecycle-policy-check`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`targetTransitionDays`	객체 생성 후 객체를 지정된 스토리지 클래스로 전환하는 시기까지의 일수	Integer	`1~36500`	기본값 없음
`targetExpirationDays`	객체 생성 후 객체가 삭제되는 시기까지의 일수	Integer	`1~36500`	기본값 없음
`targetTransitionStorageClass`	대상 S3 스토리지 클래스 유형	Enum	`STANDARD_IA, INTELLIGENT_TIERING, ONEZONE_I`	기본값 없음

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
			A, GLACIER, GLACIER_IR, DEEP_ARCHIVE	

이 컨트롤은 Amazon S3 범용 버킷에 수명 주기 구성이 있는지 여부를 확인합니다. 버킷에 수명 주기 구성이 없는 경우 제어가 실패합니다. 위 파라미터 중 하나 이상에 사용자 지정 값을 제공하는 경우 정책에 지정된 스토리지 클래스, 삭제 시간 또는 전환 시간이 포함된 경우에만 제어가 통과합니다.

S3 버킷의 수명 주기 구성을 생성하면 객체 수명 주기 동안 Amazon S3가 수행할 작업이 정의됩니다. 예를 들어, 객체를 다른 스토리지 클래스로 전환하거나, 보관하거나, 지정된 기간 후에 삭제할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Amazon S3 버킷의 수명 주기 정책 구성에 대한 자세한 내용은 Amazon S3 사용 설명서의 버킷에 수명 주기 구성 설정 및 스토리지 수명 주기 관리를 참조하십시오.

[S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

관련 요구 사항: NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5)

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: `s3-bucket-versioning-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon S3 범용 버킷에 버전 관리가 활성화되어 있는지 여부를 확인합니다. 버킷의 버전 관리가 일시 중단되면 제어가 실패합니다.

버전 관리는 동일한 S3 버킷에 객체의 여러 변형을 유지합니다. 버전 관리를 사용하여 S3 버킷에 저장된 객체의 이전 버전을 보존, 검색 및 복원할 수 있습니다. S3 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애 모두로부터 복구하는 데 도움이 됩니다.

> **Tip**
>
> 버전 관리로 인해 버킷의 객체 수가 증가하면 규칙에 따라 버전이 지정된 객체를 자동으로 보관 또는 삭제하도록 수명 주기 구성을 설정할 수 있습니다. 자세한 내용을 알아보려면 버전이 지정된 객체에 대한 Amazon S3 수명 주기 관리 참조하십시오.

이제 Security Hub가 와 통합되었습니다

S3 버킷에서 버전 관리를 사용하려면 Amazon S3 사용 설명서의 버킷 버전 관리 활성화를 참조하십시오.

[S3.15] S3 범용 버킷에는 객체 잠금이 활성화되어 있어야 합니다.

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

관련 요구 사항: NIST.800-53.r5 CP-6(2)

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: **s3-bucket-default-lock-enabled**

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`mode`	S3 객체 잠금 보존 모드	Enum	`GOVERNANCE` , `COMPLIANCE`	기본값 없음

이 컨트롤은 Amazon S3 범용 버킷에 객체 잠금이 활성화되어 있는지 확인합니다. 버킷에 대해 객체 잠금이 활성화되지 않은 경우 제어가 실패합니다. `mode` 파라미터에 사용자 지정 값을 제공하면 S3 객체 잠금이 지정된 보존 모드를 사용하는 경우에만 제어가 통과합니다.

S3 오브젝트 잠금을 사용하여 write-once-read-many (WORM) 모델을 사용하여 객체를 저장할 수 있습니다. 객체 잠금은 S3 버킷의 객체가 고정된 시간 동안 또는 무기한 삭제되거나 덮어쓰이는 것을 방지하는 데 도움이 됩니다. S3 객체 잠금을 사용하면 WORM 스토리지가 필요한 규제 요구 사항을 충족하거나 객체 변경 및 삭제에 대한 보호 계층을 추가할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

신규 및 기존 S3 버킷의 객체 잠금을 구성하려면 Amazon S3 사용 설명서의 S3 객체 잠금 구성을 참조하세요.

[S3.17] S3 범용 버킷은 저장 시 다음을 사용하여 암호화해야 합니다. AWS KMS keys

> **Important**
>
> 2024년 3월 12일에 이 컨트롤의 제목이 표시된 제목으로 변경되었습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

관련 요구 사항: NIST.800-53.r5 SC-12(2), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 CA-9(1), NIST.800-53.r5 SI-7(6), NIST.800-53.r5 AU-9

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: **`s3-default-encryption-kms`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon S3 범용 버킷이 AWS KMS key (SSE-KMS 또는 DSSE-KMS) 로 암호화되었는지 여부를 확인합니다. 버킷을 기본 암호화 (SSE-S3) 로 암호화하면 제어가 실패합니다.

서버 측 암호화(SSE)는 데이터를 받는 애플리케이션 또는 서비스에 의해 해당 대상에서 데이터를 암호화하는 것입니다. 달리 지정하지 않는 한, S3 버킷은 서버 측 암호화에 기본적으로 Amazon S3 관리형 키(SSE-S3)를 사용합니다. 하지만 제어를 강화하기 위해 대신 AWS KMS keys (SSE-KMS 또는 DSSE-KMS) 를 통한 서버 측 암호화를 사용하도록 버킷을 구성할 수 있습니다. Amazon S3는 데이터 센터의 디스크에 데이터를 쓸 때 객체 수준에서 데이터를 암호화하고, AWS 데이터에 액세스할 때 자동으로 복호화합니다.

이제 Security Hub가 와 통합되었습니다

SSE-KMS를 사용하여 S3 버킷을 암호화하려면 Amazon S3 사용 설명서의 AWS KMS (SSE-KMS) 를 사용하여 서버 측 암호화 지정을 참조하십시오. DSSE-KMS를 사용하여 S3 버킷을 암호화하려면 Amazon S3 사용 설명서의 (DSSE-KMS) 를 사용하여 이중 계층 서버 측 암호화 지정을 참조하십시오. AWS KMS keys

[S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::S3::AccessPoint`

AWS Config 규칙: **`s3-access-point-public-access-blocks`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되었는지 확인합니다. 액세스 포인트에 대해 퍼블릭 액세스 차단 설정을 활성화하지 않으면 제어가 실패합니다.

Amazon S3 퍼블릭 액세스 차단 기능을 사용하면 계정, 버킷 및 액세스 포인트 수준의 세 가지 수준에서 S3 리소스에 대한 액세스를 관리할 수 있습니다. 각 수준의 설정을 독립적으로 구성할 수 있으므로 데이터에 대해 다양한 수준의 퍼블릭 액세스 제한을 적용할 수 있습니다. 액세스 포인트 설정은 상위 수준(액세스 포인트에 할당된 계정 수준 또는 버킷)에서 더 제한적인 설정을 개별적으로 재정의할 수 없습니다. 대신 액세스 포인트 수준의 설정은 추가적이므로 다른 수준의 설정을 보완하고 그 설정과 연동합니다. S3 액세스 포인트를 공개적으로 액세스할 수 있도록 하려는 경우가 아니라면 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

이제 Security Hub가 와 통합되었습니다

Amazon S3에서는 현재 액세스 포인트가 생성된 후 액세스 포인트의 퍼블릭 액세스 차단 설정을 변경하도록 지원하지 않습니다. 신규 액세스 포인트를 생성하면 기본적으로 모든 퍼블릭 액세스 차단 설정이 활성화되어 있습니다. 특정 설정을 사용 중지해야 하는 경우가 아니면 모든 설정을 그대로 유지하는 것이 좋습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 액세스 포인트에 대한 퍼블릭 액세스 관리를 참조하세요.

[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.

관련 요구 사항: CIS AWS 재단 벤치마크 v3.0.0/2.1.2, CIS AWS 재단 벤치마크 v1.4.0/2.1.3, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 SC-5 SC-5 (2)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: **`s3-bucket-mfa-delete-enabled`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon S3 범용 버전 관리 버킷에서 멀티 팩터 인증 (MFA) 삭제가 활성화되었는지 여부를 확인합니다. 버킷에서 MFA Delete가 활성화되지 않은 경우 제어가 실패합니다. 컨트롤은 수명 주기 구성이 있는 버킷에 대한 검색 결과를 생성하지 않습니다.

Amazon S3 버킷에서 S3 버전 관리를 사용하는 경우 선택적으로 MFA Delete를 사용 설정하도록 버킷을 구성하여 다른 보안 계층을 추가할 수 있습니다. 이렇게 하면 버킷 소유자가 버전을 삭제하거나 버킷의 버전 관리 상태를 변경하는 모든 요청에 두 가지 형식의 인증을 포함해야 합니다. MFA Delete는 보안 인증이 손상된 경우에 대비하여 보안을 강화합니다. 또한 MFA Delete는 삭제 작업을 시작하는 사용자에게 MFA 코드를 통해 MFA 디바이스의 물리적 소유를 증명할 것을 요구하고 삭제 작업에 추가 마찰 및 보안 계층을 추가합니다. 따라서 실수로 인한 버킷 삭제를 방지하는 데 도움이 될 수 있습니다.

> **Note**
>
> MFA Delete를 사용하려면 종속성으로 버킷 버전 관리가 필요합니다. 버킷 버전 관리는 동일 버킷 내에 여러 개의 S3 객체 변형을 보유하는 방법입니다. 또한 루트 사용자로 로그인한 버킷 소유자만 MFA Delete를 활성화하고 S3 버킷에서 삭제 작업을 수행할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

S3 버전 관리를 활성화하고 버킷에서 MFA Delete를 구성하려면 Amazon Simple Storage Service 사용 설명서의 MFA Delete 구성을 참조하세요.

[S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.

관련 요구 사항: CIS 재단 벤치마크 v3.0.0/3.8 AWS

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: **`cloudtrail-all-write-s3-data-event-check`**

스케줄 유형: 주기적

파라미터: 없음

이 AWS 계정 컨트롤은 Amazon S3 버킷에 대한 모든 쓰기 데이터 이벤트를 기록하는 AWS CloudTrail 다중 지역 트레일이 하나 이상 있는지 확인합니다. 계정에 S3 버킷에 대한 쓰기 데이터 이벤트를 기록하는 멀티 리전 트레일이 없으면 제어가 실패합니다.

, `GetObject` `DeleteObject` `PutObject`, 및 같은 S3 객체 수준 작업을 데이터 이벤트라고 합니다. 기본적으로 은 데이터 이벤트를 기록하지 CloudTrail 않지만 S3 버킷의 데이터 이벤트를 기록하도록 트레일을 구성할 수 있습니다. 쓰기 데이터 이벤트에 대한 객체 수준 로깅을 활성화하면 S3 버킷 내의 각 개별 객체 (파일) 액세스를 로깅할 수 있습니다. 객체 수준 로깅을 활성화하면 Amazon Events를 사용하여 데이터 규정 준수 요구 사항을 충족하고, 포괄적인 보안 분석을 수행하고, 사용자 행동의 특정 패턴을 모니터링하고 AWS 계정, S3 버킷 내 객체 수준 API 활동에 대한 조치를 취하는 데 도움이 될 수 있습니다. CloudWatch 이 컨트롤은 모든 S3 버킷에 대해 쓰기 전용 또는 모든 유형의 데이터 이벤트를 기록하는 다중 지역 트레일을 구성하면 `PASSED` 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

S3 버킷에 대한 객체 수준 로깅을 활성화하려면 Amazon Simple Storage Service 사용 설명서의 S3 버킷 및 객체에 대한 CloudTrail 이벤트 로깅 활성화를 참조하십시오.

[S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.

관련 요구 사항: CIS 재단 벤치마크 v3.0.0/3.9 AWS

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: **`cloudtrail-all-read-s3-data-event-check`**

스케줄 유형: 주기적

파라미터: 없음

이 AWS 계정 컨트롤은 Amazon S3 버킷에 대한 모든 읽기 데이터 이벤트를 기록하는 AWS CloudTrail 다중 지역 트레일이 하나 이상 있는지 확인합니다. 계정에 S3 버킷에 대한 읽기 데이터 이벤트를 기록하는 멀티 리전 트레일이 없으면 제어가 실패합니다.

, `GetObject` `DeleteObject` `PutObject`, 및 같은 S3 객체 수준 작업을 데이터 이벤트라고 합니다. 기본적으로 은 데이터 이벤트를 기록하지 CloudTrail 않지만 S3 버킷의 데이터 이벤트를 기록하도록

트레일을 구성할 수 있습니다. 읽기 데이터 이벤트에 대한 객체 수준 로깅을 활성화하면 S3 버킷 내의 각 개별 객체 (파일) 액세스를 로깅할 수 있습니다. 객체 수준 로깅을 활성화하면 Amazon Events를 사용하여 데이터 규정 준수 요구 사항을 충족하고, 포괄적인 보안 분석을 수행하고, 사용자 행동의 특정 패턴을 모니터링하고 AWS 계정, S3 버킷 내 객체 수준 API 활동에 대한 조치를 취하는 데 도움이 될 수 있습니다. CloudWatch 이 컨트롤은 모든 S3 버킷에 대해 읽기 전용 또는 모든 유형의 데이터 이벤트를 기록하는 다중 지역 트레일을 구성하면 `PASSED` 결과를 생성합니다.

이제 Security Hub가 와 통합되었습니다

S3 버킷에 대한 객체 수준 로깅을 활성화하려면 Amazon Simple Storage Service 사용 설명서의 S3 버킷 및 객체에 대한 CloudTrail 이벤트 로깅 활성화를 참조하십시오.

아마존 SageMaker 컨트롤

이러한 컨트롤은 SageMaker 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

관련 요구 사항: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::SageMaker::NotebookInstance`

AWS Config 규칙: `sagemaker-notebook-no-direct-internet-access`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 SageMaker 노트북 인스턴스에 대한 직접 인터넷 액세스가 비활성화되었는지 여부를 확인합니다. `DirectInternetAccess`필드가 노트북 인스턴스에 활성화되어 있는 경우 제어가 실패합니다.

VPC 없이 SageMaker 인스턴스를 구성하면 기본적으로 인스턴스에서 직접 인터넷 액세스가 활성화됩니다. VPC로 인스턴스를 구성하고 기본 설정을 비활성화-VPC를 통해 인터넷에 액세스로 변경해야 합니다. 노트북에서 모델을 훈련하거나 호스팅하려면 인터넷 액세스가 필요합니다. 인터넷 액세스를 활성화하려면 VPC에 인터페이스 엔드포인트 (AWS PrivateLink) 또는 NAT 게이트웨이와 아웃바운드 연결을 허용하는 보안 그룹이 있어야 합니다. 노트북 인스턴스를 VPC의 리소스에 연결하는 방법에 대한 자세한 내용은 Amazon 개발자 안내서의 VPC의 리소스에 노트북 인스턴스 연결을 참조하십시오. SageMaker 또한 SageMaker 구성에 대한 액세스가 승인된 사용자로만 제한되도록 해야 합니다. 사용자가 SageMaker 설정 및 리소스를 변경할 수 있도록 허용하는 IAM 권한을 제한하십시오.

이제 Security Hub가 와 통합되었습니다

노트북 인스턴스를 생성한 후에는 인터넷 액세스 설정을 변경할 수 없습니다. 대신 인터넷 액세스가 차단된 인스턴스를 중지, 삭제하고 다시 만들 수 있습니다. 인터넷에 직접 액세스할 수 있는 노트북 인스턴스를 삭제하려면 Amazon SageMaker 개발자 안내서의 노트북 인스턴스를 사용하여 모델 구축: 정리를 참조하십시오. 인터넷 액세스를 거부하는 노트북 인스턴스를 다시 생성하려면 노트북 인스턴스 생성을 참조하십시오. 네트워크, 직접 인터넷 액세스에서 비활성화 - VPC를 통해 인터넷 액세스를 선택합니다.

[SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 높음

리소스 유형: `AWS::SageMaker::NotebookInstance`

AWS Config 규칙: `sagemaker-notebook-instance-inside-vpc`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon SageMaker 노트북 인스턴스가 사용자 지정 가상 사설 클라우드 (VPC) 내에서 시작되었는지 확인합니다. SageMaker 노트북 인스턴스가 사용자 지정 VPC 내에서 시작되지 않거나 서비스 VPC에서 시작된 경우 이 제어가 실패합니다 SageMaker .

서브넷은 VPC 내의 IP 주소 범위입니다. 인프라의 안전한 네트워크 보호를 위해 가능하면 리소스를 사용자 지정 VPC에 보관하는 것이 좋습니다. Amazon VPC는 사용자 전용 가상 네트워크입니다. AWS 계정 Amazon VPC를 사용하면 SageMaker Studio 및 노트북 인스턴스의 네트워크 액세스 및 인터넷 연결을 제어할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

노트북 인스턴스를 만든 후에는 VPC 설정을 변경할 수 없습니다. 대신 인스턴스를 중지, 삭제 및 다시 만들 수 있습니다. 지침은 Amazon SageMaker 개발자 안내서의 노트북 인스턴스를 사용하여 모델 구축: 정리를 참조하십시오.

[SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6(10), NIST.800-53.r5 AC-6(2)

범주: 보호 > 보안 액세스 관리 > 루트 사용자 액세스 제한

심각도: 높음

리소스 유형: `AWS::SageMaker::NotebookInstance`

AWS Config 규칙: `sagemaker-notebook-instance-root-access-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 Amazon SageMaker 노트북 인스턴스에 대한 루트 액세스가 켜져 있는지 여부를 확인합니다. SageMaker 노트북 인스턴스에 대한 루트 액세스가 켜져 있는 경우 제어가 실패합니다.

최소 권한 원칙을 준수하기 위해, 의도치 않게 권한을 과도하게 프로비저닝하지 않도록 인스턴스 리소스에 대한 루트 액세스를 제한하는 것이 권장되는 보안 모범 사례입니다.

이제 Security Hub가 와 통합되었습니다

SageMaker 노트북 인스턴스에 대한 루트 액세스를 제한하려면 Amazon SageMaker 개발자 안내서의 SageMaker 노트북 인스턴스에 대한 루트 액세스 제어를 참조하십시오.

[SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.

관련 요구 사항: NIST.800-53.R5 CP-10, NIST.800-53.R5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SA-13

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::SageMaker::EndpointConfig`

AWS Config 규칙: `sagemaker-endpoint-config-prod-instance-count`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 Amazon SageMaker 엔드포인트의 프로덕션 변형의 초기 인스턴스 수가 1보다 큰지 여부를 확인합니다. 엔드포인트의 프로덕션 변형에 초기 인스턴스가 1개만 있는 경우 제어가 실패합니다.

인스턴스 수가 1보다 큰 프로덕션 변형을 실행하면 에서 다중 AZ 인스턴스 중복성을 관리할 수 있습니다. SageMaker 여러 가용 영역에 리소스를 배포하는 것은 아키텍처 내에서 고가용성을 제공하기 위한 AWS 모범 사례입니다. 고가용성은 보안 사고로부터 복구하는 데 도움이 됩니다.

> **Note**
>
> 이 제어는 인스턴스 기반 엔드포인트 구성에만 적용됩니다.

이제 Security Hub가 와 통합되었습니다

엔드포인트 구성의 파라미터에 대한 자세한 내용은 Amazon SageMaker 개발자 안내서의 엔드포인트 구성 생성을 참조하십시오.

AWS Secrets Manager 제어:

이러한 제어는 Secrets Manager 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[SecretsManager.1] Secrets Manager 비밀번호에는 자동 로테이션이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15)

범주: 보호 > 보안 개발

심각도: 중간

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config 규칙: `secretsmanager-rotation-enabled-check`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`maximumAllowedRotationFrequency`	보안 암호 교체 빈도에 허용되는 최대 일수	Integer	`1~365`	기본값 없음

이 AWS Secrets Manager 컨트롤은 에 저장된 비밀이 자동 순환으로 구성되어 있는지 확인합니다. 암호가 자동 교체로 구성되지 않은 경우 제어가 실패합니다. `maximumAllowedRotationFrequency` 파라미터에 사용자 지정 값을 제공하는 경우 지정된 시간 내에 보안 암호가 자동으로 교체되는 경우에만 제어가 통과합니다.

Secrets Manager는 조직의 보안 태세를 개선하는 데 도움이 됩니다. 암호에는 데이터베이스 보안 인증, 비밀번호, 타사 API 키가 포함됩니다. Secrets Manager를 사용하여 암호를 중앙에 저장하고, 암호를 자동으로 암호화하고, 암호에 대한 액세스를 제어하고, 암호를 안전하고 자동으로 교체할 수 있습니다.

Secrets Manager는 암호를 교체할 수 있습니다. 교체를 통해 장기 암호를 단기 암호로 대체할 수 있습니다. 암호를 교체하면 권한이 없는 사용자가 손상된 암호를 사용할 수 있는 기간이 제한됩니다. 이러한 이유 때문에 보안 암호는 자주 교체해야 합니다. 회전에 대해 자세히 알아보려면 사용 설명서의 AWS Secrets Manager 암호AWS Secrets Manager 교체를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Secrets Manager 암호에 대한 자동 교체를 켜려면 사용 AWS Secrets Manager 설명서의 콘솔을 사용하여 AWS Secrets Manager 암호에 대한 자동 교체 설정을 참조하십시오. 순환 AWS Lambda 기능을 선택하고 구성해야 합니다.

[SecretsManager.2] 자동 순환으로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15)

범주: 보호 > 보안 개발

심각도: 중간

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config 규칙: `secretsmanager-scheduled-rotation-success-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 순환 일정에 따라 AWS Secrets Manager 암호가 성공적으로 순환되었는지 여부를 확인합니다. `RotationOccurringAsScheduled` 이 `false`이면 제어는 실패합니다. 제어는 교체가 설정되어 있는 암호만 평가합니다.

Secrets Manager는 조직의 보안 태세를 개선하는 데 도움이 됩니다. 암호에는 데이터베이스 보안 인증, 비밀번호, 타사 API 키가 포함됩니다. Secrets Manager를 사용하여 암호를 중앙에 저장하고, 암호를 자동으로 암호화하고, 암호에 대한 액세스를 제어하고, 암호를 안전하고 자동으로 교체할 수 있습니다.

Secrets Manager는 암호를 교체할 수 있습니다. 교체를 통해 장기 암호를 단기 암호로 대체할 수 있습니다. 암호를 교체하면 권한이 없는 사용자가 손상된 암호를 사용할 수 있는 기간이 제한됩니다. 이러한 이유 때문에 보안 암호는 자주 교체해야 합니다.

암호가 자동으로 교체되도록 구성하는 것 외에도 순환 일정에 따라 암호가 성공적으로 교체되도록 해야 합니다.

교체에 대해 자세히 알아보려면 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager 암호 교체를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

자동 교체가 실패할 경우 Secrets Manager에서 구성 오류가 발생했을 수 있습니다. Secret Manager에서 보안 암호를 교체하려면 해당 보안 암호를 소유하고 있는 데이터베이스 또는 서비스와의 상호 작용 방식을 정의하는 Lambda 함수를 사용해야 합니다.

암호 순환과 관련된 일반적인 오류를 진단하고 수정하는 데 도움이 필요하면 AWS Secrets Manager 사용 설명서의 암호 AWS Secrets Manager 순환 문제 해결을 참조하십시오.

[SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config 규칙: `secretsmanager-secret-unused`

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`unusedForDays`	보안 암호를 사용하지 않은 상태로 유지할 수 있는 최대 일수	Integer	`1~365`	`90`

이 컨트롤은 지정된 기간 내에 AWS Secrets Manager 비밀에 액세스되었는지 여부를 확인합니다. 보안 암호를 지정된 기간 이후에 사용하지 않으면 제어가 실패합니다. 액세스 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 90일을 사용합니다.

사용하지 않는 암호를 삭제하는 것은 암호를 교체하는 것만큼이나 중요합니다. 사용하지 않는 암호는 더 이상 해당 암호에 액세스할 필요가 없는 이전 사용자에 의해 악용될 수 있습니다. 또한 더 많은 사용자가 암호에 액세스할 수 있게 되면 누군가가 이를 잘못 처리하여 승인되지 않은 엔터티에 유출했을 수 있으며, 이로 인해 남용의 위험이 커집니다. 사용하지 않는 암호를 삭제하면 더 이상 필요하지 않은 사

용자의 암호 액세스를 취소하는 데 도움이 됩니다. 또한 Secrets Manager를 사용하는 비용을 줄이는 데도 도움이 됩니다. 따라서 사용하지 않는 암호는 정기적으로 삭제해야 합니다.

이제 Security Hub가 와 통합되었습니다

비활성 Secrets Manager 암호를 삭제하려면 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager 암호 삭제를 참조하십시오.

[SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config 규칙: `secretsmanager-secret-periodic-rotation`

스케줄 유형: 주기적

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`maxDaysSinceRotation`	보안 암호를 변경하지 않은 상태로 유지할 수 있는 최대 일수	Integer	`1~180`	`90`

이 컨트롤은 AWS Secrets Manager 암호가 지정된 기간 내에 한 번 이상 교체되었는지 여부를 확인합니다. 보안 암호를 이 정도로 자주 교체하지 않으면 제어가 실패합니다. 교체 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 90일을 사용합니다.

암호 회전은 AWS 계정에서 암호가 무단으로 사용되는 위험을 줄이는 데 도움이 될 수 있습니다. 그 예로는 데이터베이스 보안 인증 정보, 비밀번호, 타사 API 키, 심지어 임의의 텍스트도 포함됩니다. 오랜 기간 동안 보안 암호를 바꾸지 않으면 보안 암호가 손상될 가능성이 높아집니다.

더 많은 사용자가 보안 암호에 액세스할 수 있으므로 누군가가 잘못 취급하여 승인되지 않은 엔터티에 유출할 가능성이 높아질 수 있습니다. 보안 암호는 로그 및 캐시 데이터를 통해 유출될 수 있습니다. 디

버깅 목적으로 보안 암호를 공유할 수 있으며, 디버깅이 끝나도 보안 암호를 변경하거나 취소하지 않습니다. 이러한 모든 이유로 보안 암호는 자주 교체해야 합니다.

AWS Secrets Manager에서 암호 자동 순환을 구성할 수 있습니다. 자동 교체를 사용하면 장기 암호를 단기 암호로 대체하여 손상 위험을 크게 줄일 수 있습니다. Secrets Manager 비밀에 대한 자동 교체를 구성하는 것이 좋습니다. 자세한 내용은 AWS Secrets Manager 사용 설명서에서 AWS Secrets Manager 암호 교체를 참조하십시오.

이제 Security Hub가 와 통합되었습니다

Secrets Manager 암호에 대한 자동 교체를 켜려면 사용 AWS Secrets Manager 설명서의 콘솔을 사용하여 AWS Secrets Manager 암호에 대한 자동 교체 설정을 참조하십시오. 순환 AWS Lambda 기능을 선택하고 구성해야 합니다.

[SecretsManager.5] Secrets Manager 비밀에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config 규칙: `tagged-secretsmanager-secret` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS Secrets Manager 비밀에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 시크릿에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 컨트롤이 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태

그 키의 존재 여부만 확인하고 암호에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 aws: 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Secrets Manager 시크릿에 태그를 추가하려면AWS Secrets Manager 사용 설명서의 태그 AWS Secrets Manager 시크릿을 참조하십시오.

AWS Service Catalog 컨트롤

이러한 제어는 Service Catalog 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS

관련 요구 사항: NIST.800-53.R5 AC-3, NIST.800-53.R5 AC-4, NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-8, NIST.800-53.r5 SC-7

범주: 보호 > 보안 액세스 관리

심각도: 높음

리소스 유형: `AWS::ServiceCatalog::Portfolio`

AWS Config 규칙: `servicecatalog-shared-within-organization`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 통합이 AWS Service Catalog 활성화된 경우 조직 내에서 포트폴리오를 공유하는지 여부를 확인합니다. AWS Organizations 포트폴리오를 조직 내에서 공유하지 않으면 제어가 실패합니다.

Organizations 내에서만 포트폴리오를 공유하면 포트폴리오를 잘못 공유하지 않도록 할 수 AWS 계정있습니다. Service Catalog 포트폴리오를 조직의 계정과 공유하려면 Security Hub에서는 `ORGANIZATION_MEMBER_ACCOUNT` 대신 을 사용할 것을 권장합니다`ACCOUNT`. 이렇게 하면 조직 전체에서 계정에 부여된 액세스 권한을 관리하여 관리를 간소화할 수 있습니다. 업무상 외부 계정과 Service Catalog 포트폴리오를 공유해야 하는 경우 이 컨트롤에서 검색 결과를 자동으로 숨기거나 사용하지 않도록 설정할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Organizations와 포트폴리오를 공유할 수 있도록 하려면 Service Catalog 관리자 가이드의 공유를 참조하십시오. AWS Organizations

Amazon 심플 이메일 서비스 컨트롤

이러한 컨트롤은 Amazon SES 리소스와 관련이 있습니다.

이러한 제어 기능을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::SES::ContactList`

AWS Config규칙: `tagged-ses-contactlist` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon SES 연락처 목록에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 연락처 목록에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 연락처 목록에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Amazon SES 연락처 목록에 태그를 추가하려면 Amazon SES API v2 참조를 참조하십시오 TagResource.

[SES.2] SES 구성 세트에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::SES::ConfigurationSet`

AWS Config규칙: `tagged-ses-configurationset` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 Amazon SES 구성 세트에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 구성 세트에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 구성 세트에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Amazon SES 구성 세트에 태그를 추가하려면 Amazon SES API v2 참조서를 참조하십시오 TagResource.

Amazon Simple Notification Service 제어

이러한 제어는 Amazon SNS 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[SNS.1] SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS

> **Important**
>
> Security Hub는 2024년 4월에 AWS 기본 보안 모범 사례 표준에서 이 제어 기능을 제거했지만 여전히 NIST SP 800-53 Rev. 5 표준에는 포함되어 있습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::SNS::Topic`

AWS Config 규칙: `sns-encrypted-kms`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS Key Management Service (AWS KMS) 에서 관리되는 키를 사용하여 Amazon SNS 주제가 유휴 상태에서 암호화되는지 여부를 확인합니다. SNS 주제가 서버 측 암호화 (SSE) 에 KMS 키를 사용하지 않으면 제어가 실패합니다. 기본적으로 SNS는 디스크 암호화를 사용하여 메시지와 파일을 저장합니다. 이 제어를 전달하려면 암호화에 KMS 키를 대신 사용하도록 선택해야 합니다. 이렇게 하면 보안 계층이 추가되고 액세스 제어 유연성이 향상됩니다.

저장된 데이터를 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. AWS데이터를 읽기 전에 해독하려면 API 권한이 필요합니다. 보안을 강화하기 위해 KMS 키로 SNS 주제를 암호화하는 것이 좋습니다.

이제 Security Hub가 와 통합되었습니다

SNS 주제에 SSE를 활성화하려면 Amazon 단순 알림 서비스 개발자 안내서의 Amazon SNS 주제에 대한 서버 측 암호화 (SSE) 활성화를 참조하십시오. SSE를 사용하려면 먼저 주제 암호화와 메시지 암호화 및 암호 해독을 허용하는 AWS KMS key 정책을 구성해야 합니다. 자세한 내용은 Amazon 단순 알림 서비스 개발자 안내서의 AWS KMS 권한 구성을 참조하십시오.

[SNS.2] 주제에 전송된 알림 메시지의 전송 상태 로깅이 활성화되어야 합니다.

> **Important**
>
> Security Hub는 2024년 4월에 이 제어를 폐기했습니다. 자세한 정보는 Security Hub 제어 기능의 변경 로그을 참조하세요.

관련 요구 사항: NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::SNS::Topic`

AWS Config 규칙: `sns-topic-message-delivery-notification-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 엔드포인트에 대해 Amazon SNS 주제로 전송된 알림 메시지의 전송 상태에 대한 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되지 않은 경우 이 제어가 실패합니다.

로깅은 서비스의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. 메시지 전달 상태를 로깅하면 다음과 같은 운영 상의 인사이트를 제공하는 데 도움이 됩니다.

- 메시지가 Amazon SNS 엔드포인트에 전송되었는지 확인

- Amazon SNS 엔드포인트에서 Amazon SNS로 전송된 응답 식별

- 메시지 체류 시간(게시 타임스탬프와 Amazon SNS 엔드포인트로 전달되는 시간 사이의 시간)을 결정합니다.

이제 Security Hub가 와 통합되었습니다

주제에 대한 전송 상태 로깅을 구성하려면 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 메시지 전송 상태를 참조하십시오.

[SNS.3] SNS 주제에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::SNS::Topic`

AWS Config 규칙: `tagged-sns-topic` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon SNS 주제에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다`requiredTagKeys`. 주제에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 제어가 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 주제에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

SNS 주제에 태그를 추가하려면 Amazon 단순 알림 서비스 개발자 안내서의 Amazon SNS 주제 태그 구성을 참조하십시오.

Amazon Simple Queue Service 제어

이러한 제어는 Amazon SQS 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 AWS 리전사용할 수 있는 것은 아닙니다. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

카테고리: 보호 > 데이터 보호 > 암호화 data-at-rest

심각도: 중간

리소스 유형: `AWS::SQS::Queue`

AWS Config 규칙: `sqs-queue-encrypted` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SQS 대기열이 저장 시 암호화되었는지 여부를 확인합니다. 대기열이 SQS 관리 키 (SSE-SQS) 또는 () 키 (SSE-KMS) 로 암호화되지 않으면 제어가 AWS Key Management Service 실패합니다.AWS KMS

저장 데이터를 암호화하면 권한이 없는 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. 서버 측 암호화 (SSE) 는 SQS에서 관리하는 암호화 키 (SSE-SQS) 또는 키 (SSE-KMS) 를 사용하여 SQS 대기열에 있는 메시지의 콘텐츠를 보호합니다. AWS KMS

이제 Security Hub가 와 통합되었습니다

SQS 대기열에 SSE를 구성하려면 Amazon Simple Queue Service 개발자 안내서의 대기열 (콘솔) 에 대한 서버 측 암호화 (SSE) 구성을 참조하십시오.

[SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::SQS::Queue`

AWS Config 규칙: `tagged-sqs-queue` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 Amazon SQS 대기열에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다. `requiredTagKeys` 대기열에 태그 키가 없거나 `requiredTagKeys` 파라미터에 지정된 모든 키가 없

는 경우 제어가 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 대기열에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Amazon SQS 콘솔을 사용하여 기존 대기열에 태그를 추가하려면 Amazon 단순 대기열 서비스 개발자 안내서의 Amazon SQS 대기열 (콘솔) 에 대한 비용 할당 태그 구성을 참조하십시오.

AWS Step Functions 제어 항목:

이러한 제어는 Step Functions 리소스와 관련되어 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::StepFunctions::StateMachine`

AWS Config 규칙: `step-functions-state-machine-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`logLevel`	최소 로깅 수준	Enum	`ALL`, `ERROR`, `FATAL`	기본값 없음

이 컨트롤은 AWS Step Functions 스테이트 머신의 로깅 기능이 켜져 있는지 여부를 확인합니다. 상태 머신에 로깅이 켜져 있지 않으면 제어가 실패합니다. `logLevel` 파라미터에 사용자 지정 값을 제공하는 경우 상태 머신에 지정된 로깅 수준이 켜져 있는 경우에만 제어가 통과합니다.

모니터링을 통해 Step Functions의 안정성, 가용성 및 성능을 유지할 수 있습니다. 멀티포인트 장애를 보다 쉽게 디버깅할 수 있도록 사용하는 만큼의 AWS 서비스 모니터링 데이터를 수집해야 합니다. Step Functions 상태 머신에 대해 로깅 구성을 정의하면 Amazon CloudWatch Logs에서 실행 기록과 결과를 추적할 수 있습니다. 선택적으로 오류나 치명적인 이벤트만 추적할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Step Functions 상태 머신에 대한 로깅을 켜려면 AWS Step Functions 개발자 안내서의 로깅 구성을 참조하십시오.

[StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::StepFunctions::Activity`

AWS Config 규칙: `tagged-stepfunctions-activity` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
requiredTagKeys	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	기본값 없음

이 컨트롤은 AWS Step Functions 액티비티에 파라미터에 정의된 특정 키가 포함된 태그가 있는지 확인합니다requiredTagKeys. 액티비티에 태그 키가 없거나 파라미터에 지정된 모든 키가 없는 경우 컨트롤이 requiredTagKeys 실패합니다. 파라미터가 제공되지 requiredTagKeys 않은 경우 컨트롤은 태그 키의 존재 여부만 확인하고 액티비티에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 aws: 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Step Functions 활동에 태그를 추가하려면 AWS Step Functions 개발자 안내서의 Step Functions에서 태깅을 참조하십시오.

AWS Transfer Family 컨트롤

이러한 통제는 Transfer Family 리소스와 관련이 있습니다.

이러한 제어 기능을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Transfer::Workflow`

AWS Config 규칙: `tagged-transfer-workflow` (사용자 지정 Security Hub 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

파라미터	설명	유형	허용된 사용자 지정 값	Security Hub 기본값
`requiredTagKeys`	평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록. 태그 키는 대소문자를 구별합니다.	StringList	요구 사항을 충족하는 AWS 태그 목록	`No default value`

이 컨트롤은 AWS Transfer Family 워크플로에 매개 변수에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 워크플로에 태그 키가 없거나 매개 변수에 지정된 모든 키가 없는 경우 컨트롤이 `requiredTagKeys` 실패합니다. 매개 변수를 `requiredTagKeys` 제공하지 않으면 컨트롤은 태그 키의 존재 여부만 확인하고 워크플로에 키 태그가 지정되지 않으면 실패합니다. 자동으로 적용되고 로 `aws:` 시작되는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 구성, 검색 및 필터링할 수 있습니다. 또한 태그를 지정하면 작업 및 알림에 대한 책임 있는 리소스 소유자를 추적할 수 있습니다. 태그 지정을 사용하면 태그를 기반으로 권한을 정의하는 속성 기반 액세스 제어 (ABAC) 를 권한 부여 전략으로 구현할 수 있습니다. IAM 엔티티 (사용자 또는 역할) 및 리소스에 태그를 첨부할 수 있습니다. AWS IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 이러한 ABAC 정책을 설계할 수 있습니다. 자세한 내용은 ABAC의 용도를 참조하십시오. AWSIAM 사용 설명서에서.

> **Note**
>
> 태그에 개인 식별 정보 (PII) 또는 기타 기밀 또는 민감한 정보를 추가하지 마십시오. 태그를 포함한 많은 사람들이 AWS 서비스태그에 액세스할 수 있습니다. AWS Billing태그 지정 모범 사례에 대한 자세한 내용은 에서 AWS 리소스 태그 지정을 참조하십시오. AWS 일반 참조

이제 Security Hub가 와 통합되었습니다

Transfer Family 워크플로에 태그를 추가하려면 (콘솔)

1. AWS Transfer Family 콘솔을 엽니다.
2. 탐색 창에서 워크플로를 선택합니다. 그런 다음 태그를 지정할 워크플로를 선택합니다.
3. [태그 관리] 를 선택하고 태그를 추가합니다.

[Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.

관련 요구 사항: NIST.800-53.R5 CM-7, NIST.800-53.r5 IA-5, NIST.800-53.R5 SC-8

카테고리: 보호 > 데이터 보호 > 암호화 data-in-transit

심각도: 중간

리소스 유형: `AWS::Transfer::Server`

AWS Config 규칙: `transfer-family-server-no-ftp`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 AWS Transfer Family 서버가 엔드포인트 연결에 FTP 이외의 프로토콜을 사용하는지 여부를 확인합니다. 서버가 FTP 프로토콜을 사용하여 클라이언트를 서버의 엔드포인트에 연결하는 경우 제어가 실패합니다.

FTP (파일 전송 프로토콜) 는 암호화되지 않은 채널을 통해 엔드포인트 연결을 설정하므로 이러한 채널을 통해 전송되는 데이터는 가로채기에 취약합니다. SFTP (SSH 파일 전송 프로토콜), FTPS (파일 전송 프로토콜 보안) 또는 AS2 (Application Statement 2) 를 사용하면 전송 데이터를 암호화하여 추가

보안 계층을 제공하며 잠재적 공격자가 네트워크 트래픽을 도청하거나 조작하기 위한 person-in-the-middle 또는 유사한 공격을 사용하지 못하도록 방지하는 데 사용할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

Transfer Family 서버의 프로토콜을 수정하려면AWS Transfer Family 사용 설명서의 파일 전송 프로토콜 편집을 참조하십시오.

AWS WAF 컨트롤

이러한 컨트롤은 AWS WAF 리소스와 관련이 있습니다.

이러한 컨트롤을 모두 사용할 수 있는 것은 아닙니다 AWS 리전. 자세한 정보는 리전별 제어 기능 사용 가능 여부을 참조하세요.

[WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::WAF::WebACL`

AWS Config 규칙: `waf-classic-logging-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 AWS WAF 글로벌 웹 ACL에 대한 로깅이 활성화되었는지 여부를 확인합니다. 웹 ACL에 로깅이 활성화되지 않은 경우 이 제어는 실패합니다.

로깅은 AWS WAF 전 세계의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. 이는 많은 조직의 비즈니스 및 규정 준수 요구 사항이며, 이를 통해 애플리케이션 동작 문제를 해결할 수 있습니다. 또한 AWS WAF에 연결된 웹 ACL을 통해 분석된 트래픽에 대한 상세 정보도 제공합니다.

이제 Security Hub가 와 통합되었습니다

AWS WAF 웹 ACL에 대한 로깅을 활성화하려면 AWS WAF 개발자 안내서의 웹 ACL 트래픽 정보 로깅을 참조하십시오.

[WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21)

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAFRegional::Rule`

AWS Config 규칙: `waf-regional-rule-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS WAF 지역 규칙에 하나 이상의 조건이 있는지 확인합니다. 규칙 내에 조건이 없는 경우 제어가 실패합니다.

WAF 리전별 규칙에는 여러 조건이 포함될 수 있습니다. 규칙의 조건에 따라 트래픽을 검사하고 정의된 조치(허용, 차단 또는 계산)를 수행할 수 있습니다. 아무 조건 없이 트래픽은 검사 없이 통과합니다. 조건은 없지만 허용, 차단 또는 개수를 제안하는 이름이나 태그가 있는 WAF 리전별 규칙은 해당 작업 중 하나가 발생하고 있다고 잘못 가정할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

빈 규칙에 조건을 추가하려면 AWS WAF 개발자 안내서의 규칙에서 조건 추가 및 제거를 참조하십시오.

[WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21)

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAFRegional::RuleGroup`

AWS Config 규칙: `waf-regional-rulegroup-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS WAF 지역 규칙 그룹에 하나 이상의 규칙이 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 제어가 실패합니다.

WAF 리전별 규칙 그룹에는 여러 규칙이 포함될 수 있습니다. 규칙의 조건에 따라 트래픽을 검사하고 정의된 조치(허용, 차단 또는 계산)를 수행할 수 있습니다. 규칙이 없으면 트래픽은 검사 없이 통과합니다. 규칙이 없지만 허용, 차단 또는 개수를 암시하는 이름 또는 태그가 있는 WAF 리전별 규칙 그룹은 이러한 작업 중 하나가 발생하고 있다고 잘못 가정할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

빈 규칙 그룹에 규칙 및 규칙 조건을 추가하려면 AWS WAF 개발자 안내서의 AWS WAF 클래식 규칙 그룹에 규칙 추가 및 삭제하기 및 규칙에 조건 추가 및 제거를 참조하십시오.

[WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAFRegional::WebACL`

AWS Config 규칙: `waf-regional-webacl-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS WAF Classic Regional 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않으면 이 제어가 실패합니다.

WAF 리전별 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 웹 트래픽은 기본 작업에 따라 WAF에 의해 감지되거나 조치되지 않고 통과할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

빈 AWS WAF 클래식 지역 웹 ACL에 규칙 또는 규칙 그룹을 추가하려면 개발자 안내서의 웹 ACL 편집을 참조하십시오.AWS WAF

[WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAF::Rule`

AWS Config 규칙: `waf-global-rule-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS WAF 글로벌 규칙에 조건이 포함되어 있는지 확인합니다. 규칙 내에 조건이 없는 경우 제어가 실패합니다.

WAF 글로벌 규칙은 여러 조건을 포함할 수 있습니다. 규칙의 조건을 통해 트래픽을 검사하고 정의된 조치(허용, 차단 또는 계산)를 수행할 수 있습니다. 아무 조건 없이 트래픽은 검사 없이 통과합니다. 규칙은 없지만 허용, 차단 또는 개수를 암시하는 이름이나 태그가 있는 WAF 글로벌 규칙은 해당 작업 중 하나가 발생하고 있다고 잘못 가정할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

규칙 생성 및 조건 추가에 대한 지침은 AWS WAF 개발자 안내서의 규칙 생성 및 조건 추가를 참조하십시오.

[WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAF::RuleGroup`

AWS Config 규칙: `waf-global-rulegroup-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS WAF 글로벌 규칙 그룹에 하나 이상의 규칙이 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 제어가 실패합니다.

WAF 글로벌 규칙 그룹은 여러 규칙을 포함할 수 있습니다. 규칙의 조건에 따라 트래픽을 검사하고 정의된 조치(허용, 차단 또는 계산)를 수행할 수 있습니다. 규칙이 없으면 트래픽은 검사 없이 통과합니다. 규칙은 없지만 허용, 차단 또는 개수를 암시하는 이름이나 태그가 있는 WAF 글로벌 규칙 그룹은 해당 작업 중 하나가 발생하고 있다고 잘못 가정할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

규칙 그룹에 규칙을 추가하는 방법에 대한 지침은 AWS WAF 개발자 안내서의 AWS WAF 클래식 규칙 그룹 만들기를 참조하십시오.

[WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(21)

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAF::WebACL`

AWS Config 규칙: `waf-global-webacl-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS WAF 글로벌 웹 ACL에 하나 이상의 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않으면 제어가 실패합니다.

WAF 글로벌 웹 ACL은 웹 요청을 검사하고 제어하기 위한 규칙 및 규칙 그룹 모음을 포함할 수 있습니다. 웹 ACL이 비어 있는 경우 웹 트래픽은 기본 작업에 따라 WAF에 의해 감지되거나 조치되지 않고 통과할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

빈 AWS WAF 글로벌 웹 ACL에 규칙 또는 규칙 그룹을 추가하려면 개발자 안내서의 웹 ACL 편집을 참조하십시오.AWS WAF 필터에서 글로벌 () CloudFront 을 선택합니다.

[WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAFv2::WebACL`

AWS Config 규칙: `wafv2-webacl-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS WAF V2 웹 액세스 제어 목록 (웹 ACL) 에 하나 이상의 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 규칙 또는 규칙 그룹이 포함되어 있지 않으면 제어가 실패합니다.

웹 ACL을 사용하면 보호된 리소스가 응답하는 모든 HTTP(S) 웹 요청을 세밀하게 제어할 수 있습니다. 웹 ACL에는 웹 요청을 검사하고 제어하기 위한 규칙 및 규칙 그룹 모음이 포함되어야 합니다. 웹 ACL이 비어 있는 경우 기본 동작에 AWS WAF 따라 웹 트래픽이 감지되거나 조치를 취하지 않고 전달될 수 있습니다.

이제 Security Hub가 와 통합되었습니다

빈 WAFV2 웹 ACL에 규칙 또는 규칙 그룹을 추가하려면 AWS WAF 개발자 안내서의 웹 ACL 편집을 참조하십시오.

[WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 낮음

리소스 유형: `AWS::WAFv2::WebACL`

AWS Config 규칙: **`wafv2-logging-enabled`**

스케줄 유형: 주기적

파라미터: 없음

이 컨트롤은 AWS WAF V2 웹 액세스 제어 목록 (웹 ACL) 에 대한 로깅이 활성화되었는지 여부를 확인합니다. 웹 ACL에 대한 로깅이 비활성화되면 이 제어가 실패합니다.

로깅은 의 안정성, 가용성 및 성능을 유지합니다. AWS WAF또한 로깅은 많은 조직의 비즈니스 및 규정 준수 요구 사항입니다. 웹 ACL로 분석된 트래픽을 로깅하여 애플리케이션 동작 문제를 해결할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

AWS WAF 웹 ACL에 대한 로깅을 활성화하려면 AWS WAF 개발자 안내서의 웹 ACL에 대한 로깅 관리를 참조하십시오.

[WAF.12] AWS WAF 규칙에는 메트릭이 활성화되어 있어야 합니다. CloudWatch

관련 요구 사항: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::WAFv2::RuleGroup`

AWS Config 규칙: **`wafv2-rulegroup-logging-enabled`**

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 AWS WAF 규칙 또는 규칙 그룹에 Amazon CloudWatch 지표가 활성화되어 있는지 여부를 확인합니다. 규칙 또는 규칙 그룹에 CloudWatch 지표가 활성화되어 있지 않으면 제어가 실패합니다.

AWS WAF 규칙 및 규칙 그룹에 CloudWatch 지표를 구성하면 트래픽 흐름을 파악할 수 있습니다. 어떤 ACL 규칙이 트리거되고 어떤 요청이 수락 및 차단되었는지 확인할 수 있습니다. 이러한 가시성을 통해 관련 리소스에서 악의적인 활동을 식별할 수 있습니다.

이제 Security Hub가 와 통합되었습니다

AWS WAF 규칙 그룹에서 CloudWatch 지표를 활성화하려면 UpdateRuleGroupAPI를 호출하십시오. AWS WAF 규칙에서 CloudWatch 지표를 활성화하려면 UpdateWebACL API를 호출하십시오. `CloudWatchMetricsEnabled` 필드를 `true`로 설정합니다. AWS WAF 콘솔을 사용하여 규칙 또는 규칙 그룹을 생성하면 CloudWatch 지표가 자동으로 활성화됩니다.

보안 제어 보기 및 관리

제어는 조직이 정보의 기밀성, 무결성 및 가용성을 보호하는 데 도움이 되는 보안 표준 내의 보호 장치입니다. Security Hub에서 컨트롤은 특정 AWS 리소스와 관련이 있습니다.

통합 제어 보기

Security Hub 콘솔의 컨트롤 페이지에는 현재 AWS 리전 사용 가능한 모든 컨트롤이 표시됩니다. 보안 표준 페이지로 이동하여 활성화된 표준을 선택하면 표준 컨텍스트에서 컨트롤을 볼 수 있습니다. Security Hub는 표준 전체에 걸쳐 일관된 보안 제어 ID, 제목 및 설명을 제어에 할당합니다. 컨트롤 ID에는 관련 AWS 서비스 번호와 고유한 번호가 포함됩니다 (예: CodeBuild .3).

Security Hub 콘솔의 제어 페이지에서 다음 정보를 사용할 수 있습니다.

- 데이터가 포함된 활성화된 총 제어 수와 비교하여 통과된 제어의 비율을 기준으로 한 전체 보안 점수
- 활성화된 모든 제어에서 실패한 보안 검사 비율
- 다양한 심각도의 제어 항목에 대한 보안 검사 통과 및 실패 횟수
- 활성화 상태에 따라 여러 탭으로 구분된 제어 목록 활성화된 표준에 적용되지 않는 사용 가능한 제어는 비활성화됨 열에 표시됩니다. 처리되지 않은 제어(예: 현재 리전에서 사용할 수 없는 제어)은 데이터 없음 열에 표시됩니다. 전부 열에 있는 제어 수는 실패, 알 수 없음, 통과, 비활성화, 데이터 없음 열에 있는 제어 수의 합계와 같습니다.

제어 페이지에서 제어를 선택하여 세부 정보를 보고 제어에서 생성된 조사 결과에 대해 조치를 취할 수 있습니다. 이 페이지에서 현재 AWS 계정 AND에서 보안 제어를 활성화하거나 비활성화할 수도 있습니다. AWS 리전제어 페이지의 활성화 및 비활성화 조치는 모든 표준에 적용됩니다. 자세한 내용은 모든 표준에서 제어 활성화 및 비활성화을 참조하십시오.

관리자 계정의 경우 제어 페이지에는 구성원 계정 전체의 제어 상태가 반영됩니다. 하나 이상의 구성원 계정에서 제어 검사에 실패하면 제어 페이지의 실패 탭에 제어가 나타납니다. 집계 영역을 설정한 경우 제어 페이지에는 연결된 모든 리전의 제어 상태가 반영됩니다. 하나 이상의 연결된 리전에서 제어 검사에 실패하면 제어 페이지의 실패 탭에 해당 제어가 나타납니다.

통합 제어 보기를 사용하면 AWS 보안 검색 결과 형식 (ASFF) 의 제어 검색 결과 필드가 변경되어 워크플로에 영향을 미칠 수 있습니다. 자세한 정보는 통합 제어 보기 - ASFF 변경을 참조하세요.

제어에 대한 전체 보안 점수

제어 페이지에는 0~ 100% 의 전체 보안 점수가 표시됩니다. 전체 보안 점수는 데이터를 사용하여 활성화된 제어의 총 수와 비교한 통과된 제어의 비율을 기준으로 계산됩니다.

> **Note**
>
> 제어에 대한 전체 보안 점수를 보려면 Security Hub에 액세스하는 데 사용하는 IAM 역할에 **`BatchGetControlEvaluations`**를 호출할 수 있는 권한을 추가해야 합니다. 특정 표준의 보안 점수를 보는 데는 이 권한이 필요하지 않습니다.

Security Hub를 활성화하면 Security Hub는 사용자가 Security Hub 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 초기 보안 점수를 계산합니다. 중국 리전 및 AWS GovCloud (US) Region에 처음으로 보안 점수를 생성하는 데 최대 24시간이 걸릴 수 있습니다. 점수는 해당 페이지를 방문할 때 활성화된 표준에 대해서만 생성됩니다. 현재 활성화된 표준 목록을 보려면 `GetEnabledStandards` API 작업을 사용하십시오. 또한 점수가 표시되도록 AWS Config 리소스 기록을 구성해야 합니다. 전체 보안 점수는 표준 보안 점수의 평균입니다.

Security Hub는 점수를 처음 생성한 후 24시간마다 보안 점수를 업데이트합니다. Security Hub는 보안 점수가 마지막으로 업데이트된 시기를 나타내는 타임스탬프를 표시합니다.

집계 영역을 설정한 경우 전체 보안 점수는 연결된 리전 전반의 제어 조사 결과를 반영합니다.

주제

- 제어 범주
- 모든 표준에서 제어 활성화 및 비활성화
- 활성화된 표준에서 자동으로 새 제어 활성화
- 사용자 지정 제어 파라미터
- 비활성화할 수 있는 Security Hub 제어

- 제어에 대한 세부 정보 보기
- 제어 목록 필터링 및 정렬
- 제어 조사 결과 보기 및 조치 수행

제어 범주

각 제어에는 범주가 할당됩니다. 제어 범주에는 해당 제어가 적용되는 보안 기능이 반영됩니다.

범주 값에는 범주, 범주 내의 하위 범주 및 선택적으로 하위 범주 내의 분류자가 포함됩니다. 예:

- 식별 > 인벤토리
- 보호 > 데이터 보호 > 전송 중인 데이터 암호화

다음은 사용 가능한 범주, 하위 범주, 분류자에 대한 설명입니다.

식별

시스템, 자산, 데이터 및 기능에 대한 사이버 보안 위험을 관리하기 위한 조직의 이해를 높입니다.

인벤토리

서비스가 올바른 리소스 태깅 전략을 구현했습니까? 태깅 전략에 리소스 소유자가 포함됩니까?

서비스는 어떤 리소스를 사용합니까? 이 서비스에 대해 승인된 리소스가 있습니까?

승인된 인벤토리에 대한 가시성이 있습니까? 예를 들어, Amazon EC2 Systems Manager 및 Service Catalog와 같은 서비스를 사용하십니까?

로깅

서비스에 대한 모든 관련 로깅을 안전하게 활성화했습니까? 로그 파일의 예는 다음과 같습니다.

- Amazon VPC 흐름 로그
- Elastic Load Balancing 액세스 로그
- 아마존 CloudFront 로그
- 아마존 CloudWatch 로그
- Amazon Relational Database Service 로깅
- Amazon OpenSearch 서비스 슬로우 인덱스 로그
- X-Ray 추적

- AWS Directory Service 로그
- AWS Config 아이템
- 스냅샷

보호

중요한 인프라 서비스 및 보안 코딩 사례의 제공을 보장하기 위해 적절한 안전 장치를 개발 및 구현합니다.

보안 액세스 관리

서비스가 IAM 또는 리소스 정책에서 최소 권한 관행을 사용합니까?

암호와 보안 정보는 충분히 복잡합니까? 그들은 적절하게 교체됩니까?

서비스가 다중 인증(MFA)을 사용합니까?

서비스가 루트 사용자를 피합니까?

리소스 기반 정책에서 퍼블릭 액세스를 허용합니까?

보안 네트워크 구성

서비스가 안전하지 않은 퍼블릭 원격 네트워크 액세스를 방지합니까?

서비스가 VPC를 제대로 사용합니까? 예를 들어 작업을 VPC에서 실행해야 합니까?

서비스가 민감한 리소스를 적절하게 분할하고 격리합니까?

데이터 보호

저장 데이터 암호화 - 서비스가 저장 데이터를 암호화합니까?

전송 중인 데이터 암호화 - 서비스가 전송 중인 데이터를 암호화합니까?

데이터 무결성 - 서비스가 데이터의 무결성을 검증합니까?

데이터 삭제 보호 - 서비스가 실수로 인한 삭제로부터 데이터를 보호합니까?

데이터 관리/사용 – Amazon Macie와 같은 서비스를 사용하여 민감한 데이터의 위치를 추적합니까?

API 보호

서비스를 AWS PrivateLink 사용하여 서비스 API 작업을 보호하나요?

보호 서비스

올바른 보호 서비스가 있습니까? 그들은 정확한 양의 범위를 제공합니까?

보호 서비스는 서비스를 대상으로 하는 공격 및 손상을 차단하는 데 도움이 됩니다. 보호 서비스의 AWS 예로는 AWS Control Tower,, Vanta AWS WAF AWS Shield Advanced, Secrets Manager, IAM 액세스 분석기 등이 있습니다. AWS Resource Access Manager

안전한 개발

보안 코딩 사례를 사용합니까?

Open Web Application Security Project(OWASP) Top 10과 같은 취약점을 피합니까?

감지

사이버 보안 이벤트의 발생을 식별하기 위한 적절한 활동을 개발하고 구현합니다.

감지 서비스

올바른 감지 서비스가 있습니까?

그들은 정확한 양의 범위를 제공합니까?

AWS 탐지 서비스의 예로는 아마존 GuardDuty AWS Security Hub, 아마존 인스펙터, 아마존 디텍티브, CloudWatch 아마존 알람 AWS IoT Device Defender등이 있습니다. AWS Trusted Advisor

대처

감지된 사이버 보안 이벤트와 관련하여 조치를 취할 수 있는 적절한 활동을 개발하고 구현합니다.

응답 조치

보안 이벤트에 신속하게 대응하고 있습니까?

치명적이거나 심각도가 높은 활성 조사 결과가 있습니까?

포렌식

서비스에 대한 포렌식 데이터를 안전하게 획득할 수 있습니까? 예를 들어, 진정한 긍정적인 조사 결과와 관련된 Amazon EBS 스냅샷을 확보하고 있습니까?

포렌식 계정을 설정했습니까?

복구

복원성 계획을 유지하고 사이버 보안 이벤트로 인해 손상된 기능이나 서비스를 복원하기 위한 적절한 활동을 개발하고 구현합니다.

복원력

서비스 구성이 정상적인 장애 조치, 탄력적 확장 및 고가용성을 지원합니까?

백업을 설정했습니까?

모든 표준에서 제어 활성화 및 비활성화

AWS Security Hub 활성화된 제어에 대한 결과를 생성하고 보안 점수를 계산할 때 활성화된 모든 제어를 고려합니다. 모든 보안 표준에서 제어를 활성화 및 비활성화하도록 선택하거나 표준마다 활성화 상태를 다르게 구성할 수 있습니다. 제어 활성화 및 비활성화를 선택하여 제어의 활성화 상태를 사용 가능한 모든 표준에 맞게 조정하는 것이 좋습니다. 이 섹션에서는 표준 전반에 걸쳐 제어를 활성화 및 비활성화하는 방법을 설명합니다. 하나 이상의 특정 표준에서 제어를 활성화 또는 비활성화하려면 특정 표준에서의 제어 활성화 및 비활성화 섹션을 참조하세요.

집계 영역을 설정한 경우 Security Hub 콘솔에는 연결된 모든 리전의 제어가 표시됩니다. 연결된 리전에서는 제어를 사용할 수 있지만 집계 영역에서는 사용할 수 없는 경우, 집계 영역에서 해당 제어를 활성화하거나 비활성화할 수 없습니다.

> **Note**
>
> 제어 활성화 및 비활성화 지침은 중앙 구성 사용 여부에 따라 달라집니다. 이 섹션에서는 차이점을 설명합니다. Security Hub 및 를 통합하는 사용자는 중앙 구성을 사용할 수 AWS Organizations있습니다. 다중 계정, 다중 리전 환경에서 제어를 활성화 또는 비활성화하는 프로세스를 단순화하려면 중앙 구성을 사용하는 것이 좋습니다.

제어 활성화

표준에서 제어를 활성화하면 Security Hub가 제어에 대한 보안 검사를 실행하고 제어 결과를 생성하기 시작합니다.

Security Hub는 전체 보안 점수 및 표준 보안 점수 계산에 제어 상태를 포함합니다. 통합 제어 결과를 켜면 여러 표준에서 제어를 활성화했더라도 보안 검사에 대한 단일 검색 결과를 받게 됩니다. 자세한 내용은 Consolidated control findings를 참조하세요.

다중 계정 및 리전에서 모든 표준의 제어 활성화

여러 계정에 대한 보안 제어를 활성화하려면 중앙 구성을 사용해야 합니다. AWS 리전

중앙 구성을 사용하는 경우 위임된 관리자는 사용 가능한 표준에 대해 지정된 제어를 활성화하는 Security Hub 구성 정책을 만들 수 있습니다. 그런 다음 구성 정책을 특정 계정 및 OU(조직 단위) 또는 루트와 연결할 수 있습니다. 구성 정책은 홈 리전(집계 영역이라고도 함) 및 연결된 모든 리전에 적용됩니다.

구성 정책은 사용자 지정을 제공합니다. 예를 들어 한 OU에서는 모든 제어를 활성화하고 다른 OU에서는 Amazon Elastic Compute Cloud(EC2) 제어만 활성화하도록 선택할 수 있습니다. 세분화 수준은 조직의 보안 범위에 대한 의도한 목표에 따라 달라집니다. 표준 전반에 걸쳐 지정된 제어를 활성화하는 구성 정책을 만드는 방법에 대한 지침은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요.

> **Note**
>
> 위임된 관리자는 서비스 관리 표준을 제외한 모든 표준의 제어를 관리하는 구성 정책을 만들 수 있습니다. AWS Control Tower이 표준에 대한 컨트롤은 서비스에서 구성해야 합니다. AWS Control Tower

일부 계정에서 위임된 관리자가 아닌 자체 제어를 구성하도록 하려면 위임된 관리자가 해당 계정을 자체 관리형 계정으로 지정할 수 있습니다. 자체 관리형 계정은 각 리전에서 개별적으로 제어를 구성해야 합니다.

단일 계정 및 리전에서 모든 표준의 제어 활성화

중앙 구성을 사용하지 않거나 자체 관리형 계정인 경우 구성 정책을 사용하여 다중 계정 및 리전에서 제어를 중앙에서 활성화할 수 없습니다. 하지만 다음 단계를 사용하여 단일 계정 및 리전에서 제어를 활성화할 수 있습니다.

Security Hub console

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다.
3. 비활성화 탭을 선택합니다.
4. 제어 옆에 있는 옵션을 선택합니다.
5. 제어 활성화를 선택합니다(이 옵션은 이미 활성화된 제어에는 표시되지 않습니다).

6. 제어를 활성화하려는 각 리전에 대해 이 단계를 반복합니다.

Security Hub API

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 활성화하려면

1. ListStandardsControlAssociations API를 호출합니다. 보안 제어 ID를 제공합니다.

   요청 예:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. BatchUpdateStandardsControlAssociations API를 호출합니다. 제어가 활성화되지 않은 표준의 Amazon 리소스 이름(ARN)을 제공합니다. 표준 ARN을 가져오려면 `DescribeStandards`를 실행하십시오.
3. `AssociationStatus` 파라미터를 `ENABLED`와 동일하게 설정합니다. 이미 활성화된 제어 대해 다음 단계를 수행하면 API가 HTTP 상태 코드 200 응답을 반환합니다.

   요청 예:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
   v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
   best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
   }
   ```

4. 제어를 활성화하려는 각 리전에 대해 이 단계를 반복합니다.

AWS CLI

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 활성화하려면

1. list-standards-control-associations 명령을 실행합니다. 보안 제어 ID를 제공합니다.

   ```
   aws securityhub  --region us-east-1 list-standards-control-associations --
   security-control-id CloudTrail.1
   ```

2. batch-update-standards-control-associations 명령을 실행합니다. 제어가 활성화되지 않은 표준의 Amazon 리소스 이름(ARN)을 제공합니다. 표준 ARN을 얻으려면 `describe-standards` 명령을 실행합니다.
3. `AssociationStatus` 파라미터를 `ENABLED`와 동일하게 설정합니다. 이미 활성화된 제어에 대해 다음 단계를 수행하면 명령은 HTTP 상태 코드 200 응답을 반환합니다.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. 제어를 활성화하려는 각 리전에 대해 이 단계를 반복합니다.

활성화된 표준에서 자동으로 새 제어 활성화

Security Hub는 정기적으로 새 보안 제어를 릴리스하고 하나 이상의 표준에 추가합니다. 활성화된 표준에서 새 제어를 자동으로 활성화할 것인지를 선택할 수 있습니다.

> **Note**
>
> 새 제어를 자동으로 활성화하려면 중앙 구성을 사용하는 것이 좋습니다.
> 구성 정책에 비활성화할 제어 목록이 포함된 경우(프로그래밍 방식으로 `DisabledSecurityControlIdentifiers` 파라미터가 반영됨), Security Hub는 새로 릴리스된 제어를 포함하여 표준 전반에 걸쳐 다른 모든 제어를 자동으로 활성화합니다. 정책에 활성화할 제어 목록(`EnabledSecurityControlIdentifiers` 파라미터가 반영됨)이 포함된 경우 Security Hub는 새로 릴리스된 제어를 포함하여 표준 전반에 걸쳐 다른 모든 제어를 자동으로 비활성화합니다. 자세한 정보는 Security Hub 구성 정책의 작동 방식을 참조하세요.

원하는 액세스 방법을 선택하고 단계에 따라 활성화된 표준에서 새 제어를 자동으로 활성화하는 단계를 따릅니다. 다음 지침은 중앙 구성을 사용하지 않는 경우에만 적용됩니다.

Security Hub console

새 제어를 자동으로 활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 일반 탭을 선택합니다.
3. 제어에서 편집을 선택합니다.
4. 활성화된 표준에서 새 제어 자동 활성화를 켜십시오.
5. 저장을 선택합니다.

Security Hub API

새 제어를 자동으로 활성화하려면

1. UpdateSecurityHubConfiguration API를 호출합니다.
2. 활성화된 표준에 대해 새 제어를 자동으로 활성화하려면 `AutoEnableControls`를 `true`로 설정합니다. 새 제어를 자동으로 활성화하지 않으려면 `AutoEnableControls`를 false로 설정합니다.

AWS CLI

새 제어를 자동으로 활성화하려면

1. update-security-hub-configuration 명령을 실행합니다.
2. 활성화된 표준에 대해 새 제어를 자동으로 활성화하려면 `--auto-enable-controls`을 지정합니다. 새 제어를 자동으로 활성화하지 않으려면 `--no-auto-enable-controls`을 지정합니다.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

명령 예:

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

제어 비활성화

모든 표준에서 제어를 비활성화하면 다음과 같은 상황이 발생합니다.

- 해당 제어에 대한 보안 검사가 더 이상 수행되지 않습니다.
- 해당 제어에 대해 추가 조사 결과가 생성되지 않습니다.
- 기존 결과는 3~5일 후에 자동으로 보관됩니다(이는 최선의 노력임).
- Security Hub에서 생성한 모든 관련 AWS Config 규칙은 제거됩니다.

모든 표준에서 제어를 비활성화하는 대신 하나 이상의 특정 표준에서만 제어를 비활성화할 수 있습니다. 이렇게 하면 Security Hub는 비활성화한 표준의 제어에 대한 보안 검사를 실행하지 않으므로 해당 표준에 대한 보안 점수에 영향을 미치지 않습니다. 하지만 Security Hub는 AWS Config 규칙을 유지하고 다른 표준에서 활성화된 경우 제어에 대한 보안 검사를 계속 실행합니다. 이는 요약 보안 점수에 영향을 미칠 수 있습니다. 특정 표준으로 제어를 구성하는 방법에 대한 지침은 특정 표준에서의 제어 활성화 및 비활성화 섹션을 참조하세요.

결과 노이즈를 줄이려면 환경과 관련이 없는 제어를 비활성화하는 것이 유용할 수 있습니다. 비활성화할 제어에 대한 자세한 내용은 비활성화하면 좋을 Security Hub 제어를 참조하세요.

표준을 비활성화하면 표준에 적용되는 모든 제어가 비활성화됩니다. 그러나 다른 표준에서는 해당 제어가 활성화되어 있을 수 있습니다. 표준 비활성화에 대한 자세한 내용은 the section called “표준 활성화 및 비활성화” 섹션을 참조하세요.

표준을 비활성화하면 Security Hub는 해당하는 컨트롤 중 어떤 것이 비활성화되었는지 추적하지 않습니다. 이후에 동일한 표준을 다시 활성화하면 해당 표준에 적용되는 모든 컨트롤이 자동으로 활성화됩니다. 또한 컨트롤을 비활성화해도 영구적인 조치는 아닙니다. 제어를 비활성화한 다음 이전에 비활성화했던 표준을 활성화한다고 가정해 보겠습니다. 표준에 해당 제어가 포함되어 있는 경우 해당 표준에서도 해당 제어가 활성화됩니다. Security Hub에서 표준을 활성화하면 해당 표준에 적용되는 모든 제어가 자동으로 활성화됩니다. 특정 컨트롤을 비활성화하도록 선택할 수 있습니다.

다중 계정 및 리전에서 모든 표준의 제어 비활성화

여러 계정 및 AWS 리전에서 보안 제어를 사용하지 않도록 설정하려면 중앙 구성을 사용해야 합니다.

중앙 구성을 사용하는 경우 위임된 관리자는 사용 가능한 표준에 대해 지정된 제어를 비활성화하는 Security Hub 구성 정책을 만들 수 있습니다. 그런 다음 구성 정책을 특정 계정, OU 또는 루트와 연결할 수 있습니다. 구성 정책은 홈 리전(집계 영역이라고도 함) 및 연결된 모든 리전에 적용됩니다.

구성 정책은 사용자 지정을 제공합니다. 예를 들어 한 OU에서는 모든 AWS CloudTrail 컨트롤을 비활성화하고 다른 OU에서는 모든 IAM 컨트롤을 비활성화하도록 선택할 수 있습니다. 세분화 수준은 조직의 보안 범위에 대한 의도한 목표에 따라 달라집니다. 표준 전반에 걸쳐 지정된 제어를 비활성화하는 구성 정책을 만드는 방법에 대한 지침은 Security Hub 구성 정책 생성 및 연결 섹션을 참조하세요.

> **Note**
>
> 위임된 관리자는 구성 정책을 생성하여 서비스 관리 표준:을 제외한 모든 표준의 제어를 관리할 수 있습니다. AWS Control Tower이 표준에 대한 컨트롤은 서비스에서 구성해야 합니다. AWS Control Tower

일부 계정에서 위임된 관리자가 아닌 자체 제어를 구성하도록 하려면 위임된 관리자가 해당 계정을 자체 관리형 계정으로 지정할 수 있습니다. 자체 관리형 계정은 각 리전에서 개별적으로 제어를 구성해야 합니다.

단일 계정 및 리전에서 모든 표준의 제어 비활성화

중앙 구성을 사용하지 않거나 자체 관리형 계정인 경우 구성 정책을 사용하여 다중 계정 및 리전에서 제어를 중앙에서 비활성화할 수 없습니다. 하지만 다음 단계를 사용하여 단일 계정 및 리전에서 제어를 비활성화할 수 있습니다.

Security Hub console

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 비활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다.
3. 제어 옆에 있는 옵션을 선택합니다.
4. 제어 비활성화를 선택합니다. 이 옵션은 이미 비활성화된 제어에는 나타나지 않습니다.
5. 제어를 비활성화하는 이유를 선택하고 비활성화를 선택하여 확인합니다.
6. 제어를 비활성화하려는 각 리전에 대해 이 단계를 반복합니다.

Security Hub API

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 비활성화하려면

1. ListStandardsControlAssociations API를 호출합니다. 보안 제어 ID를 제공합니다.

요청 예:

```
{
    "SecurityControlId": "IAM.1"
}
```

2. BatchUpdateStandardsControlAssociations API를 호출합니다. 제어가 활성화된 모든 표준의 ARN을 입력합니다. 표준 ARN을 가져오려면 DescribeStandards를 실행하십시오.
3. AssociationStatus 파라미터를 DISABLED와 동일하게 설정합니다. 이미 비활성화된 제어에 대해 다음 단계를 수행하면 API가 HTTP 상태 코드 200 응답을 반환합니다.

   요청 예:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
 applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
 "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}}]
}
```

4. 제어를 비활성화하려는 각 리전에 대해 이 단계를 반복합니다.

AWS CLI

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 비활성화하려면

1. list-standards-control-associations 명령을 실행합니다. 보안 제어 ID를 제공합니다.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. batch-update-standards-control-associations 명령을 실행합니다. 제어가 활성화된 모든 표준의 ARN을 입력합니다. 표준 ARN을 얻으려면 describe-standards 명령을 실행합니다.
3. AssociationStatus 파라미터를 DISABLED와 동일하게 설정합니다. 이미 비활성화된 제어에 대해 다음 단계를 수행하면 명령이 HTTP 상태 코드 200 응답을 반환합니다.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. 제어를 비활성화하려는 각 리전에 대해 이 단계를 반복합니다.

활성화된 표준에서 자동으로 새 제어 활성화

AWS Security Hub 정기적으로 새 컨트롤을 릴리스하고 하나 이상의 표준에 추가합니다. 활성화된 표준에서 새 제어를 자동으로 활성화할 것인지를 선택할 수 있습니다.

> **Note**
>
> 중앙 구성을 사용하고 구성 정책에 비활성화할 특정 제어 목록이 포함된 경우(프로그래밍 방식으로 `DisabledSecurityControlIdentifiers` 파라미터가 반영됨), Security Hub는 새로 릴리스된 제어를 포함하여 표준 전반에 걸쳐 다른 모든 제어를 자동으로 활성화합니다. 자세한 정보는 Security Hub 구성 정책의 작동 방식을 참조하세요.

새 보안 제어를 자동으로 활성화하려면 Security Hub 중앙 구성을 사용하는 것이 좋습니다. 표준 전반에 걸쳐 비활성화할 제어 목록을 포함하는 구성 정책을 만들 수 있습니다. 새로 릴리스된 제어를 포함한 다른 모든 제어는 기본적으로 활성화됩니다. 또는 표준 전반에 걸쳐 활성화할 제어 목록을 포함하는 정책을 만들 수 있습니다. 새로 릴리스된 제어를 포함한 다른 모든 제어는 기본적으로 비활성화됩니다. 자세한 정보는 중앙 구성 작동 방식을 참조하세요.

활성화하지 않은 표준에 새 제어를 추가하면 Security Hub에서 새 제어가 활성화되지 않습니다.

다음 지침은 중앙 구성을 사용하지 않는 경우에만 적용됩니다.

원하는 액세스 방법을 선택하고 단계에 따라 활성화된 표준에서 새 제어를 자동으로 활성화하는 단계를 따릅니다.

Security Hub console

새 제어를 자동으로 활성화하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 일반 탭을 선택합니다.
3. 제어에서 편집을 선택합니다.
4. 활성화된 표준에서 새 제어 자동 활성화를 켜십시오.
5. 저장을 선택합니다.

Security Hub API

새 제어를 자동으로 활성화하려면

1. `UpdateSecurityHubConfiguration`를 실행합니다.
2. 활성화된 표준에 대해 새 제어를 자동으로 활성화하려면 `AutoEnableControls`를 `true`로 설정합니다. 새 제어를 자동으로 활성화하지 않으려면 `AutoEnableControls`를 false로 설정합니다.

AWS CLI

새 제어를 자동으로 활성화하려면

1. `update-security-hub-configuration` 명령을 실행합니다.
2. 활성화된 표준에 대해 새 제어를 자동으로 활성화하려면 `--auto-enable-controls`을 지정합니다. 새 제어를 자동으로 활성화하지 않으려면 `--no-auto-enable-controls`을 지정합니다.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

명령 예:

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

새 제어를 자동으로 활성화하지 않는 경우, 수동으로 활성화해야 합니다. 지침은 the section called “모든 표준에서 제어 활성화 및 비활성화” 섹션을 참조하세요.

사용자 지정 제어 파라미터

일부 Security Hub 제어는 제어 평가 방식에 영향을 주는 파라미터를 사용합니다. 일반적으로 이러한 제어는 Security Hub에서 정의하는 기본 파라미터 값을 기준으로 평가합니다. 하지만 이러한 제어의 일부에 대해서는 파라미터 값을 사용자 지정할 수 있습니다. 제어의 파라미터 값을 사용자 지정하면 Security Hub는 지정한 값을 기준으로 제어를 평가하기 시작합니다. 제어의 기반이 되는 리소스가 사용자 지정 값을 만족하는 경우 Security Hub는 `PASSED` 결과를 생성합니다. 리소스가 사용자 지정 값을 만족하지 않으면 Security Hub는 `FAILED` 결과를 생성합니다.

제어 파라미터를 사용자 지정하면 Security Hub에서 권장하고 모니터링하는 보안 모범 사례를 비즈니스 요구 사항 및 보안 기대치에 맞게 조정할 수 있습니다. 제어에 대한 결과를 숨기는 대신 하나 이상의 파라미터를 사용자 지정하여 보안 요구 사항에 맞는 결과를 얻을 수 있습니다.

다음은 사용자 지정 제어 파라미터의 몇 가지 샘플 사용 사례입니다.

- [CloudWatch.16] - CloudWatch 로그 그룹을 지정된 기간 동안 보존해야 합니다.

  보존 기간을 지정할 수 있습니다.
- [IAM.7] – IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.

  암호 강도와 관련된 파라미터를 지정할 수 있습니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.

  수신 트래픽을 제한 없이 허용할 수 있는 포트를 지정할 수 있습니다.
- [Lambda.5] - VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.

  결과 통과를 생성하는 최소 가용 영역 수를 지정할 수 있습니다.

이 섹션에서는 제어 파라미터를 사용자 지정 및 관리하는 방법을 설명합니다.

사용자 지정 제어 파라미터의 작동 방식

제어에는 하나 이상의 사용자 지정 파라미터 설정이 있을 수 있습니다. 개별 제어 파라미터에 가능한 데이터 유형은 다음과 같습니다.

- Boolean
- Double

- Enum
- EnumList
- Integer
- IntegerList
- String
- StringList

일부 제어의 경우 허용되는 파라미터 값도 지정된 범위에 속해야 유효합니다. 이러한 경우 Security Hub는 허용 가능한 범위를 제공합니다.

Security Hub는 기본 파라미터 값을 선택하고 때때로 이를 업데이트할 수 있습니다. 제어 파라미터를 사용자 지정한 후 해당 값은 변경하지 않는 한 파라미터에 대해 지정한 값이 계속 유지됩니다. 즉, 파라미터의 사용자 지정 값이 Security Hub에서 정의한 현재 기본값과 일치하더라도 파라미터는 기본 Security Hub 값에 대한 업데이트 추적을 중지합니다. 다음은 [ACM.1] - 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다 제어의 예제입니다.

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

위 예제에서 `daysToExpiration` 파라미터의 사용자 지정 값은 `30`입니다. 이 파라미터의 현재 기본값 또한 `30`입니다. Security Hub에서 기본값을 `14`로 변경하는 경우 이 예제의 파라미터는 해당 변경 내용을 추적하지 않습니다. 값은 `30`으로 유지됩니다.

파라미터의 기본 Security Hub 값에 대한 업데이트를 추적하려면 `ValueType` 필드를 `CUSTOM` 대신 `DEFAULT`로 설정하세요. 자세한 정보는 단일 계정 및 리전에서 기본 파라미터 값으로 되돌리기을 참조하세요.

파라미터 값을 변경하면 새 값을 기반으로 제어를 평가하는 새 보안 검사도 트리거됩니다. 그런 다음 Security Hub는 새 값을 기반으로 새로운 제어 결과를 생성합니다. 제어 결과를 정기적으로 업데이트

하는 동안 Security Hub는 새 파라미터 값도 사용합니다. 제어의 파라미터 값을 변경했지만 제어가 포함된 표준을 활성화하지 않은 경우 Security Hub는 새 값을 사용하여 보안 검사를 수행하지 않습니다. Security Hub가 새 파라미터 값을 기반으로 제어를 평가하려면 관련 표준을 하나 이상 활성화해야 합니다.

사용자 지정 파라미터 값은 활성화된 표준 전체에 적용됩니다. 현재 리전에서 지원되지 않는 제어의 파라미터는 사용자 지정할 수 없습니다. 개별 제어의 리전별 제한 목록은 제어 기능에 대한 리전별 제한 섹션을 참조하세요.

제어 파라미터 사용자 지정

제어 파라미터의 사용자 지정 지침은 중앙 구성을 사용하는지 여부에 따라 달라집니다. 중앙 구성은 위임된 Security Hub 관리자가 조직의 계정 및 OU (조직 구성 단위) AWS 리전전반에서 Security Hub 기능을 관리하는 데 사용할 수 있는 기능입니다.

조직에서 중앙 구성을 사용하는 경우 위임된 관리자는 사용자 지정 제어 파라미터가 포함된 구성 정책을 만들 수 있습니다. 이러한 정책은 중앙에서 관리되는 구성원 계정 및 OU에 연결할 수 있으며 홈 리전 및 연결된 모든 리전에 적용됩니다. 또한 위임된 관리자는 하나 이상의 계정을 자체 관리형 계정으로 지정할 수 있으며, 이렇게 하면 계정 소유자가 각 리전에서 개별적으로 자체 파라미터를 구성할 수 있습니다. 조직에서 중앙 구성을 사용하지 않는 경우 각 계정 및 리전에서 제어 파라미터를 개별적으로 사용자 지정해야 합니다.

다중 계정 및 리전에서 제어 파라미터 사용자 지정

중앙 구성을 사용하면 다중 계정 및 리전의 중앙 관리형 계정 및 OU에 대한 제어 파라미터를 사용자 지정할 수 있습니다. 중앙 구성을 사용하면 조직의 여러 부분에 걸쳐 제어 파라미터 값을 조정할 수 있으므로 중앙 구성을 사용하는 것이 좋습니다. 예를 들어 모든 테스트 계정은 특정 파라미터 값을 사용하고 모든 프로덕션 계정은 다른 값을 사용할 수 있습니다.

중앙 구성을 사용하는 조직의 Security Hub 위임된 관리자인 경우 원하는 방법을 선택하고 단계에 따라 다중 계정 및 리전의 제어 파라미터를 사용자 지정합니다.

Security Hub console

다중 계정 및 리전의 제어 파라미터를 사용자 지정하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에 로그인했는지 확인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭을 선택합니다.

4. 사용자 지정 파라미터가 포함된 새 구성 정책을 만들려면 정책 생성을 선택합니다. 기존 구성 정책에서 사용자 지정 파라미터를 지정하려면 정책을 선택한 다음 편집을 선택합니다.

   사용자 지정 파라미터를 사용하여 새 구성 정책을 만들려면

   1. 사용자 지정 정책 섹션에서 활성화하려는 보안 표준 및 제어를 선택합니다.
   2. 제어 파라미터 사용자 지정을 선택합니다.
   3. 제어를 선택한 다음 하나 이상의 파라미터에 대한 사용자 지정 값을 지정합니다.
   4. 더 많은 제어에 사용할 파라미터를 사용자 지정하려면 추가 제어 사용자 지정을 선택합니다.
   5. 계정 섹션에서 정책을 적용할 계정 또는 OU를 선택합니다.
   6. 다음을 선택합니다.
   7. 정책 생성 및 적용을 선택합니다. 홈 리전 및 연결된 모든 리전에서 이 작업은 이 구성 정책과 연결된 계정 및 OU의 기존 구성 설정보다 우선합니다. 계정과 OU는 상위로부터의 직접 적용 또는 상속을 통해 구성 정책에 연결할 수 있습니다.

   기존 구성 정책에 사용자 지정 파라미터를 추가하거나 편집하려면

   1. 제어 섹션의 사용자 지정 정책에서 원하는 새 사용자 지정 파라미터 값을 지정합니다.
   2. 이 정책의 제어 파라미터를 처음으로 사용자 지정하는 경우 제어 파라미터 사용자 지정을 선택한 다음 사용자 지정할 제어를 선택합니다. 더 많은 제어에 사용할 파라미터를 사용자 지정하려면 추가 제어 사용자 지정을 선택합니다.
   3. 계정 섹션에서 정책을 적용할 계정 또는 OU를 확인합니다.
   4. 다음을 선택합니다.
   5. 변경 내용을 검토하고 올바른지 확인합니다. 완료하면 정책 저장 및 적용을 선택합니다. 홈 리전 및 연결된 모든 리전에서 이 작업은 이 구성 정책과 연결된 계정 및 OU의 기존 구성 설정보다 우선합니다. 계정과 OU는 상위로부터의 직접 적용 또는 상속을 통해 구성 정책에 연결할 수 있습니다.

Security Hub API

다중 계정 및 리전의 제어 파라미터를 사용자 지정하려면

사용자 지정 파라미터를 사용하여 새 구성 정책을 만들려면

1. 홈 리전의 위임된 관리자 계정에서 CreateConfigurationPolicy API를 호출합니다.

2. `SecurityControlCustomParameters` 객체에는 사용자 지정하려는 각 제어의 식별자를 입력합니다.
3. `Parameters` 객체에는 사용자 지정하려는 각 파라미터의 이름을 입력합니다. 사용자 지정하는 각 파라미터의 경우 `ValueType`에 대해 `CUSTOM`을 입력합니다. `Value`에는 파라미터의 데이터 유형과 사용자 지정 값을 제공합니다. `ValueType`이 `CUSTOM`인 경우 `Value` 필드를 비워 둘 수 없습니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다. GetSecurityControlDefinition API를 호출하여 제어에 지원되는 파라미터, 데이터 유형 및 유효한 값을 찾을 수 있습니다.

기존 구성 정책에서 사용자 지정 파라미터를 추가하거나 편집하려면

1. 홈 리전의 위임된 관리자 계정에서 UpdateConfigurationPolicy API를 호출합니다.
2. `Identifier` 필드에는 업데이트하려는 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. `SecurityControlCustomParameters` 객체에는 사용자 지정하려는 각 제어의 식별자를 입력합니다.
4. `Parameters` 객체에는 사용자 지정하려는 각 파라미터의 이름을 입력합니다. 사용자 지정하는 각 파라미터의 경우 `ValueType`에 대해 `CUSTOM`을 입력합니다. `Value`에는 파라미터의 데이터 유형과 사용자 지정 값을 제공합니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다. GetSecurityControlDefinition API를 호출하여 제어에 지원되는 파라미터, 데이터 유형 및 유효한 값을 찾을 수 있습니다.

새 구성 정책을 생성하기 위한 API 요청 예시:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
```

```
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

다중 계정 및 리전의 제어 파라미터를 사용자 지정하려면

사용자 지정 파라미터를 사용하여 새 구성 정책을 만들려면

1. 홈 리전의 위임된 관리자 계정에서 create-configuration-policy 명령을 실행합니다.
2. `SecurityControlCustomParameters` 객체에는 사용자 지정하려는 각 제어의 식별자를 입력합니다.
3. `Parameters` 객체에는 사용자 지정하려는 각 파라미터의 이름을 입력합니다. 사용자 지정하는 각 파라미터의 경우 `ValueType`에 대해 `CUSTOM`을 입력합니다. `Value`에는 파라미터의 데이터 유형과 사용자 지정 값을 제공합니다. `ValueType`이 `CUSTOM`인 경우 `Value` 필드를 비워 둘 수 없습니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다. get-security-control-definition 명령을 실행하여 제어에 지원되는 파라미터, 데이터 유형 및 유효한 값을 찾을 수 있습니다.

기존 구성 정책에서 파라미터를 추가 또는 편집하려면

1. 기존 구성 정책에 사용자 지정 입력 파라미터를 추가하거나 업데이트하려면 홈 리전의 위임된 관리자 계정에서 update-configuration-policy 명령을 실행합니다.

2. `identifier` 필드에는 업데이트하려는 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. `SecurityControlCustomParameters` 객체에는 사용자 지정하려는 각 제어의 식별자를 입력합니다.
4. `Parameters` 객체에는 사용자 지정하려는 각 파라미터의 이름을 입력합니다. 사용자 지정하는 각 파라미터의 경우 `ValueType`에 대해 `CUSTOM`을 입력합니다. `Value`에는 파라미터의 데이터 유형과 사용자 지정 값을 제공합니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다. get-security-control-definition 명령을 실행하여 제어에 지원되는 파라미터, 데이터 유형 및 유효한 값을 찾을 수 있습니다.

새 구성 정책을 만들기 위한 명령 예시:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

단일 계정 및 리전의 제어 파라미터 사용자 지정

중앙 구성을 사용하지 않거나 자체 관리형 계정이 있는 경우 한 번에 한 리전의 계정에 대한 제어 파라미터를 사용자 지정할 수 있습니다.

원하는 방법을 선택하고 단계에 따라 제어 파라미터를 사용자 지정하세요. 변경 사항은 현재 리전의 계정에만 적용됩니다. 추가 리전의 제어 파라미터를 사용자 지정하려면 파라미터를 사용자 지정하려는 각 추가 계정 및 리전에서 다음 단계를 반복합니다. 동일한 제어가 리전마다 다른 파라미터 값을 사용할 수 있습니다.

Security Hub console

하나의 계정 및 리전에서 제어 파라미터를 사용자 지정하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다. 테이블에서 사용자 지정 파라미터를 지원하고 파라미터를 변경하고자 하는 제어를 선택합니다. 사용자 지정 파라미터 열에는 사용자 지정 파라미터를 지원하는 제어가 표시됩니다.
3. 제어의 세부 정보 페이지에서 파라미터 탭을 선택한 다음 편집을 선택합니다.
4. 변경하고자 하는 파라미터를 지정합니다.
5. 변경 사유 섹션에서 파라미터를 사용자 지정하는 이유를 선택할 수도 있습니다.
6. 저장을 선택합니다.

Security Hub API

하나의 계정 및 리전에서 제어 파라미터를 사용자 지정하려면

1. UpdateSecurityControl API를 호출합니다.
2. `SecurityControlId`에 사용자 지정하려는 제어의 ID를 입력합니다.
3. `Parameters` 객체에는 사용자 지정하려는 각 파라미터의 이름을 입력합니다. 사용자 지정하는 각 파라미터의 경우 `ValueType`에 대해 `CUSTOM`을 입력합니다. `Value`에는 파라미터의 데이터 유형과 사용자 지정 값을 제공합니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다. GetSecurityControlDefinition API를 호출하여 제어에 지원되는 파라미터, 데이터 유형 및 유효한 값을 찾을 수 있습니다.
4. 필요에 따라 `LastUpdateReason`에서 제어 파라미터를 사용자 지정하는 이유를 입력합니다.

API 요청 예:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 15
            }
        }
```

```
    },
    "LastUpdateReason": "Internal compliance requirement"
}
```

AWS CLI

하나의 계정 및 리전에서 제어 파라미터를 사용자 지정하려면

1. update-security-control 명령을 실행합니다.
2. `security-control-id`에 사용자 지정하려는 제어의 ID를 입력합니다.
3. `parameters` 객체에는 사용자 지정하려는 각 파라미터의 이름을 입력합니다. 사용자 지정하는 각 파라미터의 경우 `ValueType`에 대해 `CUSTOM`을 입력합니다. `Value`에는 파라미터의 데이터 유형과 사용자 지정 값을 제공합니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다. get-security-control-definition 명령을 실행하여 제어에 지원되는 파라미터, 데이터 유형 및 유효한 값을 찾을 수 있습니다.
4. 필요에 따라 `last-update-reason`에서 제어 파라미터를 사용자 지정하는 이유를 입력합니다.

명령 예시:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

제어 파라미터 상태 확인

제어 파라미터의 변경 상태를 검증하고 확인하는 것이 중요합니다. 이렇게 하면 제어가 예상대로 작동하고 의도한 보안 가치를 제공할 수 있습니다. 파라미터 업데이트가 성공했는지 확인하려면 Security Hub 콘솔에서 제어의 세부 정보를 검토할 수 있습니다. 콘솔에서 세부 정보를 표시할 제어를 선택합니다. 파라미터 탭은 파라미터의 변경 상태를 보여줍니다.

프로그래밍 방식으로, 파라미터 업데이트 요청이 유효한 경우, BatchGetSecurityControls 작업에 대한 응답으로 `UpdateStatus` 필드 값은 `UPDATING`입니다. 즉, 업데이트는 유효했지만 업데이트된 파라

미터 값이 아직 결과에 포함되어 있지 않을 수 있습니다. `UpdateState` 값이 `READY`로 변경되면 업데이트된 파라미터 값이 결과에 포함되기 시작합니다.

이 `UpdateSecurityControl` 작업은 잘못된 파라미터 값에 대한 `InvalidInputException` 응답을 반환합니다. 응답은 실패 이유에 대한 추가 세부 정보를 제공합니다. 예를 들어, 파라미터의 유효 범위를 벗어나는 값을 지정했을 수 있습니다. 또는 올바른 데이터 유형을 사용하지 않는 값을 지정했을 수 있습니다. 올바른 입력과 함께 요청을 다시 제출하세요. 파라미터 업데이트가 실패하는 경우 Security Hub는 파라미터의 현재 값을 유지합니다.

매개 변수 값을 업데이트하려고 할 때 내부 오류가 발생하는 경우 Security Hub는 AWS Config 활성화한 경우 자동으로 재시도합니다. 자세한 정보는 구성 AWS Config을 참조하세요.

제어 파라미터 검토

계정에서 개별 제어 파라미터의 현재 값을 검토할 수 있습니다. 중앙 구성을 사용하는 경우 위임된 Security Hub 관리자가 구성 정책에 지정된 파라미터 값을 검토할 수도 있습니다.

원하는 방법을 선택하고 단계에 따라 현재 제어 파라미터 값을 검토하세요.

Security Hub console

현재 파라미터 값을 검토하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다. 제어를 선택합니다.
3. 파라미터 탭을 선택합니다. 이 탭에는 제어의 현재 파라미터 값이 표시됩니다.

Security Hub API

현재 파라미터 값을 검토하려면

BatchGetSecurityControls API를 호출하고 하나 이상의 보안 제어 ID 또는 ARN을 제공하세요. 응답의 `Parameters` 객체에는 지정된 제어의 현재 파라미터 값이 표시됩니다.

API 요청 예:

```
{
    "SecurityControlIds": ["APIGateway.1", "CloudWatch.15", "IAM.7"]
}
```

AWS CLI

현재 파라미터 값을 검토하려면

batch-get-security-controls 명령을 실행하고 하나 이상의 보안 제어 ID 또는 ARN을 제공합니다. 응답의 `Parameters` 객체에는 지정된 제어의 현재 파라미터 값이 표시됩니다.

명령 예시:

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

중앙 구성 정책에서 현재 파라미터 값을 보려면 원하는 방법을 선택하세요.

Security Hub console

구성 정책의 현재 파라미터 값을 검토하려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭에서 구성 정책을 선택한 다음 세부 정보 보기를 선택합니다. 그러면 현재 파라미터 값을 포함한 정책 세부 정보가 나타납니다.

Security Hub API

구성 정책의 현재 파라미터 값을 검토하려면

1. 홈 리전의 위임된 관리자 계정에서 GetConfigurationPolicy API를 호출합니다.
2. 세부 정보를 보려는 구성 정책의 ARN 또는 ID를 입력합니다. 응답에는 현재 파라미터 값이 포함됩니다.

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

```
}
```

AWS CLI

구성 정책의 현재 파라미터 값을 검토하려면

1. 홈 리전의 위임된 관리자 계정에서 get-configuration-policy 명령을 실행합니다.
2. 세부 정보를 보려는 구성 정책의 ARN 또는 ID를 입력합니다. 응답에는 현재 파라미터 값이 포함됩니다.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

제어 결과에는 현재 파라미터 값도 표시됩니다. AWS 보안 탐지 형식 (ASFF) 구문에서는 이러한 값이 `Compliance` 객체의 `Parameters` 필드에 표시됩니다. Security Hub 콘솔에서 결과를 검토하려면 탐색 창에서 조사 결과를 선택합니다. 결과를 프로그래밍 방식으로 검토하려면 GetFindings 작업을 사용하세요.

> **Note**
>
> 사용자 지정 제어 파라미터 기능이 출시되면 Security Hub는 `Parameters` ASFF 필드를 포함하도록 기존 제어 결과를 업데이트합니다. 이 작업은 최대 24시간까지 걸릴 수 있습니다.

기본 제어 파라미터 값으로 되돌리기

제어 파라미터는 Security Hub에서 정의하는 기본값을 가질 수 있습니다. 진화하는 보안 모범 사례를 반영하여 파라미터의 기본값을 업데이트할 수 있습니다. 제어 파라미터에 사용자 지정 값을 지정하지 않은 경우 제어는 해당 업데이트를 자동으로 추적하고 새 기본값을 사용합니다.

제어의 기본 파라미터 값을 사용하도록 되돌릴 수 있습니다. 이 작업을 수행하는 방법은 중앙 구성을 사용하는지 여부에 따라 달라집니다.

> **Note**
>
> 모든 제어 파라미터에 Security Hub 기본값이 있는 것은 아닙니다. 이러한 경우 `ValueType`를 `DEFAULT`로 설정하면 Security Hub에서 사용하는 특정 기본값이 없습니다. 대신 Security Hub는 사용자 지정 값이 없는 경우 파라미터를 무시합니다.

다중 계정 및 리전에서 기본 파라미터 값으로 되돌리기

중앙 구성을 사용하는 경우 다중 계정 및 리전의 중앙 관리형 계정 및 OU에 대한 제어 파라미터를 되돌릴 수 있습니다.

원하는 방법을 선택하고 단계에 따라 중앙 구성을 사용하여 다중 계정 및 리전의 기본 파라미터 값으로 되돌리세요.

Security Hub console

다중 계정 및 리전의 기본 파라미터 값으로 되돌리려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.

   홈 리전에서 Security Hub 위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭을 선택합니다.
4. 정책을 선택한 다음 편집을 선택합니다.
5. 사용자 지정 정책의 제어 섹션에는 사용자 지정 파라미터를 지정한 제어 목록이 표시됩니다.
6. 되돌릴 파라미터 값이 하나 이상 있는 제어를 찾습니다. 그런 다음 제거를 선택하여 기본값으로 되돌립니다.
7. 계정 섹션에서 정책을 적용할 계정 또는 OU를 확인합니다.
8. 다음을 선택합니다.
9. 변경 내용을 검토하고 올바른지 확인합니다. 완료하면 정책 저장 및 적용을 선택합니다. 홈 리전 및 연결된 모든 리전에서 이 작업은 이 구성 정책과 연결된 계정 및 OU의 기존 구성 설정보다 우선합니다. 계정과 OU는 상위로부터의 직접 적용 또는 상속을 통해 구성 정책에 연결할 수 있습니다.

Security Hub API

다중 계정 및 리전의 기본 파라미터 값으로 되돌리려면

1. 홈 리전의 위임된 관리자 계정에서 UpdateConfigurationPolicy API를 호출합니다.
2. `Identifier` 필드에는 업데이트하려는 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. `SecurityControlCustomParameters` 객체에는 하나 이상의 파라미터를 되돌리려는 각 제어의 식별자를 입력합니다.
4. `Parameters` 객체에서 되돌리려는 각 파라미터에 대해 `ValueType` 필드에 `DEFAULT`를 입력합니다. `ValueType`이 `DEFAULT`로 설정된 경우 `Value` 필드에 값을 입력할 필요가 없습니다. 요청에 값이 포함된 경우 Security Hub는 해당 값을 무시합니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다.

> **Warning**
>
> `SecurityControlCustomParameters` 필드에서 제어 객체를 생략하면 Security Hub는 제어에 대한 모든 사용자 지정 파라미터를 기본값으로 되돌립니다. `SecurityControlCustomParameters`의 목록이 완전히 비어 있으면 모든 제어의 사용자 지정 파라미터를 기본값으로 되돌립니다.

API 요청 예:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "TestConfigurationPolicy",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Revert ACM.1 parameter to default value",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
```

```
            "SecurityControlsConfiguration": {
               "DisbledSecurityControlIdentifiers": [
                   "CloudTrail.2"
               ],
               "SecurityControlCustomParameters": [
                   {
                       "SecurityControlId": "ACM.1",
                       "Parameters": {
                           "daysToExpiration": {
                               "ValueType": "DEFAULT"
                           }
                       }
                   }
               ]
            }
        }
    }
}
```

AWS CLI

다중 계정 및 리전의 기본 파라미터 값으로 되돌리려면

1. 홈 리전의 위임된 관리자 계정에서 update-configuration-policy 명령을 실행합니다.
2. `identifier` 필드에는 업데이트하려는 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. `SecurityControlCustomParameters` 객체에는 하나 이상의 파라미터를 되돌리려는 각 제어의 식별자를 입력합니다.
4. `Parameters` 객체에서 되돌리려는 각 파라미터에 대해 `ValueType` 필드에 `DEFAULT`를 입력합니다. `ValueType`이 `DEFAULT`로 설정된 경우 `Value` 필드에 값을 입력할 필요가 없습니다. 요청에 값이 포함된 경우 Security Hub는 해당 값을 무시합니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다.

> **Warning**
>
> `SecurityControlCustomParameters` 필드에서 제어 객체를 생략하면 Security Hub는 제어에 대한 모든 사용자 지정 파라미터를 기본값으로 되돌립니다. `SecurityControlCustomParameters`의 목록이 완전히 비어 있으면 모든 제어의 사용자 지정 파라미터를 기본값으로 되돌립니다.

명령 예시:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

단일 계정 및 리전에서 기본 파라미터 값으로 되돌리기

중앙 구성을 사용하지 않거나 자체 관리형 계정이 있는 경우 한 번에 한 리전의 계정에 대한 기본 파라미터 값을 사용하도록 되돌릴 수 있습니다.

원하는 방법을 선택하고 단계에 따라 단일 리전 계정의 기본 파라미터 값으로 되돌리세요. 추가 리전의 기본 파라미터 값으로 되돌리려면 각 추가 리전에서 이 단계를 반복하세요.

> **Note**
>
> Security Hub를 비활성화하면 사용자 지정 제어 파라미터가 재설정됩니다. 나중에 Security Hub를 다시 활성화하면 모든 제어가 기본 파라미터 값을 사용하여 시작합니다.

Security Hub console

한 계정 및 리전의 기본 파라미터 값으로 되돌리려면

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다. 기본 파라미터 값으로 재설정할 제어를 선택합니다.

3. Parameters 탭에서 제어 파라미터 옆의 사용자 지정을 선택합니다. 그런 다음 사용자 지정 제거를 선택합니다. 이제 이 파라미터는 기본 Security Hub 값을 사용하며 기본값에 대한 향후 업데이트를 추적합니다.
4. 되돌리려는 각 파라미터 값에 대해 이전 단계를 반복합니다.

Security Hub API

한 계정 및 리전의 기본 파라미터 값으로 되돌리려면

1. UpdateSecurityControl API를 호출합니다.
2. SecurityControlId에서 파라미터를 되돌리려는 제어의 ARN 또는 ID를 입력합니다.
3. Parameters 객체에서 되돌리려는 각 파라미터에 대해 ValueType 필드에 DEFAULT를 입력합니다. ValueType이 DEFAULT로 설정된 경우 Value 필드에 값을 입력할 필요가 없습니다. 요청에 값이 포함된 경우 Security Hub는 해당 값을 무시합니다.
4. 필요에 따라 LastUpdateReason에서 기본 파라미터 값으로 되돌릴 이유를 입력합니다.

API 요청 예:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "DEFAULT"
        },
    "LastUpdateReason": "New internal requirement"
}
```

AWS CLI

한 계정 및 리전의 기본 파라미터 값으로 되돌리려면

1. update-security-control 명령을 실행합니다.
2. security-control-id에서 파라미터를 되돌리려는 제어의 ARN 또는 ID를 입력합니다.
3. parameters 객체에서 되돌리려는 각 파라미터에 대해 ValueType 필드에 DEFAULT를 입력합니다. ValueType이 DEFAULT로 설정된 경우 Value 필드에 값을 입력할 필요가 없습니다. 요청에 값이 포함된 경우 Security Hub는 해당 값을 무시합니다.
4. 필요에 따라 last-update-reason에서 기본 파라미터 값으로 되돌릴 이유를 입력합니다.

명령 예시:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

사용자 지정 파라미터를 지원하는 제어

사용자 지정 파라미터를 지원하는 보안 제어 목록을 보려면 Security Hub 콘솔의 제어 페이지 또는 Security Hub 제어 참조를 참조하세요. 프로그래밍 방식으로 이 목록을 검색하려면 ListSecurityControlDefinitions 작업을 사용하면 됩니다. 응답에서 `CustomizableProperties` 객체는 사용자 지정 가능한 파라미터를 지원하는 제어를 나타냅니다.

비활성화할 수 있는 Security Hub 제어

노이즈 감지를 줄이고 비용을 제한하려면 일부 AWS Security Hub 컨트롤을 비활성화하는 것이 좋습니다.

글로벌 리소스를 처리하는 제어

일부는 글로벌 리소스를 AWS 서비스 지원하므로 어느 곳에서나 AWS 리전리소스에 액세스할 수 있습니다. 비용을 절약하기 위해 한 지역을 제외한 모든 지역의 글로벌 리소스 기록을 비활성화할 수 있습니다. AWS Config이렇게 한 후에도 Security Hub는 제어가 활성화된 모든 리전에서 보안 검사를 계속 실행하고 리전별 계정당 검사 횟수에 따라 요금을 부과합니다. 따라서 노이즈 탐지를 줄이고 Security Hub 비용을 절약하려면 글로벌 리소스를 기록하는 지역을 제외한 모든 지역의 글로벌 리소스를 포함하는 컨트롤도 비활성화해야 합니다.

컨트롤에 글로벌 리소스가 포함되지만 한 지역에서만 사용할 수 있는 경우 해당 지역에서 컨트롤을 사용하지 않도록 설정하면 기본 리소스에 대한 검색 결과를 얻을 수 없습니다. 이 경우 컨트롤을 활성화된 상태로 유지하는 것이 좋습니다. 지역 간 집계를 사용하는 경우 컨트롤을 사용할 수 있는 지역은 집계 지역 또는 연결된 지역 중 하나여야 합니다. 다음 컨트롤에는 글로벌 리소스가 포함되지만 단일 지역에서만 사용할 수 있습니다.

- 모든 CloudFront 제어 — 미국 동부 (버지니아 북부) 에서만 사용 가능
- GlobalAccelerator.1 — 미국 서부 (오레곤) 에서만 사용 가능

- Route53.2 — 미국 동부 (버지니아 북부) 에서만 이용 가능
- WAF.1, WAF.6, WAF.7 및 WAF.8 — 미국 동부 (버지니아 북부) 에서만 사용 가능

> **Note**
>
> 중앙 구성을 사용하는 경우 Security Hub는 홈 지역을 제외한 모든 지역의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다. 구성 정책을 통해 사용하도록 선택한 기타 제어 기능은 사용 가능한 모든 지역에서 사용할 수 있습니다. 이러한 컨트롤에 대한 검색 결과를 한 지역으로만 제한하려면 AWS Config 레코더 설정을 업데이트하고 홈 지역을 제외한 모든 지역에서 글로벌 리소스 기록을 끄면 됩니다. 중앙 구성을 사용하면 홈 지역 및 연결된 지역에서 사용할 수 없는 컨트롤에 대한 적용 범위가 부족해집니다. 중앙 구성에 대한 자세한 내용은 중앙 구성 작동 방식 섹션을 참조하세요.

주기적 일정 유형의 제어의 경우 청구를 방지하려면 Security Hub에서 이를 비활성화해야 합니다. AWS Config 매개변수를 `includeGlobalResourceTypes` 로 설정해도 주기적인 Security Hub 제어에는 영향을 `false` 주지 않습니다.

다음은 글로벌 리소스와 관련된 Security Hub 컨트롤 목록입니다.

- [계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정
- [Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.

- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.10] IAM 사용자를 위한 암호 정책은 엄격한 기준을 적용해야 합니다. AWS Config
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.

- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

CloudTrail 로깅을 처리하는 컨트롤

이 컨트롤은 AWS Key Management Service (AWS KMS) 를 사용하여 AWS CloudTrail 트레일 로그를 암호화하는 작업을 처리합니다. 중앙 집중식 로깅 계정에 이러한 추적을 기록하는 경우 중앙 집중식 로깅이 수행되는 계정 및 리전에서만 이 제어를 활성화하면 됩니다.

> **Note**
>
> 중앙 구성을 사용하는 경우 제어의 활성화 상태를 홈 리전 및 연결된 리전 전체에 걸쳐 조정합니다. 일부 리전에서는 제어를 비활성화하고 다른 리전에서는 활성화할 수 없습니다. 이 경우 다음 제어에서 결과를 표시하지 않도록 하여 검색 노이즈를 줄이세요.

- [CloudTrail.2] 저장 중 암호화가 CloudTrail 활성화되어 있어야 합니다.

경보를 처리하는 CloudWatch 컨트롤

예외 항목 탐지에 Amazon GuardDuty CloudWatch 경보 대신 Amazon을 사용하려는 경우 경보에 초점을 맞춘 이러한 제어를 비활성화할 수 있습니다. CloudWatch

- [CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.
- [CloudWatch.2] 승인되지 않은 API 호출에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.3] MFA를 사용하지 않는 관리 콘솔 로그인에 대한 로그 메트릭 필터 및 경보가 있는지 확인

- [CloudWatch.4] IAM 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.5] 기간 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오 CloudTrail AWS Config.
- [CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제를 위한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.8] S3 버킷 정책 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.9] AWS Config 구성 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.10] 보안 그룹 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.11] 네트워크 액세스 제어 목록 (NACL) 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.12] 네트워크 게이트웨이 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.13] 라우팅 테이블 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인하십시오.
- [CloudWatch.14] VPC 변경에 대한 로그 메트릭 필터 및 경보가 있는지 확인

제어에 대한 세부 정보 보기

각 AWS Security Hub 컨트롤에 대해 유용한 세부 정보 페이지를 표시할 수 있습니다.

제어 세부 정보 페이지 상단에는 다음을 포함한 제어의 개요가 표시됩니다.

- 활성화 상태 - 페이지 상단에는 하나 이상의 구성원 계정에서 하나 이상의 표준에 대해 제어가 활성화되어 있는지 여부가 표시됩니다. 집계 영역을 설정한 경우 하나 이상의 리전에서 하나 이상의 표준에 대해 집계 영역을 활성화하면 제어가 활성화됩니다. 제어가 비활성화된 경우 이 페이지에서 활성화할 수 있습니다. 제어가 활성화된 경우 이 페이지에서 비활성화할 수 있습니다. 자세한 내용은 the section called “모든 표준에서 제어 활성화 및 비활성화”을 참조하십시오.
- 제어 상태 - 이 상태는 제어 조사 결과의 규정 준수 상태를 기반으로 제어 성능을 요약합니다. Security Hub는 일반적으로 Security Hub 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 초기 제어 상태를 생성합니다. 상태는 해당 페이지를 방문할 때 활성화되는 제어에만 사용할 수 있습니다. `UpdateStandardsControl` API 작업을 사용하여 제어를 활성화하거나 비활성화할 수 있습니다. 또한 제어 상태가 나타나도록 AWS Config 리소스 기록을 구성해야 합니다. 제어 상태가 처음으로 생성된 후 Security Hub는 이전 24시간 동안의 조사 결과를 기반으로 24시간마

다 제어 상태를 업데이트합니다. Security Hub는 표준 세부 정보 페이지와 제어 세부 정보 페이지에서 상태가 마지막으로 업데이트된 시간을 나타내는 타임스탬프를 표시합니다.

관리자 계정에는 관리자 계정과 구성원 계정 전체의 집계된 제어 상태가 표시됩니다. 집계 영역을 설정한 경우 제어 상태에는 연결된 모든 리전의 조사 결과가 포함됩니다. 제어 상태에 대한 자세한 내용은 the section called “규정 준수 상태 및 제어 상태”을 참조하십시오.

> **Note**
>
> 중국 리전 및 AWS GovCloud (US) Region에서 최초 제어 상태가 생성되는 경우 제어 활성화 후 최대 24시간이 소요될 수 있습니다.

표준 및 요구 사항 탭에는 제어를 사용할 수 있는 표준과 다양한 규정 준수 프레임워크의 제어 관련 요구 사항이 나열됩니다.

세부 정보 페이지 하단에는 제어에 대한 활성 조사 결과에 대한 정보가 포함되어 있습니다. 제어 조사 결과는 제어에 대한 보안 검사를 통해 생성됩니다. 제어 조사 결과 목록에는 보관된 조사 결과가 포함되지 않습니다.

결과 목록에는 목록의 여러 하위 집합을 표시하는 탭이 사용됩니다. 대부분의 탭에서 조사 결과 목록에는 워크플로 상태가 `NEW`, `NOTIFIED` 또는 `RESOLVED`인 조사 결과가 표시됩니다. 별도의 탭에는 `SUPPRESSED` 조사 결과가 표시됩니다.

각 검색 결과에 대해 목록은 규정 준수 상태 및 관련 리소스와 같은 결과 세부 정보에 대한 액세스를 제공합니다. 또한 각 조사 결과의 워크플로 상태를 설정하고 조사 결과를 사용자 지정 작업으로 전송할 수 있습니다. 자세한 내용은 the section called “제어 조사 결과 보기 및 조치 수행”을 참조하십시오.

제어에 대한 세부 정보 보기

원하는 액세스 방법을 선택하고 다음 단계에 따라 제어의 세부 정보를 확인하십시오. 세부 정보는 현재 계정 및 리전에 적용되며 다음을 포함합니다.

- 제어의 제목 및 설명
- 실패한 제어 조사 결과에 대한 수정 지침 링크
- 제어의 심각도
- 제어의 활성화 상태

- (콘솔에서) 제어에 대한 최근 조사 결과 목록. Security Hub API를 사용하는 AWS CLI경우 또는 제어 결과를 검색하는 GetFindings데 사용합니다.

Security Hub console

1. https://console.aws.amazon.com/securityhub/ 에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다.
3. 제어를 선택합니다.

Security Hub API

1. ListSecurityControlDefinitions를 실행하고 하나 이상의 표준 ARN을 입력하여 해당 표준에 대한 제어 ID 목록을 가져옵니다. 표준 ARN을 가져오려면 DescribeStandards를 실행하십시오. 표준 ARN을 입력하지 않는 경우 이 API는 모든 Security Hub 제어 ID를 반환합니다. 이 API는 이러한 기능 릴리스 이전에 존재했던 표준 기반 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

   요청 예:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. 실행하면 현재 AWS 계정 및 에 BatchGetSecurityControls 있는 하나 이상의 컨트롤에 대한 세부 정보를 볼 수 AWS 리전있습니다.

   요청 예:

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. list-security-control-definitions 명령을 실행하고 하나 이상의 표준 ARN을 입력하여 제어 ID 목록을 가져옵니다. 표준 ARN을 얻으려면 describe-standards 명령을 실행합니다. 표준 ARN을 입력하지 않는 경우 이 명령은 모든 Security Hub 제어 ID를 반환합니다.

이 명령은 이러한 기능 릴리스 이전에 존재했던 표준 기반 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. batch-get-security-controls 명령을 실행하여 현재 AWS 계정 및 AWS 리전에 있는 하나 이상의 제어에 대한 세부 정보를 가져옵니다.

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

제어 목록 필터링 및 정렬

제어 페이지에서 제어 목록을 볼 수 있습니다. 목록을 필터링하고 정렬하여 제어의 특정 하위 집합에 초점을 맞출 수 있습니다.

- 모두 활성화됨 (하나 이상의 활성화된 표준에서 활성화된 제어)
- 실패 (Failed 상태의 제어)
- 알 수 없음 (Unknown 상태의 제어)
- 통과 (Passed 상태의 제어)
- 비활성화됨 (모든 표준에서 비활성화된 제어)
- 데이터 없음 (조사 결과가 없는 제어)
- 모두 (모든 제어, 활성화 및 비활성화 모두, 제어 상태 또는 조사 결과 수에 관계 없음)

제어 상태에 대한 자세한 내용은 규정 준수 상태 및 제어 상태을 참조하십시오.

통합을 사용하고 AWS Security Hub 관리자 계정에 로그인한 경우, 모두 활성화 탭에는 하나 이상의 멤버 계정에서 활성화된 컨트롤이 포함됩니다. AWS Organizations 집계 영역을 설정한 경우 모든 활성화 탭에는 하나 이상의 연결된 리전에서 활성화된 제어가 포함됩니다.

기본적으로 실패 탭이 표시됩니다. 각 탭에서 제어는 기본적으로 심각도에 따라 심각부터 낮음까지 정렬됩니다. 제어 ID, 규정 준수 상태, 심각도 또는 실패한 검사 수를 기준으로 제어를 정렬할 수도 있습니다. 검색 창을 통해 특정 제어를 검색할 수 있습니다.

> **Tip**
>
> 제어 조사 결과를 기반으로 워크플로를 자동화하는 경우 `Title`나 `Description` 대신 `SecurityControlId` 또는 `SecurityControlArn` ASFF 필드를 필터로 사용하는 것이 좋습니다. 후자의 필드는 때때로 변경될 수 있지만 제어 ID 및 ARN은 정적 식별자입니다.

제어 옆의 옵션을 선택하면 제어가 현재 활성화되어 있는 표준을 표시하는 사이드 패널이 나타납니다. 또한 제어가 현재 비활성화되어 있는 표준도 확인할 수 있습니다. 이 패널에서는 모든 표준에서 제어를 비활성화하여 이를 비활성화할 수 있습니다. 표준 전반의 제어 기능 활성화 및 비활성화에 대한 자세한 내용은 모든 표준에서 제어 활성화 및 비활성화을 참조하십시오. 관리자 계정의 경우 사이드 패널에 표시된 정보는 모든 구성원 계정을 반영합니다.

Security Hub API에서 `ListSecurityControlDefinitions`를 실행하여 제어 ID 목록을 가져올 수 있습니다. 원하는 컨트롤 ID를 찾았으면 를 `BatchGetSecurityControls`실행하여 현재 AWS 계정 및 AWS 리전컨트롤의 해당 하위 집합에 대한 데이터를 가져오세요.

제어 조사 결과 보기 및 조치 수행

제어 세부 정보 페이지에는 제어에 대한 활성 조사 결과 목록이 표시됩니다. 이 목록에는 보관된 조사 결과가 포함되어 있지 않습니다.

제어 세부 정보 페이지는 결과 집계를 지원합니다. 집계 영역을 설정한 경우 제어 세부 정보 페이지의 제어 상태 및 보안 검사 목록에는 연결된 모든 AWS 리전의 검사가 포함됩니다.

이 목록은 조사 결과를 필터링하고 정렬하는 도구를 제공하므로 더 긴급한 조사 결과에 먼저 집중할 수 있습니다. 결과에는 관련 서비스 콘솔의 리소스 세부 정보로 연결되는 링크가 포함될 수 있습니다. AWS Config 규칙을 기반으로 하는 컨트롤의 경우 규칙 및 구성 일정에 대한 세부 정보를 볼 수 있습니다.

AWS Security Hub API를 사용하여 결과 목록을 검색할 수도 있습니다. 자세한 정보는 the section called “검색 결과 세부 정보 검토”을 참조하세요.

주제

- 제어 결과 및 결과 리소스에 대한 세부 정보 보기
- 샘플 제어 조사 결과
- 제어 조사 결과 필터링, 정렬 및 다운로드
- 제어 조사 결과에 대한 조치 취하기

제어 결과 및 결과 리소스에 대한 세부 정보 보기

AWS Security Hub 조사에 도움이 되도록 각 통제 결과에 대해 다음과 같은 세부 정보를 제공합니다.

- 사용자가 결과에 적용한 변경 내역
- 결과를 위한 `.json` 파일
- 결과와 관련된 리소스에 대한 정보
- 결과와 관련된 구성 규칙
- 사용자가 결과에 추가한 메모

다음 섹션에서는 이러한 세부 정보에 액세스하는 방법을 설명합니다.

결과 기록

결과 기록은 지난 90일 동안 결과에 대한 변경 사항을 추적할 수 있는 Security Hub 기능입니다.

조사 결과 기록은 제어 조사 결과 및 기타 Security Hub 조사 결과에 사용할 수 있습니다. 자세한 내용은 검색 결과 기록 검토을 참조하십시오.

결과에 대한 전체 .json 보기

검색 결과 전체 `.json`를 표시하고 다운로드할 수 있습니다.

`.json`를 표시하려면 Finding.json 열에서 아이콘을 선택합니다.

JSON 찾기 패널에서 다운로드를 선택하여 `.json`을 다운로드합니다.

결과 리소스에 대한 정보 보기

리소스 열에는 리소스 유형과 리소스 식별자가 포함됩니다.

리소스에 대한 정보를 표시하려면 리소스 식별자를 선택합니다. AWS 계정의 경우, 계정이 조직 구성원 계정이면 정보에는 계정 ID와 계정 이름이 모두 포함됩니다. 수동으로 초대된 계정의 경우 정보에는 계정 ID만 포함됩니다.

원래 서비스의 리소스를 볼 수 있는 권한이 있는 경우 리소스 식별자에 서비스 링크가 표시됩니다. 예를 들어 AWS 사용자의 경우 리소스 세부 정보는 IAM에서 사용자 세부 정보를 볼 수 있는 링크를 제공합니다.

리소스가 다른 계정에 있는 경우 Security Hub는 이를 알리는 메시지를 표시합니다.

결과 리소스의 구성 타임라인 보기

조사 방법 중 하나는 AWS Config의 리소스에 대한 구성 타임라인입니다.

결과 리소스에 대한 구성 타임라인을 볼 수 있는 권한이 있는 경우 결과 목록은 타임라인에 대한 링크를 제공합니다.

Security Hub는 리소스가 다른 계정에 있는 경우 알림 메시지를 표시합니다.

에서 구성 타임라인으로 이동하려면 AWS Config

1. 조사 열에서 아이콘을 선택합니다.
2. 메뉴에서 구성 타임라인을 선택합니다. 구성 타임라인에 액세스할 수 없는 경우 링크가 표시되지 않습니다.

검색 리소스의 AWS Config 규칙 보기

컨트롤이 규칙을 기반으로 하는 경우 AWS Config 규칙의 세부 정보를 보는 것도 좋습니다. AWS Config AWS Config 규칙 정보는 검사의 성공 또는 실패 이유를 더 잘 이해하는 데 도움이 될 수 있습니다.

컨트롤에 대한 AWS Config 규칙을 볼 수 있는 권한이 있는 경우 검색 결과 목록에 해당 AWS Config 규칙으로 연결되는 링크가 제공됩니다 AWS Config.

Security Hub는 리소스가 다른 계정에 있는 경우 알림 메시지를 표시합니다.

AWS Config 규칙으로 이동하려면

1. 조사 열에서 아이콘을 선택합니다.
2. 메뉴에서 Config 규칙을 선택합니다. 규칙에 액세스할 수 없는 경우 Config AWS Config 규칙은 연결되지 않습니다.

조사 결과에 대한 메모 보기

결과에 관련 메모가 있는 경우 업데이트됨 열에 메모 아이콘이 표시됩니다.

결과와 관련된 메모를 표시하려면

업데이트됨 열에서 노트 아이콘을 선택합니다.

샘플 제어 조사 결과

제어 조사 결과의 형식은 통합 제어 조사 결과를 설정했는지 여부에 따라 달라집니다. 이 기능을 켜면 Security Hub는 제어가 여러 활성 표준에 적용되는 경우에도 제어 검사를 위한 단일 결과를 생성합니다. 자세한 내용은 통합 제어 조사 결과을 참조하십시오.

다음 섹션에서는 샘플 제어 조사 결과를 보여줍니다. 여기에는 계정에서 통합 제어 조사 결과가 꺼진 경우 각 Security Hub 표준의 조사 결과와 해당 기능이 켜진 경우 표준 전반에 걸친 샘플 제어 조사 결과가 포함됩니다.

> **Note**
>
> 조사 결과는 중국 리전 및 AWS GovCloud (US) 리전의 다양한 필드와 값을 참조합니다. 자세한 내용은 ASFF 필드 및 값에 대한 통합의 영향을 참조하십시오.

통합 제어 조사 결과가 꺼져 있음

- AWS 기본 보안 모범 사례 (FSBP) 표준에 대한 샘플 결과
- 인터넷 보안 센터 (CIS) 재단 벤치마크 v1.2.0에 대한 샘플 결과 AWS
- 인터넷 보안 센터 (CIS) 재단 벤치마크 v1.4.0에 대한 샘플 결과 AWS
- 인터넷 보안 센터 (CIS) 재단 벤치마크 v3.0.0에 대한 샘플 결과 AWS
- NIST(국립 표준 기술 연구소)SP 800-53 개정 5에 대한 샘플 결과
- PCI DSS(지불 카드 산업 데이터 보안 표준)에 대한 샘플 결과
- 리소스 태깅 표준에 대한 샘플 검색 결과 AWS
- 서비스 관리 표준에 대한 샘플 검색 결과: AWS Control Tower

통합 제어 조사 결과가 켜져 있음

- 표준 전반의 샘플 결과

FSBP에 대한 샘플 결과

```
{
  "SchemaVersion": "2018-10-08",
```

```
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
```

```
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
```

```
}
```

CIS AWS 재단 벤치마크 v3.0.0에 대한 샘플 검색 결과


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
```

```
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
```

```
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

CIS 재단 벤치마크 v1.4.0에 대한 샘플 검색 결과 AWS

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies. AWS Key Management Service (KMS) is a managed service that helps create
 and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
```

```
 can be configured to leverage server side encryption (SSE) and AWS KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
```

```
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

CIS 재단 벤치마크 v1.2.0에 대한 샘플 검색 결과 AWS

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
```

```
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service (KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
```

```
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

NIST SP 800-53 개정 5에 대한 샘플 결과

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
```

```
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

```
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
```

```
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

PCI DSS에 대한 샘플 결과

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
 CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
```

```
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
```

```
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

리소스 태깅 표준에 대한 샘플 검색 AWS

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
```

```
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
```

```
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
            },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```


서비스 관리 표준에 대한 샘플 검색 결과: AWS Control Tower

> **Note**
>
> 이 표준은 에서 표준을 만든 AWS Control Tower 사용자인 경우에만 사용할 수 있습니다. AWS Control Tower자세한 정보는 서비스 관리형 표준: AWS Control Tower을 참조하세요.


```
{
```

```
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
```

```
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

표준 전반의 샘플 조사 결과(통합 제어 조사 결과가 켜진 경우)


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-10-06T02:18:23.076Z",
  "LastObservedAt": "2022-10-28T16:10:06.956Z",
  "CreatedAt": "2022-10-06T02:18:23.076Z",
  "UpdatedAt": "2022-10-28T16:10:00.093Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": "40",
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
```

```
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  }
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "PCI DSS v3.2.1/3.4",
        "CIS AWS Foundations Benchmark v1.2.0/2.7",
        "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
       { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
       { "StandardsId": "standards/pci-dss/v/3.2.1"},
       { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
       { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
       { "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
```

```
}
```

제어 조사 결과 필터링, 정렬 및 다운로드

필터링 탭을 사용하여 규정 준수 상태를 기반으로 제어 조사 결과 목록을 필터링할 수 있습니다. 다른 조사 결과 필드 값을 기준으로 목록을 필터링하고 목록에서 조사 결과를 다운로드할 수도 있습니다.

제어 결과 목록 필터링 및 정렬

모든 검사 탭에는 워크플로 상태가 NEW, NOTIFIED 또는 RESOLVED인 모든 활성 조사 결과가 나열됩니다. 기본적으로 목록은 실패한 조사 결과가 목록의 맨 위에 표시되도록 정렬됩니다. 이 정렬 순서를 사용하면 해결해야 할 조사 결과의 우선 순위를 정하는 데 도움이 됩니다.

실패, 알 수 없음, 통과 탭의 목록은 `Compliance.Status` 값을 기준으로 필터링됩니다. 또한 목록에는 워크플로 상태가 NEW, NOTIFIED 또는 RESOLVED인 활성 조사 결과만 포함됩니다.

숨김 탭에는 워크플로 상태가 SUPPRESSED인 활성 조사 결과 목록이 포함되어 있습니다.

각 탭에 내장된 필터 외에도 다음 필드의 값을 사용하여 목록을 필터링할 수 있습니다.

- 계정 ID
- 워크플로 상태
- 규정 준수 상태
- 리소스 ID
- 리소스 유형

열 중 하나를 사용하여 각 목록을 정렬할 수 있습니다.

제어 결과 목록 다운로드

보안 표준으로 이동하여 표준을 선택하면 해당 표준에 대한 제어 목록이 표시됩니다. 목록에서 컨트롤을 선택하면 컨트롤에 대한 결과 목록이 있는 컨트롤 세부 정보 페이지로 이동합니다. 여기에서 제어 조사 결과를 .csv 파일로 다운로드할 수 있습니다.

결과 목록을 필터링하면 필터와 일치하는 제어만 다운로드에 포함됩니다.

목록에서 특정 조사 결과를 선택하면 선택한 조사 결과만 다운로드에 포함됩니다.

조사 결과를 다운로드하려면 다운로드를 선택합니다. 현재 검색 결과 페이지가 다운로드됩니다.

제어 조사 결과에 대한 조치 취하기

조사의 현재 상태를 반영하기 위해 워크플로 상태를 설정합니다. 자세한 정보는 the section called “조사 결과에 대한 워크플로 상태 설정”을 참조하세요.

AWS Security Hub에서는 선택한 결과를 Amazon의 사용자 지정 작업에 보낼 수도 EventBridge 있습니다. 자세한 내용은 the section called “사용자 지정 작업에 조사 결과 전송”을(를) 참조하세요.

요약 대시보드 작업

AWS Security Hub 콘솔에서 요약 페이지의 대시보드를 사용하면 추가 분석 도구나 복잡한 쿼리 없이도 AWS 환경의 보안 문제 영역을 식별할 수 있습니다. 대시보드 레이아웃을 사용자 지정하고, 위젯을 추가 또는 제거하고, 데이터를 필터링하여 특정 관심 영역에 초점을 맞출 수 있습니다. 또한 필터 기준을 필터 세트로 저장하여 나중에 특정 유형의 데이터를 빠르게 검색할 수 있습니다.

대시보드를 사용자 지정하거나 데이터를 필터링하는 경우 Security Hub는 나중에 사용할 수 있도록 설정을 자동으로 저장합니다. 또한 Security Hub 계정의 각 사용자마다 설정이 개별적으로 저장됩니다. 즉, 사용자마다 대시보드에 다른 레이아웃, 위젯 및 필터 세트를 사용할 수 있습니다.

요약 대시보드를 열 때마다 Security Hub는 대부분의 대시보드 데이터를 자동으로 새로 고칩니다. 하지만 일부 데이터는 업데이트 빈도가 낮습니다. 예를 들어 보안 점수와 제어 상태는 24시간마다 업데이트됩니다.

Security Hub에 대해 크로스 리전 집계 영역을 구성한 경우 대시보드 데이터에는 집계 영역 및 연결된 모든 리전의 결과가 포함됩니다. 조직의 Security Hub 위임된 관리자인 경우 데이터에는 관리자 계정 및 구성원 계정에 대한 결과가 포함됩니다. 필요에 따라 계정별로 데이터를 필터링할 수 있습니다. 구성원 계정 또는 독립형 계정이 있는 경우 데이터에는 계정에 대한 결과만 포함됩니다.

요약 대시보드에 사용할 수 있는 위젯

요약 대시보드에는 AWS 고객의 보안 운영 및 경험을 바탕으로 최신 클라우드 보안 위협 환경을 반영하는 위젯이 포함됩니다. 일부 위젯은 기본적으로 표시되지만 어떤 위젯은 표시되지 않습니다. 위젯을 추가하거나 제거하여 대시보드 보기를 사용자 지정할 수 있습니다.

위젯을 추가하려면 요약 페이지 오른쪽 상단의 위젯 추가를 선택합니다. 검색창에 위젯 제목을 입력합니다. 위젯을 대시보드로 끌어다 놓습니다.

위젯은 기본적으로 표시

기본적으로 요약 대시보드에는 다음 위젯이 포함됩니다.

보안 표준

가장 최근의 요약 보안 점수와 각 Security Hub 표준에 대한 보안 점수를 표시합니다. 0~100% 범위의 보안 점수는 활성화된 모든 제어와 비교하여 통과된 제어의 비율을 나타냅니다. 이러한 점수에 대한 자세한 내용은 보안 점수 계산 방법 섹션을 참조하세요. 이 위젯은 전반적인 보안 태세를 이해하는 데 도움이 됩니다.

가장 많은 결과가 포함된 자산

가장 많은 결과가 포함된 리소스, 계정 및 애플리케이션에 대한 개요를 제공합니다. 목록은 결과 수를 기준으로 내림차순으로 정렬됩니다. 위젯의 각 탭은 해당 범주의 상위 6개 항목을 심각도 및 리소스 유형별로 그룹화하여 표시합니다. 전체 결과 열에서 숫자를 선택하면 Security Hub에서 자산에 대한 조사 결과를 보여주는 페이지가 열립니다. 이 위젯을 사용하면 핵심 자산 중 잠재적 보안 위협이 있는 자산을 신속하게 식별할 수 있습니다.

리전별 조사 결과

Security Hub가 활성화된 각 AWS 리전에서 심각도별로 그룹화한 조사 결과의 총 수를 표시합니다. 이 위젯은 특정 리전에 영향을 미칠 수 있는 보안 문제를 식별하는 데 도움이 됩니다. 집계 영역에서 대시보드를 여는 경우 이 위젯을 통해 연결된 각 리전의 잠재적 보안 문제를 모니터링할 수 있습니다.

가장 일반적인 위협 유형

AWS 환경에서 가장 일반적인 10가지 위협 유형을 분류하여 제공합니다. 여기에는 권한 에스컬레이션, 노출된 보안 인증 사용 또는 악의적인 IP 주소와의 통신과 같은 위협이 포함됩니다.

이 데이터를 보려면 Amazon GuardDuty를 활성화해야 합니다. 활성화되면 이 위젯에서 위협 유형을 선택하여 GuardDuty 콘솔을 열고 이 위협과 관련된 결과를 검토하세요. 이 위젯은 다른 보안 문제의 컨텍스트에서 잠재적 위협을 평가하는 데 도움이 됩니다.

악용을 통한 소프트웨어 취약성

AWS 환경에 존재하며 알려진 악용 사례가 있는 소프트웨어 취약성에 대한 요약을 제공합니다. 또한 수정 사항을 사용할 수 있는 취약성과 사용할 수 없는 취약성을 분류하여 검토할 수 있습니다.

이 데이터를 보려면 Amazon Inspector를 활성화해야 합니다. 활성화되면 이 위젯에서 통계를 선택하여 Amazon Inspector 콘솔을 열고 취약성에 대한 자세한 내용을 검토하세요. 이 위젯은 다른 보안 문제의 컨텍스트에서 소프트웨어 취약성을 평가하는 데 도움이 됩니다.

시간 경과에 따른 새로운 조사 결과

지난 90일 동안의 새로운 일일 조사 결과 수의 추세를 보여줍니다. 추가 컨텍스트를 위해 심각도 또는 공급자별로 데이터를 분류할 수 있습니다. 이 위젯을 사용하면 지난 90일 동안 특정 시간에 조사 결과 볼륨이 급증하거나 감소했는지 파악할 수 있습니다.

가장 많은 결과가 포함된 리소스

가장 많은 조사 결과를 생성한 리소스에 대한 요약을 제공하며, Amazon Simple Storage Service(S3) 버킷, Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 및 AWS Lambda 기능과 같은 리소스 유형별로 분류합니다.

위젯의 각 탭은 이전 리소스 유형 중 하나에 초점을 맞추어 가장 많은 조사 결과를 생성한 10개의 리소스 인스턴스를 나열합니다. 특정 리소스에 대한 조사 결과를 검토하려면 리소스 인스턴스를 선택합니다. 이 위젯을 사용하면 공통 AWS 리소스와 관련된 보안 조사 결과를 분류할 수 있습니다.

위젯은 기본적으로 숨김

다음 위젯은 요약 대시보드에서도 사용할 수 있지만 기본적으로 숨깁니다.

가장 많은 결과가 포함된 AMI

가장 많은 조사 결과를 생성한 Amazon Machine Image(AMI) 10개의 목록을 제공합니다. 이 데이터는 Amazon EC2가 사용자 계정에 대해 활성화된 경우에만 사용할 수 있습니다. 이를 통해 잠재적 보안 위험을 야기하는 AMI를 식별할 수 있습니다.

가장 많은 결과가 포함된 IAM 보안 주체

가장 많은 조사 결과를 생성한 AWS Identity and Access Management(IAM) 사용자 10명의 목록을 제공합니다. 이 위젯은 관리 및 결제 작업을 수행하는 데 도움이 됩니다. Security Hub 사용에 가장 많이 기여하는 사용자를 보여줍니다.

가장 많은 결과가 포함된 계정(심각도별)

가장 많은 조사 결과를 생성한 10개 계정을 심각도별로 그룹화하여 그래프로 표시합니다. 이 위젯은 분석 및 문제 해결 노력을 집중할 계정을 결정하는 데 도움이 됩니다.

가장 많은 결과가 포함된 계정(리소스 유형별)

가장 많은 조사 결과를 생성한 10개 계정을 리소스 유형별로 그룹화여 그래프로 표시합니다. 이 위젯은 분석 및 문제 해결을 위해 우선적으로 지정할 계정 및 리소스 유형을 결정하는 데 도움이 됩니다.

인사이트

Security Hub에서 관리하는 다섯 가지 인사이트와 이를 통해 생성된 조사 결과 수를 나열합니다. 인사이트는 주의가 필요한 특정 보안 영역을 식별합니다.

AWS 통합의 최신 조사 결과

통합 AWS 서비스에서 Security Hub로 수신한 조사 결과 수를 표시합니다. 또한 각 통합 서비스에서 가장 최근에 조사 결과를 받은 시기도 표시합니다. 이 위젯은 여러 AWS 서비스의 통합 조사 결과 데이터를 제공합니다. 자세히 살펴보려면 통합 서비스를 선택합니다. 그런 다음 Security Hub에서 해당 서비스의 콘솔을 엽니다.

요약 대시보드 필터링

요약 대시보드에서 데이터를 큐레이션하고 가장 관련성이 높은 보안 데이터만 포함하기 위해 대시보드를 필터링할 수 있습니다. 예를 들어 애플리케이션 팀의 팀원인 경우 프로덕션 환경의 중요한 애플리케이션에 대한 전용 보기를 만들 수 있습니다. 보안 팀의 팀원인 경우 심각도가 높은 조사 결과에 집중하는 데 도움이 되는 전용 보기를 만들 수 있습니다. 요약 대시보드에서 데이터를 필터링하려면 대시보드 위의 필터 상자에 필터 기준을 입력합니다. 필터 기준을 적용하면 인사이트 및 보안 표준 위젯의 데이터를 제외한 대시보드의 모든 데이터에 기준이 적용됩니다.

다음 필드를 사용하여 데이터를 필터링할 수 있습니다.

- 계정 이름
- 계정 ID
- 애플리케이션 Amazon 리소스 이름(ARN)
- 애플리케이션 이름
- 제품 이름(AWS 서비스 또는 Security Hub에 조사 결과를 보내는 타사 제품의 이름)
- 레코드 상태
- 리전
- 리소스 태그
- 심각도(Severity)
- 워크플로 상태

기본적으로 대시보드 데이터는 다음 기준을 사용하여 필터링합니다. `Workflow status`는 `NOTIFIED` 또는 `NEW`이고, `Record state`는 `ACTIVE`입니다. 이러한 기준은 대시보드 위, 필터 상자 아래에 표시됩니다. 이러한 기준을 제거하려면 제거하려는 기준에 대한 필터 토큰에서 X를 선택합니다.

다시 사용하려는 필터를 적용하는 경우, 해당 내용을 필터 세트로 저장할 수 있습니다. 필터 세트는 요약 대시보드에서 데이터를 결과를 검토할 때 다시 적용하기 위해 만들고 저장하는 필터 기준 세트입니다.

> **Note**
>
> 애플리케이션 ARN, 애플리케이션 이름, 리소스 태그와 같은 필드는 필터 세트의 일부로 저장할 수 없습니다.

필터 세트 생성 및 저장

필드 세트를 만들려면 다음 단계를 따르세요.

필터 세트를 만들고 저장하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다.
3. 요약 대시보드 위의 필터 상자에 필터 세트의 필터 기준을 입력합니다.
4. 필터 지우기 메뉴에서 새 필터 세트 저장을 선택합니다.
5. 필터 세트 저장 대화 상자에 필터 세트 이름을 입력합니다.
6. (선택 사항) 요약 페이지를 열 때마다 기본적으로 필터 세트를 사용하려면 해당 필터 세트를 기본 보기로 설정하는 옵션을 선택합니다.
7. 저장을 선택합니다.

만들고 저장한 필터 세트 간에 전환하려면 요약 대시보드 위의 필터 세트 선택 메뉴를 사용합니다. 필터 세트를 선택하면 Security Hub는 필터 세트의 기준을 대시보드의 데이터에 적용합니다.

필터 세트 업데이트 또는 삭제

기존 필터 세트를 업데이트하거나 삭제하려면 다음 단계를 따르세요. 현재 요약 대시보드의 기본 보기로 설정된 필터 세트를 삭제하면 기본 보기가 기본 Security Hub 보기로 재설정됩니다.

필터 세트를 업데이트 또는 삭제하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다.
3. 요약 페이지 위의 필터 세트 선택 메뉴에서 필터 세트를 선택합니다.
4. 필터 지우기 메뉴에서 다음 중 하나를 수행합니다.
   - 필터 세트를 업데이트하려면 현재 필터 세트 업데이트를 선택합니다. 그런 다음 나타나는 대화 상자에 변경 사항을 입력합니다.
   - 필터 세트를 삭제하려면 현재 필터 세트 삭제를 선택합니다. 그런 다음 나타나는 대화 상자에서 삭제를 선택합니다.

요약 대시보드 사용자 지정

여러 가지 방법으로 요약 대시보드를 사용자 지정할 수 있습니다. 대시보드에서 위젯을 추가하거나 제거할 수 있습니다. 대시보드에서 위젯을 재배열하고 크기를 조정할 수도 있습니다.

대시보드를 사용자 지정하는 경우 Security Hub는 변경 사항을 즉시 적용하고 새 대시보드 설정을 저장합니다. 변경 사항은 모든 AWS 리전 및 브라우저의 대시보드 보기에 적용됩니다.

요약 대시보드를 사용자 지정하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다.
3. 다음을 수행합니다.

   - 위젯을 추가하려면 페이지의 오른쪽 상단에서 위젯 추가를 선택합니다. 검색창에 추가할 위젯의 제목을 입력합니다. 그런 다음 위젯을 원하는 위치로 끌어다 놓습니다.
   - 위젯을 제거하려면 위젯의 오른쪽 상단 모서리에 있는 3개의 점을 선택합니다.
   - 위젯을 이동하려면 위젯의 왼쪽 상단 모서리에 있는 핸들을 선택한 다음 위젯을 원하는 위치로 끌어다 놓습니다.
   - 위젯의 크기를 변경하려면 위젯의 오른쪽 하단 모서리에 있는 크기 조정 핸들을 선택합니다. 위젯이 원하는 크기가 될 때까지 위젯의 가장자리를 끌어다 놓습니다.

이후에 원래 설정을 복원하려면 페이지의 상단에서 기본 레이아웃으로 리셋을 선택합니다.

AWS CloudFormation를 사용하여 Security Hub 리소스 생성

AWS Security Hub 와 AWS CloudFormation통합됩니다. 이 서비스는 리소스를 모델링하고 설정하는 데 도움이 되므로 AWS 리소스와 인프라를 만들고 관리하는 데 소요되는 시간을 줄일 수 있습니다. 원하는 모든 AWS 리소스 (예: 자동화 규칙) 를 설명하는 템플릿을 만들고 해당 리소스를 자동으로 AWS CloudFormation 프로비저닝 및 구성합니다.

를 사용하면 템플릿을 재사용하여 AWS CloudFormation Security Hub 리소스를 일관되고 반복적으로 설정할 수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정 지역과 지역에서 동일한 리소스를 반복해서 프로비저닝하세요.

Security Hub 및 AWS CloudFormation 템플릿

Security Hub 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿이 작동하는 방식을 이해해야 합니다. 템플릿은 JSON 또는 YAML 형식의 텍스트 파일입니다. 이 템플릿은 AWS CloudFormation 스택에 프로비저닝하려는 리소스를 설명합니다.

JSON이나 YAML에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하여 템플릿을 시작하는 데 도움을 받을 수 있습니다. AWS CloudFormation 자세한 내용은 디자이너란 무엇입니까? 를 참조하십시오. AWS CloudFormation AWS CloudFormation 사용 설명서에서.

다음 유형의 Security Hub 리소스에 대한 AWS CloudFormation 템플릿을 생성할 수 있습니다.

- Security Hub 활성화
- 조직에 위임된 Security Hub 관리자 지정하기
- 보안 표준 활성화
- 사용자 지정 인사이트 생성
- 자동화 규칙 생성
- 타사 제품 통합 구독

리소스에 대한 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS Security Hub 리소스 유형 참조를 참조하십시오.

에 대해 자세히 알아보십시오. AWS CloudFormation

자세히 AWS CloudFormation알아보려면 다음 리소스를 참조하십시오.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation API Reference
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

Amazon Simple Notification Service를 통한 Security Hub 공지 구독하기

이 섹션에서는 Amazon Simple Notification Service(SNS)를 통해 AWS Security Hub 공지를 구독하여 Security Hub에 대한 알림을 받는 방법에 대한 정보를 제공합니다.

구독하면 다음 이벤트에 대한 알림을 받게 됩니다(각 이벤트에 해당하는 `AnnouncementType` 참고).

- `GENERAL`— Security Hub 서비스에 대한 일반 알림.
- `UPCOMING_STANDARDS_CONTROLS`— 지정된 Security Hub 컨트롤 또는 표준이 곧 출시될 예정입니다. 이러한 유형의 발표는 릴리스에 앞서 대응 및 해결 워크플로를 준비하는 데 도움이 됩니다.
- `NEW_REGIONS`— Security Hub에 대한 지원이 새로운 AWS 리전에서 제공됩니다.
- `NEW_STANDARDS_CONTROLS`— 새로운 Security Hub 컨트롤 또는 표준이 추가되었습니다.
- `UPDATED_STANDARDS_CONTROLS`— 기존 Security Hub 컨트롤 또는 표준이 업데이트되었습니다.
- `RETIRED_STANDARDS_CONTROLS`— 기존 Security Hub 컨트롤 또는 표준이 사용 중지되었습니다.
- `UPDATED_ASFF`— AWS 보안 검색 형식(ASFF) 구문, 필드 또는 값이 업데이트되었습니다.
- `NEW_INTEGRATION`— 다른 AWS 서비스 또는 타사 제품과의 새로운 통합을 사용할 수 있습니다.
- `NEW_FEATURE`— 새로운 Security Hub 기능을 사용할 수 있습니다.
- `UPDATED_FEATURE`— 기존 Security Hub 기능이 업데이트되었습니다.

알림은 Amazon SNS에서 지원하는 모든 형식으로 사용할 수 있습니다. Security Hub를 사용할 수 있는 모든 AWS 리전에서 Security Hub 공지를 구독할 수 있습니다.

사용자가 Amazon SNS 주제를 구독할 수 있는 `Subscribe` 권한이 있어야 합니다. Amazon SNS 정책, IAM 정책 또는 둘 다를 사용하여 이를 달성할 수 있습니다. 자세한 정보는 Amazon Simple Notification Service 개발자 안내서에서 IAM 및 Amazon SNS 정책을 함께 참조하세요.

> **Note**
>
> Security Hub는 구독한 모든 AWS 계정에게 Security Hub 서비스 업데이트에 대한 Amazon SNS 공지를 전송합니다. Security Hub 검색 결과에 대한 알림을 받으려면 검색 결과 세부 정보 및 기록 관리 및 검토을 참조하세요.

Amazon SNS 주제에 대해 Amazon Simple Queue Service(Amazon SQS) 대기열을 구독할 수 있지만 동일한 리전에 있는 Amazon SNS 주제 Amazon 리소스 이름(ARN)을 사용해야 합니다. 자세한 내용은 Amazon Simple Queue Service 개발자 안내서에서 튜토리얼: Amazon SNS 주제에 대한 Amazon SQS 대기열 구독 단원을 참조하세요.

알림을 받을 때 AWS Lambda 함수를 사용하여 이벤트를 간접적으로 호출할 수도 있습니다. 샘플 함수 코드를 포함한 자세한 내용은 AWS Lambda 개발자 안내서의 튜토리얼: Amazon 단순 알림 서비스와 함께 AWS Lambda 사용을 참조하십시오.

각 리전에 대한 Amazon SNS 주제 ARN은 다음과 같습니다.

AWS 리전	Amazon SNS 주제 ARN
미국 동부(오하이오)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
미국 동부(버지니아 북부)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
미국 서부(캘리포니아 북부)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
미국 서부(오레곤)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
아프리카(케이프타운)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
아시아 태평양(홍콩)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`

AWS 리전	Amazon SNS 주제 ARN
아시아 태평양(하이데라바드)	arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements
아시아 태평양(자카르타)	arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements
아시아 태평양(뭄바이)	arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements
아시아 태평양(오사카)	arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements
아시아 태평양(서울)	arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements
아시아 태평양(싱가포르)	arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements
아시아 태평양(시드니)	arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements
아시아 태평양(도쿄)	arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements
캐나다(중부)	arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements

AWS 리전	Amazon SNS 주제 ARN
중국(베이징)	arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements
중국(닝샤)	arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements
유럽(프랑크푸르트)	arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements
유럽(아일랜드)	arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements
유럽(런던)	arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements
유럽(밀라노)	arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements
유럽(파리)	arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements
유럽(스페인)	arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements
유럽(스톡홀름)	arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements

AWS 리전	Amazon SNS 주제 ARN
유럽(취리히)	`arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements`
이스라엘(텔아비브)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
중동(바레인)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
중동(UAE)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
남아메리카(상파울루)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud(미국 동부)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud(미국 서부)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

메시지는 일반적으로 파티션 내 여러 리전에서 동일하므로 각 파티션의 한 지역을 구독하면 해당 파티션의 모든 리전에 영향을 미치는 공지를 받을 수 있습니다. 구성원 계정과 관련된 공지는 관리자 계정에 복제되지 않습니다. 따라서 관리자 계정을 포함한 각 계정에는 각 공지사항의 사본이 한 개만 남게 됩니다. Security Hub 공지를 구독하는 데 사용할 계정을 결정할 수 있습니다.

Security Hub 공지 구독 비용에 대한 자세한 내용은 Amazon SNS 요금을 참조하십시오.

Security Hub 공지 구독(콘솔)

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 리전 목록에서 Security Hub 공지를 구독하려는 리전을 선택합니다. 이 예에서는 `us-west-2` 리전을 사용합니다.
3. 탐색 창에서 구독을 선택하고 나서 구독 생성을 선택합니다.
4. 주제 ARN 상자에 주제의 ARN을 입력합니다. 예: `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. 프로토콜에서 Security Hub 공지를 수신할 방법을 선택합니다. 이메일을 선택한 경우 엔드포인트에 공지를 받을 이메일 주소를 입력합니다.
6. 구독 생성을 선택합니다.
7. 구독을 확인합니다. 예를 들어 이메일 프로토콜을 선택한 경우 Amazon SNS는 사용자가 제공한 이메일로 구독 확인 메시지를 전송합니다.

Security Hub 공지 구독(AWS CLI)

1. 다음 명령을 실행합니다:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. 구독을 확인합니다. 예를 들어 이메일 프로토콜을 선택한 경우 Amazon SNS는 사용자가 제공한 이메일로 구독 확인 메시지를 전송합니다.

Amazon SNS 메시지 형식

다음 예는 새로운 보안 제어 도입에 대한 Amazon SNS의 Security Hub 공지를 보여줍니다. 메시지 내용은 공지 유형에 따라 다르지만 형식은 모든 공지 유형에서 동일합니다. 선택적으로 공지 사항에 대한 세부 정보를 제공하는 `Link` 필드가 포함될 수 있습니다.

예: 새로운 제어 기능에 대한 Security Hub 발표(이메일 프로토콜)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub controls added to the AWS Foundational
 Security Best Practices standard",
```

```
"Description":"We have added 36 new controls to the AWS Foundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon
 CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23,
 EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon
 Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12),
 Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes
 Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured Security
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. "
}
```

예: 새로운 제어 기능에 대한 Security Hub 공지(이메일-JSON 프로토콜)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New
 Controls] 36 new Security Hub controls added to the AWS Foundational Security Best
 Practices standard\",\"Description\":\"We have added 36 new controls to the AWS
 Foundational Security Best Practices standard. These include controls for Amazon
 Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
 (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
 (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
 (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
 ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
 Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
 ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
 NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
 Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured SSecurity
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
```

```
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

AWS Security Hub의 보안

AWS에서는 클라우드 보안을 가장 중요하게 생각합니다. 여러분은 AWS 고객으로서 보안에 민감한 기관의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와(과) 귀하의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS클라우드에서 AWS서비스를 실행하는 인프라를 보호합니다.AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사원은 정기적으로 AWS 규제 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. AWS Security Hub에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 범위 내의 AWS 서비스를 참조하십시오.
- 클라우드 내 보안 – 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Security Hub 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Security Hub를 구성하는 방법을 보여줍니다. 또한 Security Hub 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- AWS Security Hub의 데이터 보호
- AWS Identity 및 Access Management에 대한 AWS Security Hub
- AWS Security Hub의 규정 준수 확인
- AWSSecurity Hub의 레질리언스
- AWS Security Hub에서 인프라 보안
- AWS Security Hub 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

AWS Security Hub의 데이터 보호

AWS 공동 책임 모델은 AWS Security Hub의 데이터 보호에 적용됩니다. 이 모델에서 설명하는 것처럼 AWS은(는) 모든 AWS 클라우드을(를) 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 Data Privacy FAQ(데

이터 프라이버시 FAQ)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS Shared Responsibility Model and GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정보안 인증 정보를 보호하고 AWS IAM Identity Center또는 AWS Identity and Access Management(IAM)를 통해 개별 사용자 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신하세요. TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- AWS CloudTrail로 API 및 사용자 활동 로깅을 설정하세요.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용합니다.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API, AWS CLI 또는 AWS SDK를 사용하여 Security Hub 또는 기타 AWS 서비스로 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 보안 인증를 URL에 포함시켜서는 안 됩니다.

Security Hub는 멀티 테넌트 서비스를 제공합니다. 데이터 보호를 위해 Security Hub는 저장 데이터, 구성 요소 서비스 간 전송되는 데이터를 암호화합니다.

AWS Identity 및 Access Management에 대한 AWS Security Hub

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 어떤 사용자가 Security Hub 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 소유)될 수 있는지 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객

고객

사용 방법 AWS Identity and Access Management (IAM) 은 Security Hub에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Security Hub 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Security Hub 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Security Hub의 기능에 액세스할 수 없는 경우 AWS Security Hub ID 및 액세스 문제 해결 단원을 참조하십시오.

서비스 관리자 - 회사에서 Security Hub 리소스를 책임지고 있는 경우 Security Hub에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Security Hub 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Security Hub에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 IAM의 AWS Security Hub 작동 방식 단원을 참조하십시오.

IAM 관리자 - IAM 관리자라면 Security Hub에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Security Hub 자격 증명 기반 정책 예제를 보려면 Security Hub의 ID 기반 정책 예제 단원을 참조하십시오.

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더

레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하십시오.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 생성 단원을 참조하십시오. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입

니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

- 서비스 간 액세스 — 일부는 다른 AWS 서비스기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접적 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자

또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

IAM의 AWS Security Hub 작동 방식

AWS Identity and Access Management (IAM) 을 사용하여 액세스를 AWS Security Hub관리하기 전에 Security Hub에서 사용할 수 있는 IAM 기능을 알아보십시오.

함께 사용할 수 있는 IAM 기능 AWS Security Hub

IAM 특성	Security Hub 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	아니요
정책 조건 키	예
액세스 제어 목록(ACL)	아니요
ABAC(속성 기반 액세스 제어) - 정책 태그	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	아니요
서비스 링크 역할	예

Security Hub 및 기타 제품이 대부분의 IAM 기능과 어떻게 AWS 서비스 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과AWS 서비스 호환되는 기능을 참조하십시오.

Security Hub에 대한 ID 기반 정책

보안 인증 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수

행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

Security Hub는 ID 기반 정책을 지원합니다. 자세한 정보는 Security Hub의 ID 기반 정책 예제을 참조하세요.

자료=Security Hub에 대한 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 등이 포함될 수 있습니다. AWS 서비스

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

Security Hub는 리소스 기반 정책을 지원하지 않습니다. IAM 정책을 Security Hub 리소스에 직접 연결할 수는 없습니다.

Security Hub에 대한 정책 조치

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

Security Hub의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
securityhub:
```

예를 들어 Security Hub API의 `EnableSecurityHub` 작동에 해당하는 작업인 Security Hub를 활성화할 수 있는 권한을 사용자에게 부여하려면 해당 `securityhub:EnableSecurityHub` 작업을 정책에 포함시키십시오. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Security Hub는 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 세트를 정의합니다.

```
"Action": "securityhub:EnableSecurityHub"
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다. 예:

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

와일드카드 (*) 를 사용하여 여러 작업을 지정할 수도 있습니다. 예를 들어, `Get`라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "securityhub:Get*"
```

하지만 가장 좋은 방법은 최소 권한의 원칙을 따르는 정책을 만드는 것입니다. 즉, 특정 작업을 수행하는 데 필요한 권한만 포함하는 정책을 만들어야 합니다.

사용자가 `DescribeStandardsControl` 작업에 액세스할 수 있어야 `BatchGetSecurityControlsBatchGetStandardsControlAssociations`, 및 `ListStandardsControlAssociations` 에 액세스할 수 있습니다.

사용자에게 UpdateStandardsControls 작업에 대한 액세스 권한이 있어야 및 에 액세스할 수 BatchUpdateStandardsControlAssociations UpdateSecurityControl 있습니다.

Security Hub 작업 목록은 서비스 권한 부여 AWS Security Hub참조에 정의된 작업을 참조하십시오. Security Hub 작업을 지정하는 정책의 예는 을 참조하십시오Security Hub의 ID 기반 정책 예제.

리소스

정책 리소스 지원	아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Security Hub는 다음과 같은 리소스 유형을 정의합니다.

- Hub(허브)
- 제품
- 검색 애그리게이터 (지역 간 애그리게이터라고도 함)
- 자동화 규칙
- 구성 정책

ARN을 사용하여 정책에서 이러한 유형의 리소스를 지정할 수 있습니다.

Security Hub 리소스 유형 및 각 유형의 ARN 구문 목록은 서비스 권한 부여 AWS Security Hub 참조에 정의된 리소스 유형을 참조하십시오. 각 리소스 유형에 지정할 수 있는 작업을 알아보려면 서비스 권한

부여 AWS Security Hub참조에 정의된 작업을 참조하십시오. 리소스를 지정하는 정책의 예는 Security Hub의 ID 기반 정책 예제 섹션을 참조하세요.

Security Hub의 정책 조건 키

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예컨대, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

Security Hub 조건 키 목록은 서비스 인증 AWS Security Hub참조의 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 정의된 작업을 참조하십시오 AWS Security Hub. 조건 키를 사용하는 정책의 예는 Security Hub의 ID 기반 정책 예제을 참조하세요.

Security Hub의 액세스 제어 목록 (ACL)

ACL 지원	아니요

ACL(액세스 통제 목록)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Security Hub는 ACL을 지원하지 않으므로 보안 허브 리소스에 ACL을 연결할 수 없습니다.

Security Hub를 통한 속성 기반 액세스 제어 (ABAC)

ABAC 지원(정책의 태그)	예

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇입니까?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

Security Hub 리소스에 태그를 첨부할 수 있습니다. 정책 `Condition` 요소에 태그 정보를 제공하여 리소스에 대한 액세스를 제어할 수도 있습니다.

Security Hub 리소스에 태그를 지정하는 방법에 대한 자세한 내용은 을 참조하십시오AWS Security Hub 리소스 태그 지정. 태그를 기반으로 리소스에 대한 액세스를 제한하는 자격 증명 기반 정책의 예는 Security Hub의 ID 기반 정책 예제 단원을 참조하십시오.

Security Hub에 대한 임시 보안 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명을 참조하세요.

임시 보안 인증을 사용하여 연동을 통해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AssumeRole또는 GetFederationToken와 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 얻습니다.

Security Hub는 임시 자격 증명의 사용을 지원합니다.

Security Hub를 위한 포워드 액세스 세션

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

예를 들어 Security Hub는 사용자가 Security Hub를 Organizations에 있는 조직에 위임된 Security Hub 관리자 AWS Organizations 계정과 통합하고 조직의 위임된 Security Hub 관리자 계정을 지정할 때 AWS 서비스 다운스트림에 FAS 요청을 보냅니다.

다른 작업의 경우 Security Hub는 서비스 연결 역할을 사용하여 사용자를 대신하여 작업을 수행합니다. 이 역할에 대한 자세한 내용은 Security Hub의 서비스 연결 역할 단원을 참조하세요.

Security Hub의 서비스 역할

Security Hub는 서비스 역할을 맡거나 사용하지 않습니다. Security Hub는 사용자를 대신하여 작업을 수행하기 위해 서비스 연결 역할을 사용합니다. 이 역할에 대한 자세한 내용은 Security Hub의 서비스 연결 역할 단원을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Security Hub 사용에 운영상 문제가 발생할 수 있습니다. Security Hub에서 이에 대한 지침을 제공하는 경우에만 서비스 역할을 편집하십시오.

Security Hub의 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Security Hub는 서비스 연결 역할을 사용하여 사용자를 대신하여 작업을 수행합니다. 이 역할에 대한 자세한 내용은 Security Hub의 서비스 연결 역할 단원을 참조하세요.

Security Hub의 ID 기반 정책 예제

기본적으로 사용자 및 역할에는 Security Hub 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS CLI또는 AWSAPI를 사용해 태스크를 수행할 수 없습니다. 관리자는 지정된 리소스에서 특정 API 태스크를 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 JSON 탭에서 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- Security Hub 콘솔 사용
- 예: 사용자가 자신이 권한을 볼 수 있도록 허용
- 예: 사용자가 구성 정책을 만들고 관리하도록 허용
- 예: 사용자가 결과를 볼 수 있도록 허용
- 예: 사용자가 자동화 규칙을 만들고 관리하도록 허용

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Security Hub 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하고 최소 권한을 향해 나아가기 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS관리형 정책을 사용합니다. 관리형 정책은 AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWSmanaged policies(관리형 정책) 또는 AWSmanaged policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한: 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 특정 AWS 서비스(예: AWS CloudFormation)을(를) 통해 사용되는 경우에만 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 IAM 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하십시오.
- 다중 인증(MFA) 필요 – AWS 계정계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 설정합니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례 섹션을 참조하십시오.

Security Hub 콘솔 사용

AWS Security Hub 콘솔에 액세스하려면 최소 권한 세트가 있어야 합니다. 이러한 권한은 AWS 계정에서 Security Hub 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보

다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWSAPI만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요가 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

이러한 사용자와 역할이 Security Hub 콘솔을 사용할 수 있도록 하려면 다음 AWS 관리형 정책도 엔티티에 연결하십시오. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

예: 사용자가 자신이 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI나 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

예: 사용자가 구성 정책을 만들고 관리하도록 허용

이 예제는 사용자가 구성 정책을 만들고, 보고, 업데이트하고, 삭제할 수 있도록 허용하는 IAM 정책을 생성하는 방법을 보여줍니다. 또한 이 예제 정책은 사용자가 정책 연결을 시작, 중지 및 볼 수 있도록 허용합니다. 이 IAM 정책이 작동하려면 사용자가 조직의 위임된 Security Hub 관리자여야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

예: 사용자가 결과를 볼 수 있도록 허용

이 예제는 사용자가 Security Hub 조사 결과를 볼 수 있도록 허용하는 IAM 정책을 생성하는 방법을 보여줍니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

예: 사용자가 자동화 규칙을 만들고 관리하도록 허용

이 예제는 사용자가 Security Hub 자동화 규칙을 만들고, 보고, 업데이트하고, 삭제할 수 있도록 허용하는 IAM 정책을 생성하는 방법을 보여줍니다. 이 IAM 정책이 작동하려면 사용자가 Security Hub 관리자여야 합니다. 권한을 제한하려면 (예: 사용자가 자동화 규칙을 볼 수만 있도록 허용하려는 경우) 생성, 업데이트 및 삭제 권한을 제거할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
```

```
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Security Hub의 서비스 연결 역할

AWS Security Hub라는 이름의 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. `AWSServiceRoleForSecurityHub` 이 서비스 연결 역할은 Security Hub에 직접 연결된 IAM 역할입니다. Security Hub에서 미리 정의하며 Security Hub에서 사용자를 대신하여 다른 사용자에게 전화를 AWS 서비스 걸고 AWS 리소스를 모니터링하는 데 필요한 모든 권한이 포함되어 있습니다. Security Hub는 Security Hub를 사용할 수 AWS 리전 있는 모든 지역에서 이 서비스 연결 역할을 사용합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Security Hub를 더 쉽게 설정할 수 있습니다. Security Hub에서 이 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 Security Hub만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 개체에 연결할 수 없습니다.

서비스 연결 역할의 세부 정보를 보려면 Security Hub 콘솔의 설정 페이지에서 일반을 선택한 다음 서비스 권한 보기를 선택합니다.

활성화된 모든 리전에서 먼저 Security Hub를 비활성화한 후에만 Security Hub 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Security Hub 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM 사용 설명서에서 IAM으로 작업하는 AWS 서비스를 살펴보고 서비스 연결 역할 열이 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

주제

Security Hub에 대한 서비스 연결 역할 권한

Security Hub에서는 AWSServiceRoleForSecurityHub인 서비스 연결 역할을 사용합니다. AWS Security Hub가 리소스에 액세스하는 데 필요한 서비스 연결 역할입니다. 서비스 연결 역할을 통해 Security Hub는 다른 AWS 서비스의 조사 결과를 수신하고 컨트롤를 위한 보안 검사를 실행하는 데 필요한 AWS Config 인프라를 구성할 수 있습니다.

AWSServiceRoleForSecurityHub 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- securityhub.amazonaws.com

AWSServiceRoleForSecurityHub 서비스 연결 역할은 관리형 정책 AWSSecurityHubServiceRolePolicy을(를) 사용합니다.

IAM 자격 증명(역할, 그룹, 사용자 등)이 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 부여해야 합니다. AWSServiceRoleForSecurityHub 서비스 연결 역할을 성공적으로 생성하기 위해서는 Security Hub에 액세스 하기 위해 사용하는 IAM 자격 증명이 필수 권한이 있어야 합니다. 필수 권한을 부여하려면 다음 정책을 역할, 그룹, 또는 사용자에 연결하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
```

```
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Security Hub에 대한 서비스 연결 역할 생성

AWSServiceRoleForSecurityHub 서비스 연결 역할은 처음으로 Security Hub를 활성화하거나 이전에 활성화하지 않은 지원 리전에서 Security Hub를 활성화할 때 자동으로 생성됩니다. 또한 IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 AWSServiceRoleForSecurityHub 서비스 연결 역할을 수동으로 생성할 수 있습니다.

> **Important**
>
> Security Hub 관리자 계정용으로 생성된 서비스 연결 역할은 Security Hub 구성원 계정에 적용되지 않습니다.

수동 서비스 역할 생성에 대한 자세한 내용은 IAM 사용 설명서의 서비스에 대한 역할 만들기를 참조하세요.

Security Hub에 대한 서비스 연결 역할 편집

Security Hub에서는 AWSServiceRoleForSecurityHub 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하십시오.

Security Hub에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔티티가 없도록 합니다.

> **Important**
>
> AWSServiceRoleForSecurityHub 서비스 연결 역할을 삭제하려면 먼저 활성화한 모든 리전에서 Security Hub를 비활성화해야 합니다.

서비스 연결 역할을 삭제하려고 할 때 Security Hub가 비활성화되지 않는 경우 삭제에 실패합니다. 자세한 설명은 Security Hub 비활성화 섹션을 참조하세요.

Security Hub를 비활성화하면 `AWSServiceRoleForSecurityHub` 서비스 연결 역할이 자동으로 삭제되지 않습니다. Security Hub를 다시 활성화하는 경우에는 기존 `AWSServiceRoleForSecurityHub` 서비스 연결 역할을 사용하기 시작합니다.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 `AWSServiceRoleForSecurityHub` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 삭제를 참조하세요.

AWSAWS Security Hub의 관리형 정책

AWS 관리형 정책은 에서 생성하고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSSecurityHubFullAccess

`AWSSecurityHubFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 모든 Security Hub 작업에 대한 전체 액세스 권한을 허용하는 관리 권한을 보안 주체에게 부여합니다. 보안 주체가 자신의 계정에 대해 Security Hub를 수동으로 활성화하려면 먼저 보안 주체에 이 정책을 연결해야 합니다. 예를 들어, 이러한 권한이 있는 보안 주체는 조사 결과의 상태를 보고 업데이트할 수 있습니다. 이들은 사용자 지정 통찰력을 구성하고 통합을 활성화할 수 있습니다. 표준 및 제어 기능을 활성화하거나 비활성화할 수 있습니다. 관리자 계정의 보안 주체는 멤버 계정을 관리할 수도 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- securityhub – 보안 주체가 Security Hub 작업에 대한 모든 액세스 권한을 가질 수 있습니다.
- guardduty— 주체가 Amazon의 계정 상태에 대한 정보를 얻을 수 있습니다. GuardDuty
- iam – 보안 주체가 서비스 연결 역할을 생성할 수 있습니다.
- inspector – 보안 주체가 Amazon Inspector의 계정 상태에 대한 정보를 가져올 수 있습니다.
- pricing— 교육자가 제품의 가격표를 받을 수 있습니다. AWS 서비스

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubAllowAll",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceLinkedRole",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OtherServicePermission",
            "Effect": "Allow",
            "Action": [
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "inspector2:BatchGetAccountStatus",
                "pricing:GetProducts"
            ],
            "Resource": "*",
        }
```

```
    ]
}
```

Security Hub 관리형 정책: AWSSecurityHubReadOnlyAccess

`AWSSecurityHubReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Security Hub의 정보를 볼 수 있는 읽기 전용 권한을 사용자에게 부여합니다. 이 정책이 연결된 보안 주체는 Security Hub에서 업데이트를 수행할 수 없습니다. 예를 들어, 이러한 권한이 있는 보안 주체는 자신의 계정과 연결된 조사 결과 목록을 볼 수 있지만 조사 결과의 상태를 변경할 수는 없습니다. 이들은 통찰력 결과는 볼 수 있지만 사용자 지정 통찰력을 만들거나 구성할 수는 없습니다. 이들은 제어 기능 또는 제품 통합을 구성할 수 없습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `securityhub`- 사용자가 항목 목록이나 항목에 대한 세부 정보를 반환하는 작업을 수행할 수 있습니다. 여기에는 `Get`, `List` 또는 `Describe`로 시작하는 API 작업이 포함됩니다.

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

AWS 관리형 정책: AWSSecurityHubOrganizationsAccess

`AWSSecurityHubOrganizationsAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Security Hub와 Organizations의 통합을 지원하는 데 필요한 관리자 권한을 부여합니다. AWS Organizations

이러한 권한을 통해 조직 관리 계정은 Security Hub의 위임된 관리자 계정을 지정할 수 있습니다. 또한, 위임된 Security Hub 관리자 계정을 통해 조직 계정을 멤버 계정으로 활성화할 수 있습니다.

이 정책은 Organizations에 대한 권한만 제공합니다. 조직 관리 계정과 위임된 Security Hub 관리자 계정에도 Security Hub의 관련 작업에 대한 권한이 필요합니다. `AWSSecurityHubFullAccess` 관리형 정책을 사용하여 이러한 권한을 부여할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `organizations:ListAccounts` – 보안 주체가 조직의 일부인 계정 목록을 검색할 수 있습니다.
- `organizations:DescribeOrganization` – 보안 주체가 조직에 대한 정보를 검색할 수 있습니다.
- `organizations:ListRoots` – 보안 주체가 조직의 루트를 나열할 수 있습니다.
- `organizations:ListDelegatedAdministrators` - 보안 주체가 조직의 위임된 관리자를 나열할 수 있습니다.
- `organizations:ListAWSServiceAccessForOrganization`— AWS 서비스 주도자가 조직에서 사용하는 정보를 나열할 수 있습니다.
- `organizations:ListOrganizationalUnitsForParent` – 보안 주체가 상위 OU의 하위 조직 단위(OU)를 나열할 수 있습니다.
- `organizations:ListAccountsForParent` – 보안 주체가 상위 OU의 하위 계정을 나열할 수 있습니다.
- `organizations:DescribeAccount` – 보안 주체가 조직의 계정에 대한 정보를 검색할 수 있습니다.
- `organizations:DescribeOrganizationalUnit` – 보안 주체가 조직의 OU에 대한 정보를 검색할 수 있습니다.
- `organizations:DescribeOrganization` – 보안 주체가 조직 구성에 대한 정보를 검색할 수 있도록 허용합니다.
- `organizations:EnableAWSServiceAccess` – 보안 주체가 Security Hub와 Organizations를 통합할 수 있도록 허용합니다.
- `organizations:RegisterDelegatedAdministrator` – 보안 주체가 Security Hub에 대해 위임된 관리자 계정을 지정할 수 있도록 허용합니다.

- `organizations:DeregisterDelegatedAdministrator` – 보안 주체가 Security Hub에 대해 위임된 관리자 계정을 제거할 수 있도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:ListRoots",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationPermissionsEnable",
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OrganizationPermissionsDelegatedAdmin",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator"
            ],
            "Resource": "arn:aws:organizations::*:account/o-*/*",
            "Condition": {
```

```
            "StringEquals": {
                "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS 관리형 정책: AWSSecurityHubServiceRolePolicy

AWSSecurityHubServiceRolePolicy를 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Security Hub에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결되어 있습니다. 자세한 내용은 the section called “서비스 연결 역할” 섹션을 참조하십시오.

이 정책은 서비스 연결 역할이 Security Hub 제어 기능에 대한 보안 검사를 수행할 수 있도록 하는 관리 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음을 할 수 있는 권한이 포함되어 있습니다.

- cloudtrail— CloudTrail 트레일에 대한 정보를 검색합니다.
- cloudwatch— 현재 CloudWatch 경보를 검색합니다.
- logs— 메트릭 필터를 CloudWatch 로그에 검색합니다.
- sns – SNS 주제에 대한 구독 목록을 검색합니다.
- config— 구성 레코더, 리소스 및 AWS Config 규칙에 대한 정보를 검색합니다. 또한, 서비스 연결 역할이 AWS Config 규칙을 생성 및 삭제하고 규칙에 대한 평가를 실행할 수 있도록 허용합니다.
- iam – 계정에 대한 자격 증명 보고서를 가져오고 생성합니다.
- organizations – 조직의 계정 및 OU(조직 단위) 정보를 검색합니다.
- securityhub – Security Hub 서비스, 표준 및 제어가 구성된 방식에 대한 정보를 검색합니다.
- tag – 리소스 태그에 대한 정보를 검색합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubServiceRolePermissions",
            "Effect": "Allow",
```

```
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "logs:DescribeMetricFilters",
                "sns:ListSubscriptionsByTopic",
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus",
                "config:DescribeConfigRules",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:BatchGetResourceConfig",
                "config:SelectResourceConfig",
                "iam:GenerateCredentialReport",
                "organizations:ListAccounts",
                "config:PutEvaluations",
                "tag:GetResources",
                "iam:GetCredentialReport",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListChildren",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "securityhub:BatchDisableStandards",
                "securityhub:BatchEnableStandards",
                "securityhub:BatchUpdateStandardsControlAssociations",
                "securityhub:BatchGetSecurityControls",
                "securityhub:BatchGetStandardsControlAssociations",
                "securityhub:CreateMembers",
                "securityhub:DeleteMembers",
                "securityhub:DescribeHub",
                "securityhub:DescribeOrganizationConfiguration",
                "securityhub:DescribeStandards",
                "securityhub:DescribeStandardsControls",
                "securityhub:DisassociateFromAdministratorAccount",
                "securityhub:DisassociateMembers",
                "securityhub:DisableSecurityHub",
                "securityhub:EnableSecurityHub",
                "securityhub:GetEnabledStandards",
                "securityhub:ListStandardsControlAssociations",
                "securityhub:ListSecurityControlDefinitions",
                "securityhub:UpdateOrganizationConfiguration",
                "securityhub:UpdateSecurityControl",
```

```
                "securityhub:UpdateSecurityHubConfiguration",
                "securityhub:UpdateStandardsControl",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceRoleConfigPermissions",
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
        },
        {
            "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "securityhub.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Security Hub AWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Security Hub의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Security Hub 문서 기록 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
AWSSecurityHubFullAccess— 기존 정책 업데이트	Security Hub는 AWS 서비스 및 제품에 대한 가격 세부 정보를 제공하도록 정책을 업데이트했습니다.	2024년 4월 24일
AWSSecurityHubReadOnlyAccess— 기존 정책 업데이트	Security Hub는 `Sid` 필드를 추가하여 이 관리형 정책을 업데이트했습니다.	2024년 2월 22일
AWSSecurityHubFullAccess— 기존 정책 업데이트	Security Hub는 Amazon GuardDuty 및 Amazon Inspector가 계정에서 활성화되어 있는지 확인할 수 있도록 정책을 업데이트했습니다. 이를 통해 고객은 여러 개의 보안 관련 정보를 통합할 수 있습니다. AWS 서비스	2023년 11월 16일
AWSSecurityHubOrganizationsAccess— 기존 정책 업데이트	Security Hub는 AWS Organizations 위임된 관리자 기능에 대한 읽기 전용 액세스를 허용하는 추가 권한을 부여하도록 정책을 업데이트했습니다. 여기에는 루트, 조직 단위(OU), 계정, 조직 구조 및 서비스 액세스와 같은 세부 정보가 포함됩니다.	2023년 11월 16일
AWSSecurityHubServiceRolePolicy-기존 정책 업데이트	Security Hub는 사용자 지정 가능한 보안 제어 속성을 읽고 업데이트할 수 있는 `BatchGetSecurityControls` , `DisassociateFromAdministratorAccount`	2023년 11월 26일

변경 사항	설명	날짜
	및 `UpdateSecurityControl` 권한을 추가했습니다.	
AWSSecurityHubServiceRolePolicy-기존 정책 업데이트	Security Hub는 조사 결과와 관련된 리소스 태그를 읽을 수 있는 `tag:GetResources` 권한을 추가했습니다.	2023년 11월 7일
AWSSecurityHubServiceRolePolicy-기존 정책 업데이트	Security Hub는 표준에서 제어 기능의 활성화 상태에 대한 정보를 가져올 수 있는 `BatchGetStandardsControlAssociations` 권한을 추가했습니다.	2023년 9월 27일
AWSSecurityHubServiceRolePolicy-기존 정책 업데이트	Security Hub는 표준 및 제어를 포함하여 AWS Organizations 데이터를 가져오고 Security Hub 구성을 읽고 업데이트할 수 있는 새로운 권한을 추가했습니다.	2023년 9월 20일
AWSSecurityHubServiceRolePolicy-기존 정책 업데이트	Security Hub는 기존 `config:DescribeConfigRuleEvaluationStatus` 권한을 이 정책 내의 다른 설명으로 옮겼습니다. 이제 `config:DescribeConfigRuleEvaluationStatus` 권한이 모든 리소스에 적용됩니다.	2023년 3월 17일

변경 사항	설명	날짜
AWSSecurityHubServiceRolePolicy-기존 정책 업데이트	Security Hub는 기존 `config:PutEvaluations` 권한을 이 정책 내의 다른 설명으로 옮겼습니다. 이제 `config:PutEvaluations` 권한이 모든 리소스에 적용됩니다.	2021년 7월 14일
AWSSecurityHubServiceRolePolicy-기존 정책 업데이트	Security Hub는 서비스 연결 역할이 평가 결과를 AWS Config에 제공할 수 있도록 허용하는 새 권한을 추가했습니다.	2021년 6월 29일
AWSSecurityHubServiceRolePolicy— 관리형 정책 목록에 추가됨	Security Hub 서비스 연결 역할에서 사용하는 관리형 정책에 AWSSecurityHubServiceRolePolicy 대한 정보가 추가되었습니다.	2021년 6월 11일
AWSSecurityHubOrganizationsAccess— 새 정책	Security Hub는 Security Hub와 Organizations의 통합에 필요한 권한을 부여하는 새 정책을 추가했습니다.	2021년 3월 15일
Security Hub가 변경 내용 추적을 시작했습니다	Security Hub는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 3월 15일

AWS Security Hub ID 및 액세스 문제 해결

다음 정보를 사용하여 Security Hub 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- 본인은 Security Hub에서 작업을 수행할 권한이 없습니다.

- 저는 IAM을 수행할 권한이 없습니다. PassRole
- Security Hub에 프로그래밍 방식으로 액세스하고 싶습니다
- 관리자인데, 다른 사용자가 Security Hub에 액세스할 수 있게 허용하려고 함
- 외부 사용자가 내 Security Hub AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

본인은 Security Hub에서 작업을 수행할 권한이 없습니다.

작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 사용자 `mateojackson`이 콘솔을 사용하여 *##*에 대한 세부 정보를 보려고 하지만 `securityhub:`*`GetWidget`* 권한이 없는 경우에 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

이 경우 Mateo는 *`my-example-widget`* 작업을 사용하여 `securityhub:`*`GetWidget`* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Security Hub에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 Security Hub에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 `iam:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

Security Hub에 프로그래밍 방식으로 액세스하고 싶습니다

사용자가 AWS 외부 사용자와 상호 작용하려는 경우 프로그래밍 방식의 액세스가 필요합니다. AWS Management Console프로그래밍 방식의 액세스 권한을 부여하는 방법은 액세스하는 사용자 유형에 따라 다릅니다. AWS

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
작업 인력 ID (IAM Identity Center가 관리하는 사용자)	임시 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 요청에 서명할 수 있습니다. AWS	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • AWS CLI 에 대한 내용은 사용 설명서의 AWS CLI사용을 AWS IAM Identity Center위한 구성을 참조하십시오.AWS Command Line Interface • AWS SDK, 도구 및 AWS API의 경우 AWS SDK 및 도구 참조 안내서의 IAM ID 센터 인증을 참조하십시오.
IAM	임시 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 방식 요청에 서명할 수 있습니다. AWS	IAM 사용 설명서의 AWS 리소스와 함께 임시 자격 증명 사용의 지침을 따르십시오.
IAM	(권장되지 않음) 장기 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 요청에 서명할 수 있습니다. AWS	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 에 대한 내용은 사용 설명서의 IAM 사용자 자격 증명을 사용한 인증을 참조하십시오. AWS CLIAWS Command Line Interface

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
		• AWS SDK 및 도구의 경우 SDK 및 도구 참조 안내서의 장기 자격 증명을 사용한 인증을 참조하십시오.AWS • AWS API의 경우 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하십시오.

관리자인데, 다른 사용자가 Security Hub에 액세스할 수 있게 허용하려고 함

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 내 사용자 및 그룹: AWS IAM Identity Center

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따르십시오.
- 보안 인증 공급자를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 서드 파티 자격 증명 공급자의 역할 만들기(연합)의 지침을 따르십시오.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 IAM 사용자의 역할 생성의 지침을 따르십시오.
  - (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르십시오.

외부 사용자가 내 Security Hub AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하십시오.

- Security Hub에서 이러한 기능을 지원하는지 여부를 알아보려면 IAM의 AWS Security Hub 작동 방식 단원을 참조하십시오.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 페더레이션)을 참조하십시오.
- 교차 계정 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

AWS Security Hub의 규정 준수 확인

타사 감사자는 여러 AWS 규정 준수 프로그램의 일환으로 AWS Security Hub의 보안 및 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램 범위에 속하는 AWS 서비스의 목록은 규정 준수 프로그램 제공 AWS 범위 내 서비스를 참조하십시오. 일반 정보는 AWS 규정 준수 프로그램을 참조하세요.

AWS Artifact를 사용하여 제3자 감사 보고서를 다운로드할 수 있습니다. 자세한 설명은 AWS Artifact의 보고서 다운로드를 참조하십시오.

Security Hub 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다. AWS는 규정 준수를 지원할 다음과 같은 리소스를 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 – 이 배포 안내서에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔 기본 AWS 환경을 배포하기 위한 단계를 제공합니다.
- AWS 규정 준수 리소스 – 사용자의 업계와 위치에 해당할 수 있는 워크북 및 안내서 모음입니다.
- AWS Config – 이 AWS 서비스로 리소스 구성이 내부 관행, 업계 지침 및 규정을 준수하는 정도를 평가할 수 있습니다.
- AWS Security Hub: 이 AWS 서비스는 보안 산업 표준 및 모범 사례 규정 준수 여부를 확인하는 데 도움이 되도록 AWS 내 보안 상태를 종합적으로 보여줍니다.

AWSSecurity Hub의 레질리언스

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며, 이러한 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라 섹션을 참조하세요.

AWS Security Hub에서 인프라 보안

관리형 서비스인 AWS Security Hub은(는) AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스와 AWS의 인프라 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안에 대한 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS에서 게시한 API 호출을 사용하여 네트워크를 통해 Security Hub에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 자격 증명 및 IAM 보안 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)을 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

AWS Security Hub 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

인터페이스 VPC 종단점을 생성하여 VPC와 AWS Security Hub 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 비공개로 Security Hub API에 액세스할 수 있도록 지원하는 AWS PrivateLink 기술로 구동됩니다. VPC의 인스턴스는 Security Hub API와 통신하는 데 퍼블릭 IP 주소를 필요로 하지 않습니다. VPC와 Security Hub 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 탄력적 네트워크 인터페이스로 표현됩니다.

자세한 내용은 AWS PrivateLink 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.

Security Hub VPC 엔드포인트에 대한 고려 사항

Security Hub에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에 AWS PrivateLink 사용 설명서에서 인터페이스 엔드포인트 속성 및 제한 사항을 검토해야 합니다.

Security Hub는 VPC에서 모든 API 작업에 대한 호출 수행을 지원합니다.

> **Note**
>
> Security Hub는 아시아 태평양(오사카) 리전에서는 VPC 엔드포인트를 지원하지 않습니다.

Security Hub에 대한 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔이나 AWS Command Line Interface (AWS CLI)을 사용하여 Security Hub 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다. 자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 사용하여 Security Hub용 VPC 종단점을 생성합니다.

- com.amazonaws.*region*.securityhub

엔드포인트에 프라이빗 DNS를 사용하도록 설정하는 경우, 리전에 대한 기본 DNS 이름(예: `securityhub.us-east-1.amazonaws.com`)을 사용하여 Secrets Manager에 API 요청을 Security Hub로 할 수 있습니다.

자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트를 통해 서비스 액세스를 참조하세요.

Secrets Manager에 대한 VPC 엔드포인트 정책 생성

Security Hub에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 태스크를 수행할 수 있는 보안 주체.

- 수행할 수 있는 작업입니다.
- 태스크를 수행할 있는 리소스.

자세한 내용은 AWS PrivateLink 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

예제: Security Hub 작업에 대한 VPC 엔드포인트 정책

다음은 Security Hub에 대한 엔드포인트 정책의 예입니다. 이 정책은 엔드포인트에 연결될 때 모든 리소스의 모든 보안 주체에 대한 액세스 권한을 나열된 Security Hub 작업에 부여합니다.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

공유 서브넷

공유하는 서브넷의 VPC 엔드포인트는 생성, 설명, 수정 또는 삭제할 수 없습니다. 그러나 공유하는 서브넷의 VPC 엔드포인트를 사용할 수는 있습니다. VPC 공유에 관한 자세한 내용은 Amazon VPC 사용 설명서의 다른 계정과 VPC 공유를 참조하세요.

AWS CloudTrail을 사용하여 AWS Security Hub API 직접 호출 로깅

AWS Security Hub는 사용자, 역할 또는 Security Hub의 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Security Hub에 대한 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 직접 호출에는 Security Hub 콘솔에서 수행한 직접 호출과 Security Hub API 작업에 대한 코드 직접 호출이 포함됩니다. 추적을 생성하면 Security Hub 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail이 수집한 정보를 사용하여 Security Hub에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 사용 방법을 포함하여 CloudTrail에 대한 자세한 내용은 AWS CloudTrail사용 설명서를 참조하세요.

CloudTrail의 Security Hub 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. 지원되는 이벤트 활동이 Security Hub에서 발생하면, 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하십시오.

Security Hub에 대한 이벤트를 포함하여 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 지역의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 추가적으로, CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

Security Hub는 모든 Security Hub API 작업을 CloudTrail 로그에 이벤트로 로깅하는 것을 지원합니다. Security Hub 작업 목록을 보려면 Security Hub API 참조를 참조하세요.

다음 작업에 대한 작업이 CloudTrail에 로깅될 때 `responseElements`의 값은 `null`로 설정됩니다. 이렇게 하면 민감한 정보가 CloudTrail 로그에 포함되지 않습니다.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 보안 인증으로 했는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 다른 AWS 서비스에서 요청했는지 여부

자세한 내용은 CloudTrail userIdentity 요소 섹션을 참조하세요.

예제: Security Hub의 로그 파일 항목

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 정렬된 스택 기록이 아니므로 특정 순서로 표시되지 않습니다.

다음은 `CreateInsight` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예입니다. 이 예에서는 `Test Insight`라는 통찰력이 생성됩니다. `ResourceId` 속성은 그룹화 기준 집계자로 지정되며 이 통찰력을 위한 선택적 필터는 지정되지 않습니다. Insights(인사이트)에 대한 자세한 내용은 AWS Security Hub에서의 인사이트 단원을 참조하십시오.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
```

```
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

AWS Security Hub 리소스 태그 지정

태그는 특정 유형의 AWS Security Hub 리소스를 포함한 AWS 리소스를 선택적으로 정의하고 연결하는 선택적 레이블입니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별하고, 분류하고 관리하는 데 도움이 됩니다. 예를 들어 태그를 사용하여 리소스를 구분하고, 특정 규정 준수 요구 사항 또는 워크플로를 지원하는 리소스를 식별하거나, 비용을 할당할 수 있습니다.

자동화 규칙, 구성 정책, Hub 리소스 등 Security Hub 리소스 유형에 태그를 할당할 수 있습니다.

주제

태그 지정 기본 사항

리소스는 최대 50개의 태그를 가질 수 있습니다. 각 태그는 사용자가 정의하는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그 키는 더 구체적인 태그 값에 대해 카테고리와 같은 역할을 하는 일반적인 레이블입니다. 태그 값은 태그 키에 대한 설명자 역할을 합니다.

예를 들어 환경마다 다른 자동화 규칙(테스트 계정용 자동화 규칙 세트 하나, 프로덕션 계정용 자동화 규칙 세트 하나)을 만드는 경우 해당 규칙에 `Environment` 태그 키를 할당할 수 있습니다. 관련 태그 값은 테스트 계정과 연결된 규칙의 경우 `Test`이고 프로덕션 계정 및 OU와 연결된 규칙의 경우 `Prod`일 수 있습니다.

AWS Security Hub 리소스에 태그를 정의하고 할당할 때 다음 사항에 유의합니다.

- 각 리소스는 최대 50개의 태그를 보유할 수 있습니다.
- 각 리소스에 대해 각 태그 키는 고유하며 하나의 태그 값만 가질 수 있습니다.
- 태그 키와 값은 대소문자를 구분합니다. 모범적으로는 태그를 대문자로 사용하는 전략을 세우고 이러한 전략을 모든 리소스 유형에 대해 일관되게 구현하는 것이 좋습니다.

- 태그 키는 최대 128개의 UTF-8 문자를 포함할 수 있습니다. 태그 값은 최대 256개의 UTF-8 문자를 포함할 수 있습니다. 문자는 문자, 숫자, 공백 또는 _ . : / = + - @ 기호일 수 있습니다.
- `aws:` 접두사는 AWS용으로 예약되어 있습니다. 정의한 태그 키나 값에는 이를 사용할 수 없습니다. 또는 이 접두사를 사용하는 태그 키 또는 값을 변경하거나 제거할 수 없습니다. 이 접두사를 사용하는 태그는 리소스당 50개의 할당량에 포함되지 않습니다.
- 할당한 모든 태그는 본인의 AWS 계정 전용이며, 지정한 AWS 리전에서만 사용할 수 있습니다.
- Security Hub를 사용하여 리소스에 태그를 할당하는 경우 해당 태그는 해당 AWS 리전의 Security Hub에 직접 저장된 리소스에만 적용됩니다. Security Hub가 다른 AWS 서비스에서 생성, 사용 또는 유지 관리하는 관련 지원 리소스에는 적용되지 않습니다. 예를 들어 Amazon Simple Storage Service(S3)와 관련된 조사 결과를 업데이트하는 자동화 규칙에 태그를 할당하는 경우 태그는 지정된 리전의 Security Hub에 있는 자동화 규칙에만 적용됩니다. S3 버킷에는 적용되지 않습니다. 또한 관련 리소스에 태그를 할당하려면 리소스를 저장하는 AWS Resource Groups 또는 AWS 서비스를 사용할 수 있습니다(예: S3 버킷의 경우 Amazon S3). 관련 리소스에 태그를 할당하면 Security Hub 리소스에 대한 지원 리소스를 식별하는 데 도움이 될 수 있습니다.
- 리소스를 삭제하면, 리소스에 지정된 태그 또한 삭제됩니다.

> **Important**
>
> 기밀 또는 기타 유형의 민감한 데이터를 태그에 저장하지 마세요. AWS Billing and Cost Management을(를) 비롯한 여러 AWS 서비스에서 태그에 액세스할 수 있습니다. 태그는 민감한 데이터에 사용하기 위한 것이 아닙니다.

Security Hub 리소스에 태그를 추가하고 관리하려면 Security Hub 콘솔, Security Hub API 또는 AWS Resource Groups Tagging API를 사용할 수 있습니다. Security Hub와 함께라면 리소스를 만들 때 태그를 리소스에 추가할 수 있습니다. 개별 기존 리소스의 태그를 추가하고 관리할 수도 있습니다. 리소스 그룹을 사용하면 Security Hub를 포함하여 여러 AWS 서비스에 걸쳐 있는 여러 기존 리소스에 대해 대량으로 태그를 추가하고 관리할 수 있습니다.

추가 태깅 팁과 모범 사례는 AWS 리소스 태깅 사용 안내서의 AWS 리소스 태그 지정을 참조하세요.

IAM 정책에서 태그 사용

리소스에 태그를 지정한 후 AWS Identity and Access Management(IAM)정책에서 태그 기반의 리소스 수준 권한을 정의할 수 있습니다. 이런 식으로 태그를 사용하면 리소스 생성 및 태그 지정할 권한을 가질 AWS 계정 사용자와 역할은 물론, 보다 일반적으로 태그를 생성, 편집 및 제거할 권한을 가질 사용자

와 역할을 세부적으로 제어할 수 있습니다. 태그를 기반으로 액세스를 제어하려면 IAM 정책의 조건 요소에서 태그 관련 조건 키를 사용하면 됩니다.

예를 들어, 리소스에 대한 Owner 태그가 사용자 이름을 지정하는 경우 사용자가 모든 AWS Security Hub 리소스에 대한 전체 액세스 권한을 갖도록 허용하는 IAM 정책을 생성할 수 있습니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

태그 기반의 리소스 수준 권한을 정의하면 권한이 즉시 적용됩니다. 즉 리소스를 생성하자마자 더 안전하게 보호할 수 있으며 새 리소스에 태그 사용 적용을 빠르게 시작할 수 있습니다. 리소스 수준 권한을 사용하여 새 리소스 및 기존 리소스와 연결할 수 있는 태그 키와 값을 제어할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 태그를 사용하여 AWS 리소스에 대한 액세스 제어를 참조하세요.

AWS Security Hub 리소스에 태그 추가

AWS Security Hub 리소스에 태그를 추가하려면 Security Hub 콘솔 또는 Security Hub API를 사용할 수 있습니다. 콘솔은 Hub 리소스에 태그를 추가하는 것을 지원하지 않습니다.

여러 Security Hub 리소스에 태그를 동시에 추가하려면 AWS Resource Groups Tagging API의 태그 지정 작업을 사용합니다.

> **Important**
>
> 리소스에 태그를 추가하면 리소스에 대한 액세스에 영향을 줄 수 있습니다. 리소스에 태그를 추가하기 전에 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 모든 AWS Identity and Access Management (IAM) 정책을 검토하세요.

Console

리소스에 태그를 추가하려면

자동화 규칙 또는 구성 정책을 만들면 Security Hub 콘솔에서 태그를 추가할 수 있는 옵션을 제공합니다. 태그 섹션에서 태그 키와 태그 값을 제공할 수 있습니다.

Security Hub API & AWS CLI

리소스에 태그를 추가하려면

리소스를 만들고 프로그래밍 방식으로 하나 이상의 태그를 추가하려면 만들려는 리소스 유형에 적합한 작업을 사용하세요.

- 구성 정책을 만들고 여기에 하나 이상의 태그를 추가하려면 CreateConfigurationPolicy API를 호출하거나, AWS CLI를 사용하는 경우 create-configuration-policy 명령을 실행합니다.
- 자동화 규칙을 생성하고 여기에 하나 이상의 태그를 추가하려면 CreateAutomationRule API를 호출하거나, AWS CLI를 사용하는 경우 create-automation-rule 명령을 실행하세요.
- Security Hub를 활성화하고 Hub 리소스에 하나 이상의 태그를 추가하려면 EnableSecurityHub API를 간접적으로 호출하거나 AWS Command Line Interface(AWS CLI)를 사용하는 경우 enable-security-hub 명령을 실행합니다.

요청에서 `tags` 파라미터를 사용하여 리소스에 추가할 각 태그의 태그 키와 선택적 태그 값을 지정합니다. `tags` 파라미터는 객체 배열을 지정합니다. 각 객체는 태그 키 및 연결된 태그 값을 지정합니다.

기존 리소스에 하나 이상의 태그를 추가하려면 Security Hub API의 TagResource 작업을 사용하거나, AWS CLI를 사용하는 경우 tag-resource 명령을 실행합니다. 요청에서 태그를 추가하려는 리소스의 Amazon 리소스 이름(ARN)을 지정합니다. `tags` 파라미터를 사용하여 추가할 각 태그의 태그 키(`key`)와 선택적 태그 값(`value`)을 지정합니다. `tags` 파라미터는 객체의 배열, 각 태그 키당 하나의 개체 및 관련 태그 값을 지정합니다.

예를 들어, 다음 AWS CLI 명령은 지정된 구성 정책에 `Prod` 태그 값을 가진 `Environment` 태그 키를 추가합니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

CLI 명령 예:

```
$ aws securityhub tag-resource \
```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod
```

위치:

- `resource-arn`은 태그를 추가할 구성 정책의 ARN을 지정합니다.
- *`Environment`*은 규칙에 추가할 태그의 태그 키입니다.
- *`Prod`*은 지정된 태그 키의 태그 값입니다(*`Environment`*).

다음 예제에서 명령은 구성 정책에 여러 태그를 추가합니다.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod key=CostCenter,value=12345 key=Owner,value=jane-
doe
```

`tags` 배열의 각 개체에는 `key` 및 `value` 인수가 모두 필요합니다. 그러나 `value` 인수 값은 빈 문자열일 수도 있습니다. 태그 값을 태그 키와 연결하지 않으려면 `value` 인수 값을 지정하지 마세요. 예를 들어 다음 명령은 관련 태그 값이 없는 `Owner` 태그 키를 추가합니다.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

태깅 작업이 성공하면 Security Hub는 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Security Hub는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

AWS Security Hub 리소스에 대한 태그 검토

Security Hub 콘솔 또는 Security Hub API를 사용하여 Security Hub 자동화 규칙 또는 구성 정책의 태그(태그 키 및 태그 값 모두)를 검토할 수 있습니다. 콘솔은 Hub 리소스에 대한 태그 검토를 지원하지 않습니다.

여러 Security Hub 리소스의 태그를 동시에 검토하려면 AWS Resource Groups Tagging API의 태그 지정 작업을 사용합니다.

Console

리소스에 대한 태그를 검토하려면

1. Security Hub 관리자의 보안 인증 정보를 사용하여 https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 태그를 추가하고 싶은 리소스 유형에 따라 다음 중 하나를 수행합니다.
   - 자동화 규칙의 태그를 검토하려면 탐색 창에서 자동화를 선택합니다. 그런 다음 자동화 규칙을 선택합니다.
   - 구성 정책의 태그를 검토하려면 탐색 창에서 구성을 선택합니다. 그런 다음 정책 탭에서 구성 정책 옆에 있는 옵션을 선택합니다. 정책에 할당된 태그 수를 보여주는 사이드 패널이 열립니다. 태그 헤더를 확장하여 태그 키와 태그 값을 볼 수 있습니다.

태그 섹션에는 현재 리소스에 할당된 모든 태그가 나열됩니다.

Security Hub API & AWS CLI

리소스에 대한 태그를 검토하려면

기존 리소스의 태그를 검색하고 검토하려면 ListTagsForResource API를 간접적으로 호출하세요. 요청에서 `resourceArn` 파라미터를 사용하여 리소스의 Amazon 리소스 이름(ARN)을 지정합니다.

AWS CLI을(를) 사용하는 경우, list-tags-for-resource 명령을 실행하고 `resource-arn` 파라미터를 사용하여 리소스의 ARN을 지정합니다. 예제:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

작업이 성공하면 Security Hub는 `tags` 배열을 반환합니다. 배열의 각 객체는 현재 리소스에 할당된 태그(태그 키와 태그 값 모두)를 지정합니다. 예제:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
```

```
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

여기서 `Environment`, `CostCenter`, `Owner`은(는) 리소스에 할당된 태그 키입니다. `Prod`은(는) `Environment` 태그 키에 연결된 태그 값입니다. `12345`은(는) `CostCenter` 태그 키에 연결된 태그 값입니다. `Owner` 태그 키에 연결된 태그 값이 없습니다.

태그가 있는 모든 Security Hub 리소스의 목록과 이러한 각 리소스와 연결된 모든 태그를 검색하려면, AWS Resource Groups Tagging API의 GetResources 작업을 사용하세요. 요청에서 `ResourceTypeFilters` 파라미터 값을 `securityhub`로 설정합니다. AWS CLI을(를) 사용하여 이 작업을 수행하려면 get-resources 명령을 실행하고 `resource-type-filters` 파라미터 값을 `securityhub`로 설정합니다. 예제:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

작업이 성공하면 Resource Groups가 `ResourceTagMappingList` 배열을 반환합니다. 배열에는 태그가 있는 각 Security Hub 리소스에 대해 하나의 객체가 포함됩니다. 각 객체는 Security Hub 리소스의 ARN과 리소스에 할당된 태그 키 및 값을 지정합니다.

AWS Security Hub 리소스의 태그 편집

AWS Security Hub 리소스의 태그(태그 키 또는 태그 값)를 편집하려면 Security Hub API를 사용할 수 있습니다. Security Hub 콘솔은 현재 태그 편집을 지원하지 않습니다.

여러 Security Hub 리소스의 태그를 동시에 편집하려면 AWS Resource Groups Tagging API의 태그 지정 작업을 사용합니다.

> **Important**
>
> 리소스의 태그를 편집하면 리소스 액세스에 영향을 미칠 수 있습니다. 리소스의 태그 키 또는 값을 편집하기 전에 해당 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 모든 AWS Identity and Access Management (IAM) 정책을 검토하세요.

Security Hub API & AWS CLI

리소스의 태그를 편집하려면

프로그래밍 방식으로 리소스의 태그를 편집하면 기존 태그를 새 값으로 덮어씁니다. 따라서 태그를 편집하는 가장 좋은 방법은 태그 키를 편집할지, 태그 값을 편집할지 또는 둘 다를 편집할지에 따라 달라집니다. 태그 키를 편집하려면 현재 태그를 제거하고 새 태그를 추가합니다.

태그 키와 연결된 태그 값만 편집하거나 제거하려면 Security Hub API의 TagResource 작업을 사용하여 기존 값을 덮어씁니다. AWS CLI를 사용하는 경우 tag-resource 명령을 실행하세요. 요청에서 태그 값을 편집하거나 제거하려는 리소스의 Amazon 리소스 이름(ARN)을 지정합니다.

태그 값을 편집하려면 `tags` 파라미터를 사용하여 태그 값을 변경하려는 태그 키를 지정합니다. 또한 키에 새 태그 값을 지정해야 합니다. 예를 들어 다음 AWS CLI 명령은 지정된 자동화 규칙에 할당된 `Environment` 태그 키의 태그 값을 `Prod`에서 `Test`으로 바꿉니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Test
```

위치:

- `resource-arn`은 구성 정책의 ARN을 지정합니다.
- *`Environment`*은 변경할 태그 값과 연결된 태그 키입니다.
- *`Test`*은 지정된 태그 키(*`Environment`*)에 사용할 새 태그 값입니다.

태그 키에서 태그 값을 제거하려면 `tags` 파라미터에 키 `value` 인수 값을 지정하지 마세요. 예제:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

작업이 성공하면 Security Hub는 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Security Hub는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

AWS Security Hub 리소스에서 태그 제거

AWS Security Hub 리소스에서 태그를 제거하려면 Security Hub API를 사용할 수 있습니다. Security Hub 콘솔은 현재 태그 제거를 지원하지 않습니다.

여러 Security Hub 리소스에서 태그를 동시에 제거하려면 AWS Resource Groups Tagging API의 태그 지정 작업을 사용합니다.

> **Important**
>
> 리소스에서 태그를 제거하면 리소스에 대한 액세스에 영향을 줄 수 있습니다. 태그를 제거하기 전에 해당 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 모든 AWS Identity and Access Management (IAM) 정책을 검토하세요.

Security Hub API & AWS CLI

리소스에서 태그를 제거하려면

리소스에서 하나 이상의 태그를 프로그래밍 방식으로 삭제하려면 Security Hub API의 UntagResource 작업을 사용합니다. 요청에서 `resourceArn` 파라미터를 사용하여 태그를 제거할 리소스의 Amazon 리소스 이름 (ARN)을 지정합니다. `tagKeys`파라미터를 사용하여 제거할 태그의 태그 키를 지정합니다. 여러 태그를 제거하려면 제거할 각 태그의 `tagKeys` 파라미터와 인수를 앰퍼샌드(&)로 구분하여 추가합니다—예: `tagKeys=`*`key1`*`&tagKeys=`*`key2`*. 리소스에서 특정 태그 값(태그 키 제외)만 제거하려면 태그를 제거하는 대신 태그를 편집하세요.

AWS CLI를 사용하는 경우 untag-resource 명령을 실행하여 리소스에서 하나 이상의 태그를 제거합니다. `resource-arn` 파라미터에는 태그를 제거할 리소스의 ARN을 지정합니다. `tag-keys`파라미터를 사용하여 제거할 태그의 태그 키를 지정합니다. 예를 들어 다음 명령은 지정된 구성 정책에서 `Environment` 태그(태그 키와 태그 값 모두)를 제거합니다.

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

여기서 `resource-arn`은 태그를 제거할 구성 정책의 ARN을 지정하고, *`Environment`*는 제거할 태그의 태그 키입니다.

리소스에서 여러 태그를 제거하려면, 각 추가 키를 `tag-keys` 파라미터의 인수로 추가합니다. 예제:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

작업이 성공하면 Security Hub는 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Security Hub는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

Security Hub 할당량

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량(이전에는 제한이라고 함)이 있습니다. 이러한 할당량이라 함은 계정의 최대 서비스 리소스 또는 작업 수입니다. 이 주제는 귀하의 계정에 대한 AWS Security Hub 리소스 및 운영에 적용되는 할당량으로 연결됩니다. 별도로 명시되지 않는 한, 각 할당량이 각각의 AWS 리전에서 귀하의 계정에 적용됩니다.

일부 할당량만 늘릴 수 있습니다. 할당량 증가를 요청하려면 Service Quotas 콘솔을 사용합니다. 증가를 요청하는 방법을 알아보려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요. Service Quotas 콘솔에서 할당량을 사용할 수 없는 경우, AWS Support Center Console에 있는 서비스 한도 증가 양식을 사용하여 할당량 증가를 요청하십시오.

최대 할당량

Security Hub 리소스에 적용되는 할당량 목록은 AWS 일반 참조에 있는 AWSSecurity Hub 엔드포인트 및 할당량을 참고하십시오.

비율 할당량

Security Hub API 작업에 적용되는 할당량 목록은 AWSSecurity Hub API 참조 사항을 참고하십시오.

크로스 리전 집계 활성화을(를) 설정한 경우, `BatchImportFindings` 및 `BatchUpdateFindings`에 대한 호출 한 번이 연결된 지역 및 집계 영역에 영향을 줍니다. 이 `GetFindings` 작업은 연결된 영역 및 집계 영역에서 조사 결과를 검색합니다. 하지만, `BatchEnableStandards` 및 `UpdateStandardsControl` 작업은 영역별로 다릅니다.

Security Hub 리전 제한

일부 AWS Security Hub 기능은 특정 지역에서만 사용할 수 AWS 리전있습니다. 다음 섹션에서는 이러한 리전별 제한을 지정합니다.

Security Hubf를 사용할 수 있는 리전 목록은 AWS 일반 참조의 AWS Security Hub 엔드포인트 및 할당량을 참조하십시오.

크로스 리전 집계 제한

에서는 AWS GovCloud (US)지역 간 집계를 검색 결과, 업데이트 검색, 전체 AWS GovCloud (US) 인사이트에만 사용할 수 있습니다. 특히 AWS GovCloud (미국 동부) 와 (미국 서부) 간의 결과, 업데이트 검색 결과 및 인사이트만 집계할 수 있습니다. AWS GovCloud

중국 리전에서는 중국 리전 전반에 대해서만 조사 결과, 조사 결과 업데이트, 인사이트에 대해 크로스 리전 집계를 사용할 수 있습니다. 특히 중국(베이징) 및 중국(닝샤) 간에는 조사 결과, 조사 결과 업데이트, 인사이트만 집계할 수 있습니다.

기본적으로 비활성화된 리전은 집계 리전으로 사용할 수 없습니다. 기본적으로 비활성화되는 리전 목록은 AWS 일반 참조에서 리전 활성화를 참조하십시오.

리전별 통합 사용 가능 여부

일부 통합은 일부 리전에서 사용할 수 없습니다. 특정 리전에서 통합을 사용할 수 없는 경우, 해당 리전을 선택할 때 Security Hub 콘솔의 통합 페이지에 통합이 나열되지 않습니다.

중국(베이징) 및 중국(닝샤)에서 지원되는 통합

중국(베이징) 및 중국(닝샤) 리전에서는 다음과 같은 AWS 서비스와의 통합만 지원합니다.

- AWS Firewall Manager
- 아마존 GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer

- AWS Systems Manager OpsCenter
- AWS Systems Manager 패치 매니저

중국(베이징) 및 중국(닝샤) 리전에서는 다음과 같은 타사 통합만 지원합니다.

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 에서 지원되는 통합

AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 지역은 다음과 같은 서비스 통합만 지원합니다. AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- 아마존 GuardDuty
- AWS Health
- IAM 액세스 분석기
- Amazon Inspector
- AWS IoT Device Defender

AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 지역은 다음과 같은 타사 통합만 지원합니다.

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series((미국 서부) 에서만 사용 가능 AWS GovCloud)
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

리전별 표준 사용 가능 여부

서비스 관리형 표준: 다음을 AWS Control Tower 포함하여 AWS Control Tower 지원하는 지역에서만 사용할 수 있습니다. AWS GovCloud (US) AWS Control Tower 지원하는 지역 목록은 AWS Control Tower 사용 설명서의 AWS 리전 사용 방법을 참조하십시오. AWS Control Tower

AWS 리소스 태깅 표준은 캐나다 서부 (캘거리), 중국 및 지역에서는 사용할 수 없습니다. AWS GovCloud (US)

기타 보안 표준은 Security Hub를 사용할 수 있는 모든 리전에서 사용할 수 있습니다.

리전별 제어 기능 사용 가능 여부

일부 리전에서는 Security Hub 제어 기능을 사용하지 못할 수 있습니다. 각 리전에서 사용할 수 없는 제어 기능의 목록을 보려면 제어 기능에 대한 리전별 제한을 참고하세요. 로그인한 리전에서 제어 기능을 사용할 수 없는 경우 Security Hub 콘솔의 제어 기능 목록에 제어 기능이 표시되지 않습니다. 단, 집계 영역에 로그인한 경우는 예외입니다. 이 경우 집계 영역 또는 하나 이상의 연결된 리전에서 사용할 수 있는 제어 기능을 볼 수 있습니다.

제어 기능에 대한 리전별 제한

AWS Security Hub 컨트롤을 전혀 사용할 수 없는 경우도 AWS 리전있습니다. 이 페이지에는 특정 리전에서 사용할 수 없는 제어 기능이 표시됩니다. 로그인한 리전에서 제어 기능을 사용할 수 없는 경우 Security Hub 콘솔의 제어 기능 목록에 제어 기능이 표시되지 않습니다. 단, 집계 영역에 로그인한 경우는 예외입니다. 이 경우 집계 영역 또는 하나 이상의 연결된 리전에서 사용할 수 있는 제어 기능을 볼 수 있습니다.

목차

- 아시아 태평양(뭄바이)
- 아시아 태평양(멜버른)
- 아시아 태평양(오사카)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- 캐나다(중부)
- 중국(베이징)
- 중국(닝샤)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(밀라노)
- 유럽(파리)
- 유럽(스페인)
- 유럽(스톡홀름)
- 유럽(취리히)
- 이스라엘(텔아비브)
- 중동(바레인)
- 중동(UAE)
- 남아메리카(상파울루)
- AWS GovCloud (미국 동부)
- AWS GovCloud (미국 서부)

미국 동부(버지니아 북부)

다음 제어 기능은 미국 동부(버지니아 북부)에서 지원되지 않습니다.

- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.

- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.
- [ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.

미국 동부(오하이오)

다음 제어 기능은 미국 동부(오하이오)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.

- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.

- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

미국 서부(캘리포니아 북부)

다음 제어 기능은 미국 서부(캘리포니아 북부)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.

- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

미국 서부(오레곤)

다음 제어 기능은 미국 서부(오리건)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.

- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

아프리카(케이프타운)

다음 제어 기능은 아프리카(케이프타운)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.

- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.
- [ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.

- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.

- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

아시아 태평양(홍콩)

다음 제어 기능은 아시아 태평양(홍콩)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.

- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.

- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

아시아 태평양(하이데라바드)

다음 제어 기능은 아시아 태평양(하이데라바드)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations
- [API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다

- [AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.
- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.
- [CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.

- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.

- [EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ELB.5] 애플리케이션 및 Classic Load Balancer 로깅이 활성화되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.

- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess

- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.

- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.

- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
- [Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.6] S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정
- [S3.17] S3 범용 버킷은 저장 시 다음을 사용하여 암호화해야 합니다. AWS KMS keys
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

- [StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

아시아 태평양(자카르타)

다음 제어 기능은 아시아 태평양(자카르타)에서 지원되지 않습니다.

- [Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations
- [API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성에서는 인스턴스 메타데이터 서비스 버전 2 (IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [AutoScaling.9] Amazon EC2 Auto Scaling 그룹은 Amazon EC2 시작 템플릿을 사용해야 합니다.

- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudWatch.17] CloudWatch 알람 조치를 활성화해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.

- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.

- [ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.

- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
- [Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.

- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

아시아 태평양(뭄바이)

다음 제어 기능은 아시아 태평양(뭄바이)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.

- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

아시아 태평양(멜버른)

다음 제어 기능은 아시아 태평양(멜버른)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.4] AWS AppSync GraphQL API는 태그가 지정되어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다
- [AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.

- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.

- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.1] Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.

- [EC2.33] EC2 트랜짓 게이트웨이 첨부 파일에는 태그를 지정해야 합니다.
- [EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.52] EC2 트랜짓 게이트웨이에는 태그가 지정되어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [EKS.6] EKS 클러스터에는 태그를 지정해야 합니다.
- [EKS.7] EKS ID 공급자 구성에는 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] Redis 캐시 ElastiCache 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.

- [ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.
- [ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.

- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.10] IAM 사용자를 위한 암호 정책은 엄격한 기준을 적용해야 합니다. AWS Config
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch

- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.

- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.
- [S3.15] S3 범용 버킷에는 객체 잠금이 활성화되어 있어야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.

- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.1] SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

아시아 태평양(오사카)

다음 제어 기능은 아시아 태평양(오사카)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations
- [API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.

- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.
- [CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.2] DynamoDB 테이블에는 복구가 활성화되어 있어야 합니다. point-in-time
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.1] Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.
- [EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.7] EBS 기본 암호화를 활성화해야 합니다.
- [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.
- [EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.
- [EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.

- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.52] EC2 트랜짓 게이트웨이에는 태그가 지정되어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.
- [ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.
- [ELB.6] 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다.
- [ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config
- [ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.

- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.3] 을 (를) 실수로 AWS KMS keys 삭제해서는 안 됩니다.

- [Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.
- [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.
- [Lambda.3] Lambda 함수는 VPC에 있어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.
- [RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch

- [RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
- [Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
- [S3.15] S3 범용 버킷에는 객체 잠금이 활성화되어 있어야 합니다.
- [S3.17] S3 범용 버킷은 저장 시 다음을 사용하여 암호화해야 합니다. AWS KMS keys
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SecretsManager.1] Secrets Manager 비밀번호에는 자동 로테이션이 활성화되어 있어야 합니다.
- [SecretsManager.2] 자동 순환으로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제
- [SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.1] SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

아시아 태평양(서울)

다음 제어 기능은 아시아 태평양(서울)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.

- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

아시아 태평양(싱가포르)

다음 제어 기능은 아시아 태평양(싱가포르)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.

- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

아시아 태평양(시드니)

다음 제어 기능은 아시아 태평양(시드니)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch

- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

아시아 태평양(도쿄)

다음 제어 기능은 아시아 태평양(도쿄)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.

- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

캐나다(중부)

다음 제어 기능은 캐나다(중부)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.

- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

중국(베이징)

다음 제어 기능은 중국(베이징)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [ACM.3] ACM 인증서에는 태그를 지정해야 합니다.
- [Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [AppSync.4] AWS AppSync GraphQL API는 태그가 지정되어야 합니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다
- [AutoScaling.10] EC2 Auto Scaling 그룹에는 태그를 지정해야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.

- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudTrail.9] CloudTrail 트레일에는 태그를 지정해야 합니다.
- [CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.
- [CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.

- [DynamoDB.5] DynamoDB 테이블에는 태그를 지정해야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.
- [EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.33] EC2 트랜짓 게이트웨이 첨부 파일에는 태그를 지정해야 합니다.
- [EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.35] EC2 네트워크 인터페이스에는 태그를 지정해야 합니다.
- [EC2.36] EC2 고객 게이트웨이에는 태그를 지정해야 합니다.
- [EC2.37] EC2 엘라스틱 IP 주소에는 태그를 지정해야 합니다.
- [EC2.38] EC2 인스턴스에는 태그를 지정해야 합니다.
- [EC2.39] EC2 인터넷 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.41] EC2 네트워크 ACL에는 태그를 지정해야 합니다.
- [EC2.42] EC2 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.43] EC2 보안 그룹에는 태그를 지정해야 합니다.
- [EC2.44] EC2 서브넷에는 태그가 지정되어야 합니다.
- [EC2.45] EC2 볼륨에는 태그가 지정되어야 합니다.
- [EC2.46] 아마존 VPC는 태그가 지정되어야 합니다
- [EC2.47] Amazon VPC 엔드포인트 서비스는 태그가 지정되어야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.
- [EC2.49] Amazon VPC 피어링 연결에는 태그를 지정해야 합니다.
- [EC2.50] EC2 VPN 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.52] EC2 트랜짓 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.
- [EC2.54] EC2 보안 그룹은: :/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.

- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.13] ECS 서비스에는 태그를 지정해야 합니다.
- [ECS.14] ECS 클러스터에는 태그를 지정해야 합니다.
- [ECS.15] ECS 작업 정의에는 태그를 지정해야 합니다.
- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [EKS.6] EKS 클러스터에는 태그를 지정해야 합니다.
- [EKS.7] EKS ID 공급자 구성에는 태그를 지정해야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .
- [ES.9] Elasticsearch 도메인에는 태그를 지정해야 합니다.
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.

- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.23] IAM 액세스 분석기 분석기는 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess
- [IAM.28] IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.2] Kinesis 스트림에는 태그가 지정되어야 합니다.
- [Lambda.6] Lambda 함수는 태그가 지정되어야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.7] Network Firewall 방화벽에는 태그를 지정해야 합니다.
- [NetworkFirewall.8] Network Firewall 방화벽 정책에 태그를 지정해야 합니다.
- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [PCA.1] AWS Private CA 루트 인증 기관을 비활성화해야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.
- [RDS.29] RDS DB 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [RDS.30] RDS DB 인스턴스에는 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.32] RDS DB 스냅샷에는 태그가 지정되어야 합니다.
- [RDS.33] RDS DB 서브넷 그룹에는 태그가 지정되어야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.11] Redshift 클러스터에는 태그를 지정해야 합니다.
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [Redshift.14] Redshift 클러스터 서브넷 그룹은 태그가 지정되어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
- [S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.
- [S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.
- [S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제
- [SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.
- [SecretsManager.5] Secrets Manager 비밀에는 태그를 지정해야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

중국(닝샤)

다음 제어 기능은 중국(닝샤)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [ACM.3] ACM 인증서에는 태그를 지정해야 합니다.
- [Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.

- [AppSync.4] AWS AppSync GraphQL API는 태그가 지정되어야 합니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다
- [AutoScaling.10] EC2 Auto Scaling 그룹에는 태그를 지정해야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudTrail.9] CloudTrail 트레일에는 태그를 지정해야 합니다.
- [CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.
- [CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.

- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.5] DynamoDB 테이블에는 태그를 지정해야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.
- [EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.33] EC2 트랜짓 게이트웨이 첨부 파일에는 태그를 지정해야 합니다.
- [EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.35] EC2 네트워크 인터페이스에는 태그를 지정해야 합니다.
- [EC2.36] EC2 고객 게이트웨이에는 태그를 지정해야 합니다.
- [EC2.37] EC2 엘라스틱 IP 주소에는 태그를 지정해야 합니다.
- [EC2.38] EC2 인스턴스에는 태그를 지정해야 합니다.
- [EC2.39] EC2 인터넷 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.41] EC2 네트워크 ACL에는 태그를 지정해야 합니다.
- [EC2.42] EC2 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.43] EC2 보안 그룹에는 태그를 지정해야 합니다.
- [EC2.44] EC2 서브넷에는 태그가 지정되어야 합니다.
- [EC2.45] EC2 볼륨에는 태그가 지정되어야 합니다.

- [EC2.46] 아마존 VPC는 태그가 지정되어야 합니다
- [EC2.47] Amazon VPC 엔드포인트 서비스는 태그가 지정되어야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.
- [EC2.49] Amazon VPC 피어링 연결에는 태그를 지정해야 합니다.
- [EC2.50] EC2 VPN 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.52] EC2 트랜짓 게이트웨이에는 태그가 지정되어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.13] ECS 서비스에는 태그를 지정해야 합니다.
- [ECS.14] ECS 클러스터에는 태그를 지정해야 합니다.
- [ECS.15] ECS 작업 정의에는 태그를 지정해야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [EKS.6] EKS 클러스터에는 태그를 지정해야 합니다.
- [EKS.7] EKS ID 공급자 구성에는 태그를 지정해야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .
- [ES.9] Elasticsearch 도메인에는 태그를 지정해야 합니다.
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.23] IAM 액세스 분석기 분석기는 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess
- [IAM.28] IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.2] Kinesis 스트림에는 태그가 지정되어야 합니다.
- [Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.
- [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.

- [Lambda.3] Lambda 함수는 VPC에 있어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.6] Lambda 함수는 태그가 지정되어야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.7] Network Firewall 방화벽에는 태그를 지정해야 합니다.
- [NetworkFirewall.8] Network Firewall 방화벽 정책에 태그를 지정해야 합니다.
- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.

- [PCA.1] AWS Private CA 루트 인증 기관을 비활성화해야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.
- [RDS.29] RDS DB 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [RDS.30] RDS DB 인스턴스에는 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.32] RDS DB 스냅샷에는 태그가 지정되어야 합니다.
- [RDS.33] RDS DB 서브넷 그룹에는 태그가 지정되어야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.11] Redshift 클러스터에는 태그를 지정해야 합니다.
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [Redshift.14] Redshift 클러스터 서브넷 그룹은 태그가 지정되어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.

- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
- [S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제
- [SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.
- [SecretsManager.5] Secrets Manager 비밀에는 태그를 지정해야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

유럽(프랑크푸르트)

다음 제어 기능은 유럽(프랑크푸르트)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.

- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

유럽(아일랜드)

다음 제어 기능은 유럽(아일랜드)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.

- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

유럽(런던)

다음 제어 기능은 유럽(런던)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.

- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

유럽(밀라노)

다음 제어 기능은 유럽(밀라노)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.

- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.
- [ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [KMS.3] 을 (를) 실수로 AWS KMS keys 삭제해서는 안 됩니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.
- [RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

유럽(파리)

다음 제어 기능은 유럽(파리)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch

- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

유럽(스페인)

다음 제어 기능은 유럽(스페인)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations
- [API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.

- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다
- [AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.
- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.
- [CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail
- [CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.

- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.
- [DynamoDB.2] DynamoDB 테이블에는 복구가 활성화되어 있어야 합니다. point-in-time
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.1] Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.
- [EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.
- [EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.

- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.
- [EC2.7] EBS 기본 암호화를 활성화해야 합니다.
- [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.
- [EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.
- [EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS

- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.
- [ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.
- [ELB.5] 애플리케이션 및 Classic Load Balancer 로깅이 활성화되어야 합니다.
- [ELB.6] 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다.
- [ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config
- [ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess

- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS
- [Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.
- [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.
- [Lambda.3] Lambda 함수는 VPC에 있어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.

- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config
- [RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.
- [RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.
- [RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.
- [RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

- [RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.
- [RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
- [Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.
- [S3.6] S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정
- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

- [S3.9] S3 범용 버킷은 서버 액세스 로깅을 활성화해야 합니다.
- [S3.15] S3 범용 버킷에는 객체 잠금이 활성화되어 있어야 합니다.
- [S3.17] S3 범용 버킷은 저장 시 다음을 사용하여 암호화해야 합니다. AWS KMS keys
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SecretsManager.2] 자동 순환으로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.1] SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

유럽(스톡홀름)

다음 제어 기능은 유럽(스톡홀름)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.

- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

유럽(취리히)

다음 제어 기능은 유럽(취리히)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.

- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다
- [AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.
- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.
- [CloudTrail.7] S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인하십시오. CloudTrail
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.

- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.
- [DynamoDB.2] DynamoDB 테이블에는 복구가 활성화되어 있어야 합니다. point-in-time
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

- [EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.
- [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.
- [EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.
- [EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.

- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.
- [ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.
- [ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config
- [ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.

- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다

- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.

- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.
- [RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.
- [RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SecretsManager.2] 자동 순환으로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.1] SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

이스라엘(텔아비브)

다음 제어 기능은 이스라엘(텔아비브)에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.4] AWS AppSync GraphQL API는 태그가 지정되어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다
- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.

- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

- [EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.33] EC2 트랜짓 게이트웨이 첨부 파일에는 태그를 지정해야 합니다.
- [EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.52] EC2 트랜짓 게이트웨이에는 태그가 지정되어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.

- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [EKS.6] EKS 클러스터에는 태그를 지정해야 합니다.
- [EKS.7] EKS ID 공급자 구성에는 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.4] Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다.
- [ELB.6] 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다.
- [ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] Redis 캐시 ElastiCache 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.
- [ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.10] IAM 사용자를 위한 암호 정책은 엄격한 기준을 적용해야 합니다. AWS Config
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.

- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.23] IAM 액세스 분석기 분석기는 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess
- [IAM.28] IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.2] Kinesis 스트림에는 태그가 지정되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.

- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [PCA.1] AWS Private CA 루트 인증 기관을 비활성화해야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.

- [RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.
- [RDS.29] RDS DB 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.
- [S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다.
- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
- [S3.9] S3 범용 버킷은 서버 액세스 로깅을 활성화해야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.

- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SecretsManager.1] Secrets Manager 비밀번호에는 자동 로테이션이 활성화되어 있어야 합니다.
- [SecretsManager.2] 자동 순환으로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제
- [SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.1] SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.12] AWS WAF 규칙에는 메트릭이 활성화되어 있어야 합니다. CloudWatch

중동(바레인)

다음 제어 기능은 중동(바레인)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.20] 사이트 간 AWS VPN 연결을 위한 두 VPN 터널이 모두 작동해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.

- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS

- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

중동(UAE)

다음 제어 기능은 중동(UAE)에서 지원되지 않습니다.

- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [API Gateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다
- [AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.
- [백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.

- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없도록 하십시오.
- [CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.
- [CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.
- [CloudWatch.17] CloudWatch 알람 조치를 활성화해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.

- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.
- [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.

- [EFS.1] 유휴 파일 데이터를 사용하여 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.
- [ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.
- [ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] Redis 캐시 ElastiCache 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.
- [ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.

- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.18] 다음과 같은 사고를 관리할 지원 역할이 생성되었는지 확인하십시오. AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.

- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.4] 키 로테이션을 활성화해야 합니다. AWS KMS
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.7] Network Firewall 방화벽에는 태그를 지정해야 합니다.
- [NetworkFirewall.8] Network Firewall 방화벽 정책에 태그를 지정해야 합니다.
- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.

- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.2] RDS DB 인스턴스는 기간에 따라 퍼블릭 액세스를 금지해야 합니다. PubliclyAccessible AWS Config
- [RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.
- [RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.
- [RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.
- [RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.

- [S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다.
- [S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.
- [S3.6] S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정
- [S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SecretsManager.1] Secrets Manager 비밀번호에는 자동 로테이션이 활성화되어 있어야 합니다.
- [SecretsManager.2] 자동 순환으로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제
- [SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.1] SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [SSM.1] Amazon EC2 인스턴스는 다음을 통해 관리해야 합니다. AWS Systems Manager
- [StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.

남아메리카(상파울루)

다음 제어 기능은 남아메리카(상파울루)에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.

- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.16] RDS DB 클러스터는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

AWS GovCloud (미국 동부)

다음 컨트롤은 AWS GovCloud (미국 동부) 에서 지원되지 않습니다.

- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [ACM.3] ACM 인증서에는 태그를 지정해야 합니다.

- [계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정
- [Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.4] AWS AppSync GraphQL API는 태그가 지정되어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포함해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성에서는 인스턴스 메타데이터 서비스 버전 2 (IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [AutoScaling.9] Amazon EC2 Auto Scaling 그룹은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [AutoScaling.10] EC2 Auto Scaling 그룹에는 태그를 지정해야 합니다.
- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudTrail.9] CloudTrail 트레일에는 태그를 지정해야 합니다.
- [CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.
- [CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.
- [CloudWatch.17] CloudWatch 알람 조치를 활성화해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.

- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.5] DynamoDB 테이블에는 태그를 지정해야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.
- [EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.33] EC2 트랜짓 게이트웨이 첨부 파일에는 태그를 지정해야 합니다.
- [EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.35] EC2 네트워크 인터페이스에는 태그를 지정해야 합니다.
- [EC2.36] EC2 고객 게이트웨이에는 태그를 지정해야 합니다.
- [EC2.37] EC2 엘라스틱 IP 주소에는 태그를 지정해야 합니다.
- [EC2.38] EC2 인스턴스에는 태그를 지정해야 합니다.
- [EC2.39] EC2 인터넷 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.41] EC2 네트워크 ACL에는 태그를 지정해야 합니다.
- [EC2.42] EC2 라우팅 테이블에는 태그를 지정해야 합니다.

- [EC2.43] EC2 보안 그룹에는 태그를 지정해야 합니다.
- [EC2.44] EC2 서브넷에는 태그가 지정되어야 합니다.
- [EC2.45] EC2 볼륨에는 태그가 지정되어야 합니다.
- [EC2.46] 아마존 VPC는 태그가 지정되어야 합니다
- [EC2.47] Amazon VPC 엔드포인트 서비스는 태그가 지정되어야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.
- [EC2.49] Amazon VPC 피어링 연결에는 태그를 지정해야 합니다.
- [EC2.50] EC2 VPN 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.52] EC2 트랜짓 게이트웨이에는 태그가 지정되어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.
- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [ECS.13] ECS 서비스에는 태그를 지정해야 합니다.
- [ECS.14] ECS 클러스터에는 태그를 지정해야 합니다.
- [ECS.15] ECS 작업 정의에는 태그를 지정해야 합니다.
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.

- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [EKS.6] EKS 클러스터에는 태그를 지정해야 합니다.
- [EKS.7] EKS ID 공급자 구성에는 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ELB.2] SSL/HTTPS 리스너를 사용하는 클래식 로드 밸런서는 에서 제공한 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.8] SSL 리스너를 사용하는 클래식 로드 밸런서는 지속 기간이 엄격한 사전 정의된 보안 정책을 사용해야 합니다. AWS Config
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] Redis 캐시 ElastiCache 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.
- [ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .

- [ES.9] Elasticsearch 도메인에는 태그를 지정해야 합니다.
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.1] 을 GuardDuty 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.23] IAM 액세스 분석기 분석기는 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.
- [IAM.28] IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.2] Kinesis 스트림에는 태그가 지정되어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.6] Lambda 함수는 태그가 지정되어야 합니다.

- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.7] Network Firewall 방화벽에는 태그를 지정해야 합니다.
- [NetworkFirewall.8] Network Firewall 방화벽 정책에 태그를 지정해야 합니다.
- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [PCA.1] AWS Private CA 루트 인증 기관을 비활성화해야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.
- [RDS.29] RDS DB 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [RDS.30] RDS DB 인스턴스에는 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.32] RDS DB 스냅샷에는 태그가 지정되어야 합니다.
- [RDS.33] RDS DB 서브넷 그룹에는 태그가 지정되어야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.11] Redshift 클러스터에는 태그를 지정해야 합니다.

- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [Redshift.14] Redshift 클러스터 서브넷 그룹은 태그가 지정되어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷은 수명 주기 구성을 가져야 합니다.
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.
- [S3.12] ACL은 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 됩니다.
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.
- [S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제
- [SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.
- [SecretsManager.5] Secrets Manager 비밀에는 태그를 지정해야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.

- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.12] AWS WAF 규칙에는 메트릭이 활성화되어 있어야 합니다. CloudWatch

AWS GovCloud (미국 서부)

다음 컨트롤은 AWS GovCloud (미국 서부) 에서 지원되지 않습니다.

- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [ACM.3] ACM 인증서에는 태그를 지정해야 합니다.
- [계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정
- [Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [ApiGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.
- [AppSync.4] AWS AppSync GraphQL API는 태그가 지정되어야 합니다.
- [AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.
- [Athena.2] Athena 데이터 카탈로그에는 태그가 지정되어야 합니다.
- [Athena.3] Athena 워크그룹은 태그가 지정되어야 합니다

- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포함해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성에서는 인스턴스 메타데이터 서비스 버전 2 (IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [AutoScaling.9] Amazon EC2 Auto Scaling 그룹은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [AutoScaling.10] EC2 Auto Scaling 그룹에는 태그를 지정해야 합니다.
- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [백업.2] AWS Backup 복구 지점에 태그를 지정해야 합니다.
- [백업.3] AWS Backup 저장소에 태그를 지정해야 합니다.
- [백업.4] AWS Backup 보고서 계획에는 태그를 지정해야 합니다.
- [백업.5] AWS Backup 백업 계획에 태그를 지정해야 합니다.
- [CloudFormation.2] CloudFormation 스택에는 태그를 지정해야 합니다.
- [CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요해야 합니다.
- [CloudFront.4] CloudFront 배포에는 원본 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에는 태그를 지정해야 합니다.
- [CloudTrail.9] CloudTrail 트레일에는 태그를 지정해야 합니다.
- [CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.
- [CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.
- [CloudWatch.17] CloudWatch 알람 조치를 활성화해야 합니다.
- [CodeArtifact.1] CodeArtifact 저장소에는 태그를 지정해야 합니다.

- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 일반 텍스트 자격 증명이 포함되어서는 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild1.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config기간이 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.
- [Detective.1] 탐정 행동 그래프에는 태그를 지정해야 합니다
- [DMS.2] DMS 인증서에는 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에는 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에는 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에는 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.5] DynamoDB 테이블에는 태그를 지정해야 합니다.
- [DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.
- [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.

- [EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.33] EC2 트랜짓 게이트웨이 첨부 파일에는 태그를 지정해야 합니다.
- [EC2.34] EC2 트랜짓 게이트웨이 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.35] EC2 네트워크 인터페이스에는 태그를 지정해야 합니다.
- [EC2.36] EC2 고객 게이트웨이에는 태그를 지정해야 합니다.
- [EC2.37] EC2 엘라스틱 IP 주소에는 태그를 지정해야 합니다.
- [EC2.38] EC2 인스턴스에는 태그를 지정해야 합니다.
- [EC2.39] EC2 인터넷 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.41] EC2 네트워크 ACL에는 태그를 지정해야 합니다.
- [EC2.42] EC2 라우팅 테이블에는 태그를 지정해야 합니다.
- [EC2.43] EC2 보안 그룹에는 태그를 지정해야 합니다.
- [EC2.44] EC2 서브넷에는 태그가 지정되어야 합니다.
- [EC2.45] EC2 볼륨에는 태그가 지정되어야 합니다.
- [EC2.46] 아마존 VPC는 태그가 지정되어야 합니다
- [EC2.47] Amazon VPC 엔드포인트 서비스는 태그가 지정되어야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에는 태그를 지정해야 합니다.
- [EC2.49] Amazon VPC 피어링 연결에는 태그를 지정해야 합니다.
- [EC2.50] EC2 VPN 게이트웨이에는 태그가 지정되어야 합니다.
- [EC2.52] EC2 트랜짓 게이트웨이에는 태그가 지정되어야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리는 태그를 지정해야 합니다.

- [ECS.1] Amazon ECS 작업 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다.
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [ECS.13] ECS 서비스에는 태그를 지정해야 합니다.
- [ECS.14] ECS 클러스터에는 태그를 지정해야 합니다.
- [ECS.15] ECS 작업 정의에는 태그를 지정해야 합니다.
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 자격 증명을 적용해야 합니다.
- [EFS.5] EFS 액세스 포인트는 태그가 지정되어야 합니다.
- [EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.
- [EKS.6] EKS 클러스터에는 태그를 지정해야 합니다.
- [EKS.7] EKS ID 공급자 구성에는 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF
- [ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

- [ElastiCache.2] Redis 캐시 ElastiCache 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.
- [ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.
- [ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .
- [ES.9] Elasticsearch 도메인에는 태그를 지정해야 합니다.
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템은 백업에 태그를 복사하도록 구성해야 합니다.
- [GlobalAccelerator.1] 글로벌 액셀러레이터 액셀러레이터에는 태그를 지정해야 합니다.
- [Glue.1] AWS Glue 작업에는 태그를 지정해야 합니다.
- [GuardDuty.2] GuardDuty 필터에는 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPset에는 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에는 태그를 지정해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.23] IAM 액세스 분석기 분석기는 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에는 태그를 지정해야 합니다.

- [IAM.25] IAM 사용자에게는 태그를 지정해야 합니다.
- [IAM.28] IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.
- [IoT.1] AWS IoT Core 보안 프로필에 태그를 지정해야 합니다.
- [IoT.2] AWS IoT Core 완화 조치에는 태그를 지정해야 합니다.
- [IoT.3] AWS IoT Core 치수에 태그를 지정해야 합니다.
- [IoT.4] AWS IoT Core 권한 부여자는 태그를 지정해야 합니다
- [IoT.5] AWS IoT Core 역할 별칭은 태그가 지정되어야 합니다
- [IoT.6] AWS IoT Core 정책에는 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.2] Kinesis 스트림에는 태그가 지정되어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.6] Lambda 함수는 태그가 지정되어야 합니다.
- [Macie.1] Amazon Macie를 활성화해야 합니다
- [Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch
- [MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [MQ.4] Amazon MQ 브로커에는 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.

- [NetworkFirewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] Network Firewall 정책에는 하나 이상의 규칙 그룹이 연결되어 있어야 합니다.
- [NetworkFirewall.4] Network Firewall 정책의 기본 상태 비저장 작업은 전체 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.5] Network Firewall 정책의 기본 상태 비저장 작업은 프래그먼트화된 패킷의 경우 삭제 또는 전달이어야 합니다.
- [NetworkFirewall.6] 스테이트리스 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.7] Network Firewall 방화벽에는 태그를 지정해야 합니다.
- [NetworkFirewall.8] Network Firewall 방화벽 정책에 태그를 지정해야 합니다.
- [NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 중 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] 로그에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다 CloudWatch .
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .
- [Opensearch.9] OpenSearch 도메인에는 태그를 지정해야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다.
- [PCA.1] AWS Private CA 루트 인증 기관을 비활성화해야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.

- [RDS.28] RDS DB 클러스터에는 태그를 지정해야 합니다.
- [RDS.29] RDS DB 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [RDS.30] RDS DB 인스턴스에는 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에는 태그를 지정해야 합니다.
- [RDS.32] RDS DB 스냅샷에는 태그가 지정되어야 합니다.
- [RDS.33] RDS DB 서브넷 그룹에는 태그가 지정되어야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.11] Redshift 클러스터에는 태그를 지정해야 합니다.
- [Redshift.12] Redshift 이벤트 알림 구독에는 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에는 태그를 지정해야 합니다.
- [Redshift.14] Redshift 클러스터 서브넷 그룹은 태그가 지정되어야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다.
- [Route53.1] Route 53 상태 확인에는 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷은 수명 주기 구성을 가져야 합니다.
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.
- [S3.12] ACL은 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 됩니다.
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.
- [S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.

- [SES.1] SES 연락처 목록에는 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 시크릿 삭제
- [SecretsManager.4] Secrets Manager 비밀은 지정된 일수 내에 교체되어야 합니다.
- [SecretsManager.5] Secrets Manager 비밀에는 태그를 지정해야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS
- [SNS.3] SNS 주제에는 태그를 지정해야 합니다.
- [SQS.2] SQS 대기열에는 태그가 지정되어야 합니다.
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.1] AWS Transfer Family 워크플로에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다.
- [WAF.1] AWS WAF 클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.
- [WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.12] AWS WAF 규칙에는 메트릭이 활성화되어 있어야 합니다. CloudWatch

Security Hub 비활성화

> **Note**
>
> 중앙 구성을 사용하는 경우 AWS Security Hub 위임된 관리자는 특정 계정 및 OU(조직 단위)에서 Security Hub를 비활성화하고 다른 계정에서는 Security Hub를 활성화하도록 유지하는 구성 정책을 만들 수 있습니다. 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다. 자세한 내용은 중앙 구성 작동 방식 섹션을 참조하세요.

Security Hub를 비활성화하려면 Security Hub 콘솔, Security Hub API 또는 AWS CLI를 사용하면 됩니다.

계정에 대해 Security Hub를 비활성화하면 다음과 같은 결과가 발생합니다.

- 계정에 대한 새로운 조사 결과는 처리되지 않습니다.
- 90일 후에는 기존 결과와 통찰력 및 모든 Security Hub 구성 설정이 삭제되고 복구할 수 없게 됩니다.

  기존 결과를 저장하려면 Security Hub를 비활성화하기 전에 결과를 내보내야 합니다. 자세한 내용은 the section called “계정 작업이 Security Hub 데이터에 미치는 영향” 섹션을 참조하세요.
- 활성화된 표준 및 제어가 모두 비활성화됩니다.

다음과 같은 경우에는 Security Hub를 비활성화할 수 없습니다.

- 계정이 조직의 지정된 Security Hub 관리자 계정입니다. 중앙 구성을 사용하는 경우 Security Hub를 비활성화하는 구성 정책을 위임된 관리자 계정과 연결할 수 없습니다. 다른 계정에도 연결할 수 있지만 Security Hub는 이러한 정책을 위임된 관리자 계정에 적용하지 않습니다.
- 계정이 초대에 의한 Security Hub 관리자 계정이며 활성화된 구성원 계정이 있습니다. Security Hub를 비활성화하려면 먼저, 모든 구성원 계정을 연결 해제해야 합니다. the section called “멤버 계정 연결 해제” 섹션을 참조하세요.

구성원 계정에 대해 Security Hub를 비활성화하려면 먼저 계정을 관리자 계정에서 연결을 해제해야 합니다. 조직 계정의 경우 관리자 계정만 구성원 계정 연결을 해제할 수 있습니다. 자세한 내용은 the section called “조직 구성원 계정의 연결 해제” 섹션을 참조하세요. 수동으로 초대된 계정의 경우 관리자 계정 또는 구성원 계정으로 구성원 계정 연결을 해제할 수 있습니다. 자세한 내용은 the section called “멤버 계정 연결 해제” 또는 the section called “관리자 계정과의 연결 해제” 섹션을 참조하세요.

중앙 구성을 사용하는 경우 특정 구성원 계정에서 Security Hub를 비활성화하는 정책을 만들 수 있으므로 연결 해제가 필요하지 않습니다.

계정에서 Security Hub를 비활성화하면 현재 리전에서만 비활성화됩니다. 하지만 중앙 구성을 사용하여 특정 계정에서 Security Hub를 비활성화하면 홈 리전 및 연결된 모든 리전에서 Security Hub가 비활성화됩니다.

원하는 방법을 선택하고 단계에 따라 Security Hub를 비활성화하세요.

Security Hub console

Security Hub를 비활성화하려면

1. https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 일반을 선택합니다.
4. AWS Security Hub 비활성화에서 AWS Security Hub 비활성화를 선택합니다. 그런 다음 AWS Security Hub 비활성화를 다시 선택합니다.

Security Hub API

Security Hub를 비활성화하려면

`DisableSecurityHub` API를 호출합니다.

AWS CLI

Security Hub를 비활성화하려면

`disable-security-hub` 명령을 실행합니다.

명령 예시:

```
aws securityhub disable-security-hub
```

Security Hub 제어 기능의 변경 로그

다음 변경 로그는 기존 AWS Security Hub 보안 통제에 대한 중요한 변경 사항을 추적하며, 이로 인해 제어의 전체 상태와 조사 결과의 규정 준수 상태가 변경될 수 있습니다. Security Hub가 제어 기능의 상태를 평가하는 방법에 대한 자세한 내용은 규정 준수 상태 및 제어 상태을 참조하십시오. 변경 사항이 이 로그에 입력한 후 제어 기능을 사용할 수 있는 모든 AWS 리전 항목에 영향을 미치려면 며칠이 걸릴 수 있습니다.

이 로그는 2023년 4월 이후 발생한 변경 사항을 추적합니다.

컨트롤을 선택하면 컨트롤에 대한 자세한 내용을 볼 수 있습니다. 제목 변경은 90일 동안 각 컨트롤의 세부 설명에 기록됩니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 6월 25일	[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.	이 AWS Config 컨트롤은 활성화 여부를 확인하고, 서비스 연결 역할을 사용하고, 활성화된 컨트롤의 리소스를 기록합니다. Security Hub는 컨트롤의 평가 내용을 반영하도록 컨트롤 제목을 업데이트했습니다.
2024년 6월 14일	[RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch	이 컨트롤은 Amazon Aurora MySQL DB 클러스터가 감사 로그를 Amazon Logs에 게시하도록 구성되어 있는지 여부를 확인합니다. CloudWatch Security Hub는 Aurora 서버리스 v1 DB 클러스터에 대한 검색 결과를 생성

변경 날짜	제어 ID 및 제목	변경 내용 설명
		하지 않도록 제어를 업데이트했습니다.
2024년 6월 10일	[Config.1] AWS Config 을 활성화하고 리소스 기록에 서비스 연결 역할을 사용해야 합니다.	이 AWS Config 컨트롤은 활성화되어 있고 AWS Config 리소스 기록이 켜져 있는지 확인합니다. 이전에는 모든 리소스에 대해 기록을 구성한 경우에만 컨트롤에서 PASSED 검색 결과를 생성했습니다. Security Hub는 컨트롤을 활성화하는 데 필요한 리소스에 대해 기록이 켜져 있을 때 PASSED 검색 결과를 생성하도록 컨트롤을 업데이트했습니다. 또한 필요한 리소스를 기록할 수 있는 권한을 제공하는 AWS Config 서비스 연결 역할의 사용 여부를 확인하도록 컨트롤이 업데이트되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 5월 8일	[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.	이 컨트롤은 Amazon S3 범용 버전 관리 버킷에 멀티 팩터 인증(MFA) 삭제가 활성화되어 있는지 확인합니다. 이전에는 컨트롤에서 수명 주기 구성이 있는 버킷에 대한 FAILED 검색 결과를 생성했습니다. 하지만 수명 주기 구성이 있는 버킷에서는 버전 관리를 통한 MFA 삭제를 활성화할 수 없습니다. Security Hub는 수명 주기 구성이 있는 버킷에 대한 검색 결과가 나오지 않도록 제어를 업데이트했습니다. 제어 설명이 현재 동작을 반영하도록 업데이트되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 5월 2일	[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.	Security Hub가 조사 결과를 합격으로 생성하기 위해 Amazon EKS 클러스터를 실행할 수 있는 가장 오래된 지원 버전의 Kubernetes를 업데이트했습니다. 현재 지원되는 버전 중 가장 오래된 버전은 Kubernetes 1.26입니다.
2024년 4월 30일	[CloudTrail.3] 하나 이상의 트레일을 활성화해야 합니다. CloudTrail	제어 제목이 CloudTrail 활성화되어야 함에서 하나 이상의 CloudTrail 트레일로 변경되었습니다. 이 AWS 계정 컨트롤은 현재 a에 하나 이상의 CloudTrail 트레일이 활성화되어 있는지 여부를 PASSED 검색합니다. 제목과 설명이 현재 행동을 정확하게 반영하도록 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 4월 29일	[AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.	제어 제목이 Classic Load Balancer와 연결된 Auto Scaling 그룹에서 로드 밸런서 상태 확인을 사용해야 한다는 것으로 변경되었습니다. 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다. 이 컨트롤은 현재 애플리케이션, 게이트웨이, 네트워크 및 클래식 로드 밸런서를 평가합니다. 제목과 설명이 현재 동작을 정확하게 반영하도록 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 4월 19일	[CloudTrail.1] 은 읽기 및 쓰기 관리 이벤트가 포함된 다중 지역 트레일을 하나 이상 사용하여 활성화하고 CloudTrail 구성해야 합니다.	AWS CloudTrail 컨트롤은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 지역 트레일로 활성화 및 구성되었는지 여부를 확인합니다. 이전에는 계정에서 하나 이상의 다중 지역 트레일을 CloudTrail 활성화하고 구성한 경우, 읽기 및 쓰기 관리 이벤트를 캡처한 트레일이 없더라도 컨트롤에서 PASSED 검색 결과를 잘못 생성했습니다. 이제 CloudTrail 컨트롤은 읽기 및 쓰기 관리 이벤트를 캡처하는 다중 지역 트레일을 하나 이상 사용하도록 설정하고 구성한 경우에만 PASSED 검색 결과를 생성합니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 4월 10일	[Athena.1] Athena 워크그룹은 유휴 상태에서 암호화되어야 합니다	Security Hub는 이 제어 기능을 사용 중지했으며 모든 표준에서 제거했습니다. Athena 워크그룹은 아마존 심플 스토리지 서비스(Amazon S3) 버킷으로 로그를 전송합니다. Amazon S3는 이제 새로운 S3 버킷과 기존 S3 버킷에 S3 관리형 키(SS3-S3)를 사용한 기본 암호화를 제공합니다.
2024년 4월 10일	[AutoScaling.4] Auto Scaling 그룹 시작 구성의 메타데이터 응답 홉 제한은 1보다 커서는 안 됩니다.	Security Hub는 이 제어 기능을 사용 중지했으며 모든 표준에서 제거했습니다. Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스의 메타데이터 응답 홉 제한은 워크로드에 따라 다릅니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 4월 10일	[CloudFormation.1] CloudFormation 스택은 Simple Notification Service (SNS) 와 통합되어야 합니다.	Security Hub는 이 제어 기능을 사용 중지했으며 모든 표준에서 제거했습니다. AWS CloudFormation 스택을 Amazon SNS 주제와 통합하는 것은 더 이상 보안 모범 사례가 아닙니다. 중요한 CloudFormation 스택을 SNS 주제와 통합하는 것이 유용할 수 있지만 모든 스택에 반드시 필요한 것은 아닙니다.
2024년 4월 10일	[CodeBuild.5] CodeBuild 프로젝트 환경에는 권한 모드가 활성화되어 있지 않아야 합니다.	Security Hub는 이 제어 기능을 사용 중지했으며 모든 표준에서 제거했습니다. CodeBuild 프로젝트에서 권한 모드를 활성화해도 고객 환경에 추가적인 위험이 초래되지는 않습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 4월 10일	[IAM.20] 루트 사용자의 사용을 피하세요.	Security Hub는 이 제어 기능을 사용 중지했으며 모든 표준에서 제거했습니다. 이 컨트롤의 용도는 다른 컨트롤인 에서 다릅니다. [CloudWatch.1] “root” 사용자가 사용하려면 로그 메트릭 필터 및 경보가 있어야 합니다.
2024년 4월 10일	[SNS.2] 주제에 전송된 알림 메시지에 대해 배달 상태 로깅을 활성화해야 합니다.	Security Hub는 이 제어 기능을 사용 중지했으며 모든 표준에서 제거했습니다. SNS 주제에 대한 전송 상태를 기록하는 것은 더 이상 보안 모범 사례가 아닙니다. 중요한 SNS 주제에 대한 로깅 전송 상태가 유용할 수 있지만 모든 주제에 필수 사항은 아닙니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 4월 10일	[S3.10] 버전 관리가 활성화된 S3 범용 버킷은 수명 주기 구성을 가져야 합니다.	Security Hub는 AWS 기본 보안 모범 사례 및 서비스 관리 표준:에서 이 컨트롤을 제거했습니다. AWS Control Tower이 컨트롤의 용도는 두 개의 다른 컨트롤인 및 에서 다룹니다. [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다. [S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다. 이 컨트롤은 여전히 NIST SP 800-53 개정판 5의 일부입니다.
2024년 4월 10일	[S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.	Security Hub는 AWS 기본 보안 모범 사례 및 서비스 관리 표준:에서 이 컨트롤을 제거했습니다. AWS Control Tower S3 버킷에 대한 이벤트 알림이 유용한 경우도 있지만 이는 보편적인 보안 모범 사례는 아닙니다. 이 컨트롤은 여전히 NIST SP 800-53 버전 5의 일부입니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 4월 10일	[SNS.1] SNS 주제는 유휴 상태에서 다음을 사용하여 암호화해야 합니다. AWS KMS	Security Hub는 AWS 기본 보안 모범 사례 및 서비스 관리 표준:에서 이 컨트롤을 제거했습니다. AWS Control Tower SNS는 이미 기본적으로 주제를 암호화하므로 주제를 암호화하는 AWS KMS 데 사용하는 것은 더 이상 보안 모범 사례로 권장되지 않습니다. 이 컨트롤은 여전히 NIST SP 800-53 버전 5의 일부입니다.
2024년 4월 8일	[ELB.6] 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다.	제어 제목을 Application Load Balancer 삭제 보호를 활성화해야 하지만 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서는 삭제 보호를 활성화해야 합니다. 이 컨트롤은 현재 애플리케이션, 게이트웨이 및 네트워크 로드 밸런서를 평가합니다. 제목과 설명이 현재 동작을 정확하게 반영하도록 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 3월 22일	[Opensearch.8] 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다 OpenSearch .	제어 제목이 TLS 1.2를 사용하여 OpenSearch 도메인에 대한 연결을 암호화해야 함에서 OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다. 이전에는 컨트롤이 OpenSearch 도메인 연결에서 TLS 1.2를 사용하는지 여부만 확인했습니다. 이제 컨트롤을 통해 OpenSearch 도메인이 최신 TLS 보안 정책을 사용하여 암호화되었는지 여부를 확인할 수 있습니다. PASSED 컨트롤 제목과 설명이 현재 동작을 반영하도록 업데이트되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 3월 22일	[ES.8] Elasticsearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다.	Elasticsearch 도메인으로의 연결에서 변경된 제어 제목은 TLS 1.2를 사용하여 암호화해야 하고, Elasticsearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화해야 합니다. 이전에는 컨트롤이 Elasticsearch 도메인에 대한 연결에서 TLS 1.2를 사용하는지 여부만 확인했습니다. 이제 컨트롤을 통해 Elasticsearch 도메인이 최신 TLS 보안 정책을 사용하여 암호화되었는지 여부를 확인할 수 있습니다. PASSED 컨트롤 제목과 설명이 현재 동작을 반영하도록 업데이트되었습니다.
2024년 3월 12일	[S3.1] S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다.	S3 퍼블릭 액세스 차단 설정에서 S3 범용 버킷의 제목을 퍼블릭 액세스 차단 설정이 활성화되도록 변경해야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 3월 12일	[S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.	S3 버킷에서 제목을 변경하면 S3 범용 버킷에 대한 공개 읽기 액세스가 금지되어야 합니다. 범용 버킷은 공개 읽기 액세스를 차단해야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다.	S3 버킷에서 제목을 변경하면 S3 범용 버킷에 대한 공개 쓰기 액세스가 금지되어야 합니다. 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.5] S3 범용 버킷에는 SSL 사용 요청이 있어야 합니다.	S3 버킷에서 제목을 변경하면 보안 소켓 계층 사용 요청이 필요하고, S3 범용 버킷은 SSL 사용 요청이 필요하고, S3 범용 버킷은 SSL 사용 요청이 필요합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 3월 12일	[S3.6] S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정	버킷 정책에서 다른 AWS 계정 사람에게 부여된 S3 권한에서 제목을 변경한 경우 S3로 제한해야 합니다. 범용 버킷 정책은 다른 사용자에 대한 액세스를 제한해야 AWS 계정 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.7] S3 범용 버킷은 지역 간 복제를 사용해야 합니다.	S3 버킷에서 제목을 변경하면 지역 간 복제가 활성화되어야 하고 S3 범용 버킷은 지역 간 복제를 사용해야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.7] S3 범용 버킷은 지역 간 복제를 사용해야 합니다.	S3 버킷에서 제목을 변경하면 지역 간 복제가 활성화되어야 하고 S3 범용 버킷은 지역 간 복제를 사용해야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 3월 12일	[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.	S3 퍼블릭 액세스 차단 설정의 제목을 버킷 수준에서 활성화해야 하며 S3 범용 버킷은 퍼블릭 액세스를 차단하도록 변경되었습니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.9] S3 범용 버킷은 서버 액세스 로깅을 활성화해야 합니다.	제목을 S3 버킷 서버 액세스 로깅을 활성화해야 하는 것에서 S3 범용 버킷에 대해 서버 액세스 로깅을 활성화해야 하는 것으로 변경했습니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.10] 버전 관리가 활성화된 S3 범용 버킷은 수명 주기 구성을 가져야 합니다.	버전 관리가 활성화된 S3 버킷에서 제목을 변경한 경우 수명 주기 정책이 구성되어 있어야 하며 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 3월 12일	[S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.	제목을 S3 버킷에서 변경하면 이벤트 알림이 활성화되고, S3 범용 버킷에는 이벤트 알림이 활성화되어야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.12] ACL은 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 됩니다.	S3 액세스 제어 목록(ACL) 에서 변경된 제목은 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 되며, ACL은 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 사용해서는 안 됩니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.	S3 버킷에서 제목을 변경하면 수명 주기 정책이 구성되어 있어야 하고 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 3월 12일	[S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.	S3 버킷에서 변경된 제목은 버전 관리를 사용해야 하며, S3 범용 버킷은 버전 관리를 활성화해야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.15] S3 범용 버킷에는 객체 잠금이 활성화되어 있어야 합니다.	S3 버킷에서 변경된 제목은 객체 잠금을 사용하도록 구성해야 하며, S3 범용 버킷은 객체 잠금을 활성화해야 합니다. Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.
2024년 3월 12일	[S3.17] S3 범용 버킷은 저장 시 다음을 사용하여 암호화해야 합니다. AWS KMS keys	S3 버킷에서 변경된 제목은 저장 상태에서 AWS KMS keys암호화해야 하며 S3 범용 버킷은 저장 시 암호화해야 합니다. AWS KMS keys Security Hub는 새로운 S3 버킷 유형을 반영하도록 제목을 변경했습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 3월 7일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. Security Hub는 이제 `nodejs20.x` 및 `ruby3.3` 을 매개변수로 지원합니다.
2024년 2월 22일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. 이제 Security Hub는 파라미터로 `dotnet8`를 지원합니다.
2024년 2월 5일	[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.	Security Hub가 조사 결과를 합격으로 생성하기 위해 Amazon EKS 클러스터를 실행할 수 있는 가장 오래된 지원 버전의 Kubernetes를 업데이트했습니다. 현재 지원되는 버전 중 가장 오래된 버전은 Kubernetes `1.25`입니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2024년 1월 10일	[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 자격 증명이 포함되어서는 안 됩니다.	CodeBuild GitHub 제목이나 Bitbucket 소스 리포지토리 URL은 OAuth를 사용해야 하며 CodeBuild Bitbucket 소스 리포지토리 URL은 민감한 자격 증명을 포함해서는 안 됩니다. Security Hub는 다른 연결 방법도 안전할 수 있기 때문에 OAuth에 대한 언급을 삭제했습니다. Security Hub는 GitHub 소스 저장소 URL에 더 이상 개인 액세스 토큰 또는 사용자 이름 및 암호를 포함할 수 GitHub 없으므로 에 대한 언급을 삭제했습니다.
2024년 1월 8일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. Security Hub는 더 이상 `go1.x` 및 `java8`을 파라미터로 지원하지 않습니다. 사용 중지된 런타임이기 때문입니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 12월 29일	[RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.	RDS.8은 지원되는 데이터베이스 엔진 중 하나를 사용하는 Amazon RDS DB 인스턴스에 삭제 보호가 활성화되어 있는지 확인합니다. 이제 Security Hub는 `custom-oracle-ee`, `oracle-ee-cdb` 및 `oracle-se2-cdb` 를 데이터베이스 엔진으로 지원합니다.
2023년 12월 22일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. 이제 Security Hub는 `java21` 및 `python3.12` 을 파라미터로 지원합니다. Security Hub는 더 이상 `ruby2.7`를 파라미터로 지원하지 않습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 12월 15일	[CloudFront.1] CloudFront 배포판에는 기본 루트 개체가 구성되어 있어야 합니다.	CloudFront.1은 Amazon CloudFront 배포에 기본 루트 객체가 구성되어 있는지 확인합니다. Security Hub는 기본 루트 객체를 추가하는 것이 사용자의 애플리케이션 및 특정 요구 사항에 따라 달라지는 권장 사항이기 때문에 이 제어의 심각도를 심각에서 높음으로 낮췄습니다.
2023년 12월 5일	[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.	제어 기능의 제목이 보안 그룹은 0.0.0.0/0에서 포트 22로의 수신을 허용하지 않아야 합니다에서 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용하지 않아야 합니다로 변경되었습니다.
2023년 12월 5일	[EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.	제어 기능의 제목이 0.0.0.0/0에서 포트 3389로의 수신을 허용하는 보안 그룹이 없는지 확인합니다에서 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용하지 않아야 합니다로 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 12월 5일	[RDS.9] RDS DB 인스턴스는 로그를 로그에 게시해야 합니다. CloudWatch	데이터베이스 로깅에서 RDS로 제어 제목을 변경해야 합니다. DB 인스턴스는 로그를 Logs에 CloudWatch 게시해야 합니다. Security Hub는 이 컨트롤이 로그가 Amazon Logs에 게시되었는지 여부만 확인하고 RDS CloudWatch 로그의 활성화 여부는 확인하지 않는다는 것을 확인했습니다. 컨트롤은 RDS DB 인스턴스가 로그를 Logs에 게시하도록 구성되었는지 여부를 확인합니다. PASSED CloudWatch 제어 기능의 제목이 현재 동작을 반영하여 업데이트되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 11월 17일	[EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.	EC2.19가 보안 그룹에 대한 무제한 수신 트래픽이 위험이 높다고 간주되는 지정된 포트에 액세스할 수 있는지 여부를 확인합니다. 관리형 접두사 목록이 보안 그룹 규칙의 원본으로 제공될 때 이를 반영하도록 Security Hub가 이 제어 기능을 업데이트했습니다. 이 제어는 접두사 목록에 '0.0.0.0/0' 또는 '::/0' 문자열이 포함된 경우 FAILED 결과를 생성합니다.
2023년 11월 16일	[CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.	제어 제목을 CloudWatch 경보에서 변경하려면 ALARM 상태에 맞게 CloudWatch 구성된 작업이 있어야 하며 경보에는 지정된 작업이 구성되어 있어야 합니다.
2023년 11월 16일	[CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.	CloudWatch 로그 그룹에서 변경된 제어 제목은 최소 1년 동안 보존되어야 하며, CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 11월 16일	[Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.	제어 기능의 제목이 VPC Lambda 함수는 두 개 이상의 가용 영역에서 작동해야 합니다에서 VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다로 변경되었습니다.
2023년 11월 16일	[AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.	제어 기능의 제목이 AWS AppSync 는 request-level 및 field-level 로깅을 활성화된 상태로 두어야 합니다에서 AWS AppSync 는 field-level 로깅을 활성화된 상태로 두어야 합니다로 변경되었습니다.
2023년 11월 16일	[EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.	Amazon Elastic MapReduce 클러스터 마스터 노드에는 퍼블릭 IP 주소가 없어야 하며 Amazon EMR 클러스터 기본 노드에는 퍼블릭 IP 주소가 없어야 한다는 제어 제목이 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 11월 16일	[Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.	제어 제목이 OpenSearch 도메인에서 VPC에 있어야 하며 OpenSearch도메인은 공개적으로 액세스할 수 없도록 변경되었습니다.
2023년 11월 16일	[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.	제어 기능의 제목이 Elasticsearch 도메인은 VPC에 있어야 합니다에서 Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다로 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 10월 31일	[ES.4] 로그에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다 CloudWatch .	ES.4는 Elasticsearch 도메인이 오류 로그를 Amazon Logs로 전송하도록 구성되어 있는지 확인합니다. CloudWatch 이 컨트롤은 이전에 Logs로 전송하도록 구성된 로그를 포함하는 Elasticsearch 도메인에 대한 PASSED 검색 결과를 생성했습니다. CloudWatch Security Hub는 오류 로그를 로그로 전송하도록 구성된 Elasticsearch 도메인에 대한 검색 PASSED 결과만 생성하도록 제어를 업데이트했습니다. CloudWatch 또한, 오류 로그를 지원하지 않는 Elasticsearch 버전을 평가에서 제외하도록 제어 기능을 업데이트했습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 10월 16일	[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.	EC2.13은 보안 그룹이 포트 22에 대한 무제한 수신 액세스를 허용하는지 확인합니다. 관리형 접두사 목록이 보안 그룹 규칙의 원본으로 제공될 때 이를 반영하도록 Security Hub가 이 제어 기능을 업데이트했습니다. 이 제어는 접두사 목록에 '0.0.0.0/0' 또는 '::/0' 문자열이 포함된 경우 FAILED 결과를 생성합니다.
2023년 10월 16일	[EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.	EC2.14는 보안 그룹이 포트 3389에 대한 무제한 수신 액세스를 허용하는지 확인합니다. 관리형 접두사 목록이 보안 그룹 규칙의 원본으로 제공될 때 이를 반영하도록 Security Hub가 이 제어 기능을 업데이트했습니다. 이 제어는 접두사 목록에 '0.0.0.0/0' 또는 '::/0' 문자열이 포함된 경우 FAILED 결과를 생성합니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 10월 16일	[EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.	EC2.18은 사용 중인 보안 그룹이 무제한 수신 트래픽을 허용하는지 여부를 확인합니다. 관리형 접두사 목록이 보안 그룹 규칙의 원본으로 제공될 때 이를 반영하도록 Security Hub가 이 제어 기능을 업데이트했습니다. 이 제어는 접두사 목록에 '0.0.0.0/0' 또는 '::/0' 문자열이 포함된 경우 FAILED 결과를 생성합니다.
2023년 10월 16일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. 이제 Security Hub는 파라미터로 python3.11 를 지원합니다.
2023년 10월 4일	[S3.7] S3 범용 버킷은 지역 간 복제를 사용해야 합니다.	Security Hub가 S3 버킷에서 동일 리전 복제 대신 리전 간 복제가 활성화되도록 하기 위해 값이 CROSS-REGION 인 파라미터 ReplicationType 을 추가했습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 9월 27일	[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.	Security Hub가 조사 결과를 합격으로 생성하기 위해 Amazon EKS 클러스터를 실행할 수 있는 가장 오래된 지원 버전의 Kubernetes를 업데이트했습니다. 현재 지원되는 버전 중 가장 오래된 버전은 Kubernetes `1.24`입니다.
2023년 9월 20일	CloudFront.2 — CloudFront 배포에는 원본 액세스 ID가 활성화되어 있어야 합니다.	Security Hub는 이 제어 기능을 사용 중지했으며 모든 표준에서 제거했습니다. 대신에 [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다. 섹션을 참조하세요. 원본 액세스 제어 기능은 현재 보안 모범 사례입니다. 이 제어는 90일 후에 설명서에서 제거됩니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 9월 20일	[EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.	Security Hub는 AWS 기본 보안 모범 사례(FSBP) 및 미국 국립 표준 기술 연구소(NIST) SP 800-53 개정 5에서 이 제어 기능을 제거했습니다. 이는 여전히 서비스 관리 표준의 일부입니다. AWS Control Tower 이 제어는 보안 그룹이 EC2 인스턴스 또는 탄력적 네트워크 인터페이스에 연결된 경우 통과된 결과를 생성합니다. 하지만, 특정 사용 사례에 대해서는 연결되지 않은 보안 그룹이 보안 위험을 초래하지는 않습니다. EC2.2, EC2.13, EC2.14, EC2.18, EC2.19 등의 다른 EC2 제어를 사용하여 보안 그룹을 모니터링할 수 있습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 9월 20일	EC2.29 – EC2 인스턴스는 VPC에서 시작되어야 합니다.	Security Hub는 이 제어 기능을 사용 중지했으며 모든 표준에서 제거했습니다. Amazon EC2는 EC2-Classic 인스턴스를 VPC로 마이그레이션했습니다. 이 제어는 90일 후에 설명서에서 제거됩니다.
2023년 9월 20일	S3.4 – S3 버킷에는 서버 측 암호화가 활성화되어 있어야 합니다.	Security Hub는 이 제어 기능을 사용 중지했으며 모든 표준에서 제거했습니다. Amazon S3는 이제 새로운 S3 버킷과 기존 S3 버킷에 S3 관리형 키(SS3-S3)를 사용한 기본 암호화를 제공합니다. SS3-S3 또는 SS3-KMS 서버 측 암호화로 암호화된 기존 버킷의 암호화 설정은 변경되지 않습니다. 이 제어는 90일 후에 설명서에서 제거됩니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 9월 14일	[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.	제어 기능의 제목이 VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됨에서 VPC 기본 보안 그룹들은 인바운드 또는 아웃바운드 트래픽을 허용해서는 안 됨으로 변경되었습니다.
2023년 9월 14일	[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.	제어 기능의 제목이 가상 MFA는 루트 사용자에 대해 활성화되어야 함에서 MFA는 루트 사용자에 대해 활성화되어야 함으로 변경되었습니다.
2023년 9월 14일	[RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.	제어 기능의 제목이 중요 클러스터 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 함에서 중요 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 함으로 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 9월 14일	[RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.	제어 기능의 제목이 중요 데이터베이스 인스턴스 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 함에서 중요 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 함으로 변경되었습니다.
2023년 9월 14일	[WAF.2] AWS WAF 클래식 지역 규칙에는 하나 이상의 조건이 있어야 합니다.	제어 기능의 제목이 WAF 리전 규칙에는 하나 이상의 조건이 있어야 함에서 AWS WAF 클래식 리전 규칙에는 하나 이상의 조건이 있어야 함으로 변경되었습니다.
2023년 9월 14일	[WAF.3] AWS WAF 클래식 지역 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.	제어 기능의 제목이 WAF 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 함에서 AWS WAF 클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 함으로 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 9월 14일	[WAF.4] AWS WAF 클래식 지역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.	제어 기능의 제목이 WAF 리전 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함에서 AWS WAF 클래식 리전 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함으로 변경되었습니다.
2023년 9월 14일	[WAF.6] AWS WAF 클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.	제어 기능의 제목이 WAF 전역 규칙에는 하나 이상의 조건이 있어야 함에서 AWS WAF 클래식 전역 규칙에는 하나 이상의 조건이 있어야 함으로 변경되었습니다.
2023년 9월 14일	[WAF.7] AWS WAF 클래식 글로벌 규칙 그룹에는 규칙이 하나 이상 있어야 합니다.	제어 기능이 제목이 WAF 전역 규칙 그룹에는 하나 이상의 규칙이 있어야 함에서 AWS WAF 클래식 전역 규칙 그룹에는 하나 이상의 규칙이 있어야 함으로 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 9월 14일	[WAF.8] AWS WAF 클래식 글로벌 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.	제어 기능의 제목이 WAF 전역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함에서 AWS WAF 클래식 전역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함으로 변경되었습니다.
2023년 9월 14일	[WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.	제어 기능의 제목이 WAFv2 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함에서 AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함으로 변경되었습니다.
2023년 9월 14일	[WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.	제어 기능의 제목이 AWS WAF v2 웹 ACL 로깅을 활성화해야 함에서 AWS WAF 웹 ACL 로깅을 활성화해야 함으로 변경되었습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 7월 20일	S3.4 – S3 버킷에는 서버 측 암호화가 활성화되어 있어야 합니다.	S3.4는 Amazon S3 버킷에 서버 측 암호화가 활성화되어 있는지 또는 S3 버킷 정책이 서버 측 암호화되지 않은 `PutObject` 요청을 명시적으로 거부하는지 확인합니다. Security Hub가 KMS 키를 사용한 이중 계층 서버 측 암호화(DSSE-KMS)를 포함하도록 이 제어 기능을 업데이트했습니다. 이 제어 기능은 S3 버킷이 SSE-S3, SSE-KMS 또는 DSSE-KMS로 암호화될 때 조사 결과를 합격으로 발생시킵니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 7월 17일	[S3.17] S3 범용 버킷은 저장 시 다음을 사용하여 암호화해야 합니다. AWS KMS keys	S3.17은 Amazon S3 버킷이 AWS KMS key를 사용하여 암호화되었는지 여부를 확인합니다. Security Hub가 KMS 키를 사용한 이중 계층 서버 측 암호화(DSSE-KMS)를 포함하도록 이 제어 기능을 업데이트했습니다. 이 제어 기능은 S3 버킷이 SSE-KMS 또는 DSSE-KMS로 암호화될 때 조사 결과를 합격으로 발생시킵니다.
2023년 6월 9일	[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.	EKS.2는 Amazon EKS 클러스터가 지원되는 Kubernetes 버전에서 실행되고 있는지 확인합니다. 현재 지원되는 가장 오래된 버전은 `1.23`입니다.
2023년 6월 9일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. 이제 Security Hub는 파라미터로 `ruby3.2`를 지원합니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 6월 5일	[APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.	APIGateway.5.는 Amazon API Gateway REST API 스테이지의 모든 메서드가 저장 시 암호화되어 있는지 확인합니다. Security Hub가 특정 메서드에 대해 캐싱이 활성화된 경우에만 해당 메서드의 암호화를 평가하도록 제어 기능을 업데이트했습니다.
2023년 5월 18일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. 이제 Security Hub는 파라미터로 `java17`를 지원합니다.
2023년 5월 18일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. Security Hub는 더 이상 `nodejs12.x` 를 파라미터로 지원하지 않습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 4월 23일	[ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.	ECS.10은 Amazon ECS Fargate 서비스가 최신 Fargate 플랫폼 버전을 실행하고 있는지 여부를 확인합니다. 고객은 ECS를 통해 직접 또는 를 사용하여 Amazon ECS를 배포할 수 있습니다. CodeDeploy Security Hub는 ECS Fargate 서비스를 배포하는 CodeDeploy 데 사용할 때 합격 결과를 생성하도록 이 제어 기능을 업데이트했습니다.
2023년 4월 20일	[S3.6] S3 범용 버킷 정책은 다른 버킷에 대한 액세스를 제한해야 합니다. AWS 계정	S3.6은 Amazon Simple Storage Service (Amazon S3) 버킷 정책이 다른 AWS 계정 보안 주체가 S3 버킷의 리소스에서 거부된 작업을 수행하는 것을 방지하는지 확인합니다. Security Hub가 버킷 정책에서 조건문을 반영하도록 제어 기능을 업데이트했습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 4월 18일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. 이제 Security Hub는 파라미터로 `python3.10` 를 지원합니다.
2023년 4월 18일	[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 설정된 예상 값과 일치하는지 확인합니다. Security Hub는 더 이상 `dotnetcore3.1` 를 파라미터로 지원하지 않습니다.

변경 날짜	제어 ID 및 제목	변경 내용 설명
2023년 4월 17일	[RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.	RDS.11은 Amazon RDS 인스턴스에 백업 보존 기간이 7일 이상인 자동 백업이 활성화되어 있는지 여부를 확인합니다. 모든 엔진이 읽기 전용 복제본의 자동 백업을 지원하는 것은 아니므로 Security Hub는 읽기 전용 복제본을 평가에서 제외하도록 이 제어 기능을 업데이트했습니다. 또한, RDS는 읽기 전용 복제본을 생성할 때 백업 보존 기간을 지정하는 옵션을 제공하지 않습니다. 읽기 전용 복제본은 기본적으로 백업 보존 기간을 0으로 설정하여 생성됩니다.

AWS Security Hub 사용 설명서의 문서 기록

다음 표에서는 AWS Security Hub 설명서의 업데이트 내용을 설명합니다.

> **Note**
>
> 보안 제어 릴리스의 경우 지정된 날짜는 모든 계정 및 리전에서 제어 기능을 사용할 수 있는 날짜입니다. 제어 기능이 모든 계정 및 리전에 도달하는 데 1~2주가 소요될 수 있습니다.

변경 사항	설명	날짜
CIS AWS 재단 벤치마크 v3.0.0 출시	Security Hub는 인터넷 보안 센터 (CIS) AWS 재단 벤치마크 v3.0.0을 출시했습니다. 이 릴리스에는 다음과 같은 새 컨트롤과 여러 기존 컨트롤에 대한 매핑이 포함됩니다. • the section called “[EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.” • the section called “[EC2.54] EC2 보안 그룹은: :/0에서 원격 서버 관리 포트로의 수신을 허용해서는 안 됩니다.” • the section called “[IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다.” • the section called “[IAM.27] IAM ID에는 정책이 연결되어 있지 않아야 합니다. AWSCloudShellFullAccess ”	2024년 5월 13일

- the section called “[IAM.28] IAM 액세스 분석기 외부 액세스 분석기를 활성화해야 합니다.”
- the section called “[S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.”
- the section called “[S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.”

새 보안 제어	다음 새 Security Hub 제어를 사용할 수 있습니다. • the section called “[DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화되어야 합니다.” • the section called “[DMS.10] Neptune 데이터베이스의 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.” • the section called “[DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.” • the section called “[DMS.12] Redis용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.” • the section called “[DynamoDB.7] DynamoDB 액셀러레이터 클러스터는 전송 중에 암호화되어야 합니다.” • the section called “[EFS.6] EFS 탑재 대상은 퍼블릭 서브넷과 연결되지 않아야 합니다.” • the section called “[EKS.3] EKS 클러스터는 암호화된 쿠버네티스 비밀을 사용해야 합니다.” • the section called “[FSx.2] FSx for Lustre 파일 시스템	2024년 5월 3일

은 백업에 태그를 복사하도록 구성해야 합니다."

- the section called "[MQ.2] ActiveMQ 브로커는 감사 로그를 다음으로 스트리밍해야 합니다. CloudWatch "
- the section called "[MQ.3] Amazon MQ 브로커는 자동 마이너 버전 업그레이드를 활성화해야 합니다."
- the section called "[Opensearch.11] OpenSearch 도메인에는 전용 기본 노드가 3개 이상 있어야 합니다."
- the section called "[Redshift.15] Redshift 보안 그룹은 제한된 출처의 클러스터 포트에서만 수신을 허용해야 합니다."
- the section called "[SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다."
- the section called "[Service Catalog.1] Service Catalog 포트폴리오는 조직 내에서만 공유해야 합니다. AWS"
- the section called "[Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용하지 않아야 합니다."

AWS 리소스 태깅 표준	Security Hub의 AWS 리소스 태깅 표준은 이제 표준에 적용되는 새로운 컨트롤과 함께 정식 버전으로 제공됩니다.	2024년 4월 30일
기존 관리형 정책 업데이트	Security Hub는 AWS 서비스 및 제품에 대한 가격 세부 정보를 가져오기 `AmazonSecurityHubFullAccess` 위해 이름이 지정된 AWS 관리형 정책을 업데이트했습니다.	2024년 4월 24일
제어 매개변수의 컨텍스트 내 구성	중앙 구성을 사용하는 경우 이제 Security Hub 콘솔에 있는 컨트롤의 세부 정보 페이지에서 컨텍스트에 맞게 제어 매개변수를 구성할 수 있습니다.	2024년 3월 29일
기존 관리형 정책 업데이트	Security Hub는 `Sid` 필드를 `AWSSecurityHubReadOnlyAccess` 추가하여 이름이 지정된 AWS 관리형 정책을 업데이트했습니다.	2024년 2월 22일
새로운 보안 제어	이제 Macie.2] Macie의 민감한 데이터 자동 검색 기능을 활성화할 수 있습니다. 이 제어에 대한 지역별 제한은 지역별 제어 사용 가능 여부를 참조하십시오.	2024년 2월 19일

Security Hub를 캐나다 서부(캘거리)에서 사용 가능	Security Hub를 이제 캐나다 서부(캘거리)에서 사용할 수 있습니다. 이제 특정 보안 제어를 제외한 모든 Security Hub 기능을 이 리전에서 사용할 수 있습니다. 자세한 내용은 리전별 제어 가용성을 참조하세요.	2023년 12월 20일

새 보안 제어	다음 새 Security Hub 제어를 사용할 수 있습니다. • the section called “[백업.1] AWS Backup 복구 지점은 유휴 상태에서 암호화해야 합니다.” • the section called “[DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.” • the section called “[EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.” • the section called “[EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.” • the section called “[EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.” • the section called “[FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.” • the section called “[Macie.1] Amazon Macie를 활성화해야 합니다” • the section called “[MSK.2] MSK 클러스터에는 향상된	2023년 12월 14일

모니터링이 구성되어 있어야 합니다.”

- the section called “[Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.”
- the section called “[Network Firewall.1] Network Firewall 방화벽은 여러 가용 영역에 배포해야 합니다.”
- the section called “[Network Firewall.2] Network Firewall 로깅을 활성화해야 합니다.”
- the section called “[Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.”
- the section called “[PCA.1] AWS Private CA 루트 인증 기관을 비활성화해야 합니다.”
- the section called “[S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.”
- the section called “[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.”

조사 결과 보강	Security Hub는 새 검색 결과 필드 `AwsAccountName` 및 `ApplicationName` 를 AWS 보안 검색 형식 (ASFF) 에 추가했습니다. `ApplicationArn`	2023년 11월 27일
요약 대시보드 개선 사항	이제 Security Hub 콘솔의 요약 페이지에서 더 많은 대시보드 위젯에 액세스하고, 대시보드 필터 세트를 저장하여 특정 보안 문제에 빠르게 집중하고, 대시보드 레이아웃을 사용자 지정할 수 있습니다.	2023년 11월 27일
중앙 구성	이제 중앙 구성을 사용할 수 있습니다. 중앙 구성을 통해 Security Hub 위임된 관리자는 여러 조직 계정, 조직 단위(OU) 및 리전에 걸쳐 Security Hub, 표준 및 제어를 구성할 수 있습니다.	2023년 11월 27일
관리형 정책으로 업데이트	Security Hub는 사용자 지정 가능한 보안 제어 속성을 읽고 업데이트할 수 있는 새 권한을 관리형 `AWSSecurityHubServiceRolePolicy` 정책에 추가했습니다.	2023년 11월 26일
사용자 지정 제어 파라미터	이제 일부 Security Hub 제어의 파라미터 값을 사용자 지정할 수 있습니다. 이렇게 하면 특정 제어에 대한 결과를 비즈니스 요구 사항 및 보안 기대치에 더 적합하게 만들 수 있습니다.	2023년 11월 26일

관리형 정책으로 업데이트	Security Hub는 Security Hub 기능 `AWSSecurityHubFullAccess` 및 통합을 사용할 수 있도록 허용하는 `AWSSecurityHubOrganizationsAccess` 관리형 정책 및 관리형 정책을 각각 AWS Organizations업데이트했습니다.	2023년 11월 16일

서비스 관리형 표준에 추가된 기존 보안 제어: AWS Control Tower	다음과 같은 기존 Security Hub 컨트롤이 서비스 관리형 표준에 추가되었습니다. AWS Control Tower • ACM.2 • AppSync5. • CloudTrail6. • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache3. • ElastiCache4. • ElastiCache5. • ElastiCache6. • EventBridge3. • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	2023년 11월 14일

관리형 정책으로 업데이트	Security Hub는 Security Hub가 조사 결과와 관련된 리소스 태그를 읽을 수 있도록 하는 새로운 태그 지정 권한을 `AWSSecurityHubServiceRolePolicy` 관리형 정책에 추가했습니다.	2023년 11월 7일

새 보안 제어	다음 새 Security Hub 제어를 사용할 수 있습니다. • the section called “[AppSync.5] AWS AppSync GraphQL API는 API 키로 인증해서는 안 됩니다.” • the section called “[DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.” • the section called “[DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.” • the section called “[DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.” • the section called “[DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.” • the section called “[DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.” • the section called “[DocumentDB.4] Amazon DocumentDB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch ” • the section called “[DocumentDB.5] Amazon	2023년 10월 10일

DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.”

- the section called “[ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.”
- the section called “[EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 첨부되어야 합니다.”
- the section called “[EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.”
- the section called “[MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.”
- the section called “[MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.”
- the section called “[MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다”
- the section called “[NetworkFirewall.9] Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.”
- the section called “[RDS.34] Aurora MySQL DB 클러스터

	는 감사 로그를 로그에 게시해야 합니다. CloudWatch ” • the section called “[RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.” • the section called “[Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.” • the section called “[WAF.12] AWS WAF 규칙에는 메트릭이 활성화되어 있어야 합니다. CloudWatch ”	
관리형 정책으로 업데이트	Security Hub는 Security Hub가 계정 및 조직 단위(OU) 정보를 검색할 수 있도록 하는 새로운 조직 작업을 `AWSSecurityHubServiceRolePolicy` 관리형 정책에 추가했습니다. 또한 Security Hub가 표준 및 제어를 포함한 서비스 구성을 읽고 업데이트할 수 있도록 하는 새로운 Security Hub 작업도 추가했습니다.	2023년 9월 27일

서비스 관리형 표준에 추가된 기존 보안 제어: AWS Control Tower	다음과 같은 기존 Security Hub 컨트롤이 서비스 관리형 표준에 추가되었습니다. AWS Control Tower • the section called “[Athena.1] Athena 워크그룹은 저장 시 암호화되어야 합니다” • the section called “[DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.” • the section called “[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.” • the section called “[Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.” • the section called “[Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch ” • the section called “[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.” • the section called “[Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.” • the section called “[Neptune.5] Neptune DB 클러스터에	2023년 9월 26일

	는 자동 백업이 활성화되어 있어야 합니다.” • the section called “[Neptune .6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.” • the section called “[Neptune .7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.” • the section called “[Neptune .8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.” • the section called “[RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.”	
에서 통합 제어 보기 및 통합 제어 결과를 사용할 수 있습니다. AWS GovCloud (US)	이제 AWS GovCloud (US) Region에서 통합 제어 보기 및 통합 제어 조사 결과를 사용할 수 있습니다. Security Hub 콘솔의 제어 페이지에는 표준 전체의 모든 제어가 표시됩니다. 표준 전체에서 각 제어에는 동일한 제어 ID가 있습니다. 통합 제어 조사 결과를 켜면 제어가 활성화된 여러 표준에 적용되는 경우에도 보안 검사당 단일 조사 결과를 받게 됩니다.	2023년 9월 6일

중국 리전에서 통합 제어 보기 및 통합 제어 조사 결과를 사용 가능	이제 중국 리전에서 통합 제어 보기 및 통합 제어 조사 결과를 사용할 수 있습니다. Security Hub 콘솔의 제어 페이지에는 표준 전체의 모든 제어가 표시됩니다. 표준 전체에서 각 제어에는 동일한 제어 ID가 있습니다. 통합 제어 조사 결과를 켜면 제어가 활성화된 여러 표준에 적용되는 경우에도 보안 검사당 단일 조사 결과를 받게 됩니다.	2023년 8월 28일
이스라엘(텔아비브) 리전에서 Security Hub 사용 가능	이제 이스라엘 (텔아비브)에서 Security Hub를 사용할 수 있습니다. 이제 특정 보안 제어를 제외한 모든 Security Hub 기능을 이 리전에서 사용할 수 있습니다. 자세한 정보는 리전별 제어 가용성을 참조하십시오.	2023년 8월 8일

새 보안 제어	다음 새 Security Hub 제어를 사용할 수 있습니다. • the section called “[Athena.1] Athena 워크그룹은 저장 시 암호화되어야 합니다” • the section called “[DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.” • the section called “[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.” • the section called “[Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.” • the section called “[Neptune.2] Neptune DB 클러스터는 감사 로그를 로그에 게시해야 합니다. CloudWatch ” • the section called “[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.” • the section called “[Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.” • the section called “[Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.”	2023년 7월 28일

	• the section called “[Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.” • the section called “[Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.” • the section called “[Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.” • the section called “[RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.”	
자동화 규칙 기준에 대한 새로운 연산자	이제 자동화 규칙 맵 및 문자열 기준에 CONTAINS 및 NOT_CONTAINS 비교 연산자를 사용할 수 있습니다.	2023년 7월 25일
자동화 규칙	이제 Security Hub는 사용자가 지정한 기준을 바탕으로 조사 결과를 자동으로 업데이트하는 자동화 규칙을 제공합니다.	2023년 6월 13일
새로운 타사 통합	Snyk는 Security Hub에 조사 결과를 전송하는 새로운 타사 통합입니다.	2023년 6월 12일

서비스 관리형 표준에 추가된 기존 보안 제어: AWS Control Tower	다음과 같은 기존 Security Hub 컨트롤이 서비스 관리형 표준에 추가되었습니다. AWS Control Tower • the section called “[계정.1] 다음을 위한 보안 연락처 정보를 제공해야 합니다. AWS 계정” • the section called “[APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.” • the section called “[APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.” • the section called “[CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.” • the section called “[EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.” • the section called “[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.” • the section called “[Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다” • the section called “[SageMaker.2] SageMaker	2023년 6월 12일

노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.”

- the section called “[SageMaker.3] 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.”
- the section called “[WAF.10] AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.”

새 보안 제어	다음 새 Security Hub 제어를 사용할 수 있습니다. • the section called “[ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.” • the section called “[AppSync.2] 에는 필드 수준 AWS AppSync 로깅이 활성화되어 있어야 합니다.” • the section called “[CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk는 로그를 다음으로 스트리밍해야 합니다. CloudWatch ” • the section called “[S3.17] S3 범용 버킷은 저장 시 다음을 사용하여 암호화해야 합니다. AWS KMS keys” • the section called “[StepFunctions.1] Step Functions 상태 머신은 로깅이 켜져 있어야 합니다.”	2023년 6월 6일

아시아 태평양(멜버른)에서 Security Hub 사용 가능	이제 아시아 태평양(멜버른)에서 Security Hub를 사용할 수 있습니다. 이제 특정 보안 제어를 제외한 모든 Security Hub 기능을 이 리전에서 사용할 수 있습니다. 자세한 정보는 리전별 제어 가용성을 참조하십시오.	2023년 5월 25일
결과 기록	Security Hub는 이제 지난 90일 동안의 조사 결과 기록을 추적할 수 있습니다.	2023년 5월 4일
새 보안 제어	다음 새 Security Hub 제어를 사용할 수 있습니다. • the section called “[EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.” • the section called “[ELB.16] 애플리케이션 로드 밸런서는 웹 ACL과 연결되어야 합니다. AWS WAF” • the section called “[Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다” • the section called “[S3.15] S3 범용 버킷에는 객체 잠금이 활성화되어 있어야 합니다.”	2023년 3월 29일
통합 제어 조사 결과에 대한 지원 확대	AWS v2.0.0의 자동 보안 대응은 이제 통합 제어 결과를 지원합니다.	2023년 3월 24일

Security Hub 새 버전으로 제공 AWS 리전	Security Hub는 이제 아시아 태평양(하이데라바드), 유럽(스페인) 및 유럽(취리히)에서 사용할 수 있습니다. 이러한 리전에서 사용할 수 있는 제어에는 제한이 있습니다.	2023년 3월 21일
관리형 정책으로 업데이트	Security Hub는 `AWSSecurityHubServiceRolePolicy` 관리형 정책에서 기존 권한을 업데이트했습니다.	2023년 3월 17일

NIST 800-53 표준에 대한 새 보안 제어	Security Hub는 NIST 800-53 표준에 적용할 수 있는 다음 보안 제어를 추가했습니다. • the section called “[Account.2] 는 조직의 AWS 계정 일부여야 합니다. AWS Organizations” • the section called “[CloudWatch.15] CloudWatch 경보에는 지정된 동작이 구성되어 있어야 합니다.” • the section called “[CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.” • the section called “[CloudWatch.17] CloudWatch 알람 조치를 활성화해야 합니다.” • the section called “[DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.” • the section called “[EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.” • EC2.29 – EC2 인스턴스는 VPC에서 시작되어야 합니다(사용 중지됨). • the section called “[RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.” • the section called “[S3.14] S3 범용 버킷은 버전 관리를 활성화해야 합니다.”	2023년 3월 3일

	• the section called “[WAF.11] AWS WAF 웹 ACL 로깅을 활성화해야 합니다.”	
NIST(국립 표준 기술 연구소) 800-53 버전 5	Security Hub는 이제 200개 이상의 적용 가능한 보안 제어를 사용해 NIST 800-53 버전 5 표준을 지원합니다.	2023년 2월 28일
통합 제어 보기 및 제어 조사 결과	통합 제어 보기가 릴리스됨에 따라, Security Hub 콘솔의 제어 페이지에는 표준 전체의 모든 제어가 표시됩니다. 표준 전체에서 각 제어에는 동일한 제어 ID가 있습니다. 통합 제어 조사 결과를 켜면 제어가 활성화된 여러 표준에 적용되는 경우에도 보안 검사당 단일 조사 결과를 받게 됩니다.	2023년 2월 23일

새 보안 제어	다음 새 Security Hub 제어를 사용할 수 있습니다. 일부 제어에는 리전 제한이 있습니다. • the section called “[ElastiCache.1] ElastiCache Redis 클러스터에는 자동 백업이 활성화되어 있어야 합니다.” • the section called “[ElastiCache.2] Redis 캐시 ElastiCache 클러스터의 경우 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.” • the section called “[ElastiCache.3] ElastiCache Redis의 경우 복제 그룹에 자동 장애 조치가 활성화되어 있어야 합니다.” • the section called “[ElastiCache.4] Redis 복제 그룹의 ElastiCache 경우 유휴 상태에서 그룹을 암호화해야 합니다.” • the section called “[ElastiCache.5] ElastiCache Redis의 경우 복제 그룹은 전송 중에 암호화되어야 합니다.” • the section called “[ElastiCache.6] 버전 6.0 이전의 Redis 복제 그룹의 ElastiCache 경우 Redis 인증을 사용해야 합니다.” • the section called “[ElastiCache.7] ElastiCache 클러스	2023년 2월 16일

	터는 기본 서브넷 그룹을 사용해서는 안 됩니다."	
새 ASFF 필드	Security Hub가 추가되었습니다 ProductFields. ArchivalReasons보안 ProductFields 허브가 추가되었습니다. ----sep----:0/설명 및. ArchivalReasons:0/설명 ReasonCode 및. AWS ----sep----:0/ 보안 검색 결과 형식 (ASFF) 으로	2023년 2월 8일
새 ASFF 필드	Security Hub는 규정 준수를 추가했습니다. AssociatedStandards 및 규정 준수. SecurityControlId AWS 보안 탐지 형식 (ASFF) 을 준수합니다.	2023년 1월 31일
이제 취약성 세부 정보 사용 가능	이제 Security Hub 콘솔에서 Amazon Inspector가 Security Hub로 전송하는 조사 결과에 대한 취약성 세부 정보를 볼 수 있습니다.	2023년 1월 14일
Security Hub를 중동(UAE)에서 사용할 수 있습니다	이제 Security Hub를 중동(UAE)에서 사용할 수 있습니다 일부 제어에는 리전 제한이 있습니다.	2023년 1월 12일
MetricStream과의 타사 통합 추가	Security Hub는 이제 중국을 제외한 모든 MetricStream 지역에서 타사 통합을 지원합니다 AWS GovCloud (US).	2023년 1월 11일

조직 계정 한도 확대	Security Hub는 이제 리전당 각 Security Hub 관리자에 대해 최대 11,000개의 구성원 계정을 지원합니다.	2022년 12월 27일
ElasticBeanstalk.3 롤백	Security Hub는 제어 기능을 롤백했습니다 ElasticBeanstalk.[.3] Elastic Beanstalk는 모든 지역의 FSBP 표준으로 CloudWatch 로그를 스트리밍해야 합니다.	2022년 12월 21일
Security Hub 새 보안 제어 추가	FSBP 표준을 활성화한 고객은 새 Security Hub 제어를 사용할 수 있습니다. 일부 제어에는 리전 제한이 있습니다.	2022년 12월 15일
향후 기능에 대한 지침	Security Hub는 통합 제어 보기와 통합 제어 조사 결과라는 두 가지 새로운 기능을 릴리스할 계획입니다. 곧 나올 이러한 기능은 제어 조사 결과 필드 및 값에 의존하는 기존 워크플로우에 영향을 미칠 수 있습니다.	2022년 12월 9일
이제 Amazon Security Lake 사용 가능	이제 Security Lake는 Security Hub 조사 결과를 수신하여 Security Hub와 통합되었습니다.	2022년 11월 29일
서비스 관리형 표준 지원: AWS Control Tower	Security Hub는 서비스 관리형 표준이라는 새로운 보안 표준을 지원합니다. AWS Control Tower AWS Control Tower 이 표준을 관리합니다.	2022년 11월 28일

CIS AWS 재단 벤치마크 v1.4.0을 이제 중국 지역에서 사용할 수 있습니다.	Security Hub는 이제 중국 지역에서 CIS AWS 재단 벤치마크 v1.4.0을 지원합니다.	2022년 11월 18일
이제 Jira Service Management Cloud 통합 사용 가능	Jira Service Management Cloud는 이제 중국 리전을 제외하고 사용 가능한 모든 리전에서 Security Hub 조사 결과를 수신합니다.	2022년 11월 17일
AWS IoT Device Defender 이제 통합이 가능합니다.	AWS IoT Device Defender 이제 사용 가능한 모든 지역의 Security Hub에 조사 결과를 전송합니다.	2022년 11월 17일
CIS AWS 재단 벤치마크 v1.4.0에 대한 지원	Security Hub는 이제 CIS AWS 재단 벤치마크 v1.4.0을 지원하는 보안 제어 기능을 제공합니다. 이 표준은 중국 리전을 제외한 모든 사용 가능한 리전에서 사용할 수 있습니다.	2022년 11월 9일
Security Hub 공지 사항 지원 AWS GovCloud (US)	이제 (미국 동부) AWS GovCloud 및 (미국 서부) AWS GovCloud 에서 Amazon Simple Service (Amazon SNS)를 통해 Security Hub 공지를 구독하여 Security Hub에 대한 알림을 받을 수 있습니다.	2022년 10월 3일
AWS Security Hub는 새로운 보안 제어를 추가합니다	새로운 Security Hub 컨트롤 AutoScaling.9는 FSBP 표준을 활성화한 고객이 사용할 수 있습니다. 제어에는 리전 제한이 있을 수 있습니다.	2022년 9월 1일

Security Hub 공지 구독	이제 Amazon Simple Notification Service (Amazon SNS)를 통해 Security Hub 공지를 구독하여 Security Hub에 대한 알림을 받을 수 있습니다.	2022년 8월 29일
크로스 리전 집계 활성화를 위한 리전 확장	이제 크로스 리전 집계 활성화를 조사 결과, 조사 결과 업데이트, AWS GovCloud (US)전체의 인사이트에 사용할 수 있습니다.	2022년 8월 2일
새로운 타사 제품 통합	Fortinet - FortiCNP는 Security Hub 조사 결과를 수신하는 타사 통합이며, JFrog는 조사 결과를 Security Hub로 보내는 타사 통합입니다.	2022년 7월 26일
EC2.27은 사용 중지되었습니다	Security Hub는 EC2.27을 폐기했습니다. 이전에는 FSBP (AWS 기본 보안 모범 사례) 표준의 제어 기능이었던 키 페어를 EC2 인스턴스를 실행하면 안 됩니다.	2022년 7월 20일
Lambda.2는 더 이상 python3.6을 지원하지 않습니다	Security Hub는 더 이상 python3.6을 Lambda의 파라미터로 지원하지 않습니다.2 - Lambda 함수는 기본 보안 모범 사례 (FSBP) 표준의 제어인 지원되는 런타임을 사용해야 합니다. AWS	2022년 7월 19일
AWS Security Hub 새 보안 제어 추가	FSBP 표준을 활성화한 고객은 새 Security Hub 제어를 사용할 수 있습니다. 일부 제어에는 리전 제한이 있습니다.	2022년 6월 22일

AWS Security Hub는 새 지역을 지원합니다	이제 아시아 태평양(자카르타)에서 Security Hub를 사용할 수 있습니다. 일부 제어는 이 리전에서 사용할 수 없습니다.	2022년 6월 7일
AWS Security Hub와 (과) 간의 통합 개선 AWS Config	Security Hub 사용자는 Security Hub에서 AWS Config 규칙 평가 결과를 조사 결과로 볼 수 있습니다.	2022년 6월 6일
자동 활성화 표준을 옵트아웃하는 기능 추가	를 통합한 사용자의 경우 이 기능을 통해 Security Hub 관리자 계정에 로그인하여 자동 활성화 표준에서 새 구성원 계정을 옵트아웃할 수 있습니다. AWS Organizations	2022년 4월 25일
크로스 리전 집계 활성화 확장	상태 및 보안 점수를 제어하기 위해 크로스 리전 집계 활성화를 추가했습니다.	2022년 4월 20일
CompanyName 이제는 최상위 ProductName 속성입니다.	사용자 지정 통합과 관련된 회사 및 제품 이름을 설정하기 위한 새로운 최상위 속성 추가	2022년 4월 1일
AWS 기본 보안 모범 사례 표준에 새 제어 기능 추가	AWS Foundational Security Best Practices 표준에 5가지 새 제어가 추가되었습니다.	2022년 3월 31일
ASFF에 새 리소스 세부 정보 객체 추가	ASFF에 `AwsRdsDbSecurityGroup` 리소스 유형이 추가되었습니다.	2022년 3월 25일

ASFF에 추가 리소스 세부 정보 추가	`AwsAutoScalingScalingGroup` , `AwsElbLoadBalancer` , `AwsRedshiftCluster` 및 `AwsCodeBuildProject` 에 추가 세부 정보가 추가되었습니다.	2022년 3월 25일
AWS 기본 보안 모범 사례 표준에 새로운 제어 기능 추가	AWS Foundational Security Best Practices 표준에 15가지 새 제어가 추가되었습니다.	2022년 3월 16일
AWS 기본 보안 모범 사례 표준 및 결제 카드 산업 데이터 보안 표준 (PCI DSS) 에 새로운 제어 항목 추가	Amazon OpenSearch 서비스, Amazon RDS, Amazon EC2, Elastic Load Balancing CloudFront 및 기본 보안 모범 사례 표준에 대한 AWS 새로운 제어 항목을 추가했습니다. 또한 PCI DSS에 OpenSearch 서비스를 위한 두 가지 새로운 컨트롤을 추가했습니다.	2022년 2월 15일
ASFF에 새 필드 추가	새 필드 추가: 샘플.	2022년 1월 26일
다음과 통합이 추가되었습니다. AWS Health	AWS Health service-to-service 이벤트 메시징을 사용하여 Security Hub에 결과를 전송합니다.	2022년 1월 19일
다음과 통합이 추가되었습니다. AWS Trusted Advisor	Trusted Advisor 검사 결과를 Security Hub 검색 결과로 Security Hub에 전송합니다. Security Hub는 AWS 기본 보안 모범 사례 검사 결과를 에 보냅니다. Trusted Advisor	2022년 1월 18일

ASFF에서 리소스 세부 정보 객체 업데이트	AwsAutoScalingAutoScalingGroup 에 MixedInstancesPolicy 및 AvailabilityZones 추가. AwsAutoScalingLaunchConfiguration 에 MetadataOptions 이 추가. AwsS3Bucket 에 BucketVersioningConfiguration 가 추가되었습니다.	2021년 12월 20일
ASFF 설명서의 출력 업데이트	이전에는 ASFF 속성에 대한 설명이 단일 주제에 있었습니다. 이제 각 최상위 객체와 각 리소스 세부 정보 객체가 고유한 주제에 속합니다. ASFF 구문 주제에는 해당 항목에 대한 링크가 포함되어 있습니다.	2021년 12월 20일
에 대한 새 리소스 세부 정보 개체를 ASFF에 추가했습니다. AWS Network Firewall	에 AWS Network Firewall 다음과 같은 리소스 세부 정보 개체가 추가되었습니다: AwsNetworkFirewallFirewall AwsNetworkFireFirewallPolicy , 및AwsNetworkFirewallRuleGroup .	2021년 12월 20일
새 버전의 Amazon Inspector에 대한 지원 추가	Security Hub는 새 버전의 Amazon Inspector 및 Amazon Inspector Classic과 통합되었습니다. Amazon Inspector가 조사 결과를 Security Hub로 전송합니다.	2021년 11월 29일

EC2.19의 심각도 변경	EC2.19의 심각도(보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됨)가 높음에서 심각으로 변경되었습니다.	2021년 11월 17일
Sonrai Dig과의 새로운 통합	Security Hub는 이제 Sonrai Dig과의 통합을 제공합니다. Sonrai Dig는 클라우드 환경을 모니터링하여 보안 위험을 식별합니다. Sonrai Dig은 조사사조사 결과를 Security Hub로 전송합니다.	2021년 11월 12일
CIS 2.1 및 CloudTrail .1 컨트롤에 대한 점검이 업데이트되었습니다.	CIS CloudTrail 2.1과 0.1에서는 하나 이상의 다중 지역 CloudTrail 트레일이 제자리에 있는지 확인하는 것 외에도 이제 다중 지역 CloudTrail 트레일 중 하나 이상에서 `ExcludeManagementEventSources` 매개변수가 비어 있는지 확인합니다.	2021년 11월 9일
VPC 엔드포인트에 대한 지원 추가	Security Hub는 이제 VPC AWS PrivateLink 엔드포인트와 통합되어 지원됩니다.	2021년 11월 3일
AWS 기본 보안 모범 사례 표준에 제어를 추가했습니다.	Elastic Load Balancing (ELB.2 및 ELB.8) 및 (SSM.4) 에 대한 새로운 컨트롤이 추가되었습니다. AWS Systems Manager	2021년 11월 2일

EC2.19 제어 점검에 포트 추가	또한 EC2.19는 이제 보안 그룹이 3000(Go, Node.js, 루비 웹 개발 프레임워크), 5000(Python 웹 개발 프레임워크), 8088(레거시 HTTP 포트), 8888(대체 HTTP 포트) 포트에 대한 무제한 수신 액세스를 허용하지 않는지 점검합니다.	2021년 10월 27일
Logz.io Cloud SIEM과의 통합 추가	Logz.io는 보안 팀이 보안 위협을 실시간으로 탐지, 분석 및 대응하는 데 도움을 주기 위해 로그 및 이벤트 데이터의 고급 상관 관계를 제공하는 Cloud SIEM 공급자입니다. Logz.io는 Security Hub에서 조사 결과를 받습니다.	2021년 10월 25일
조사 결과의 크로스 리전 집계 활성화를 위한 지원 추가	크로스 리전 집계 활성화를 사용하면 리전을 변경하지 않고도 모든 조사 결과를 볼 수 있습니다. 관리자 계정은 집계 리전 및 연결 리전을 선택합니다. 관리자 계정 및 해당 구성원 계정에 대한 조사 결과는 연결 리전에서 집계 리전으로 집계됩니다.	2021년 10월 20일

ASFF에서 리소스 세부 정보 객체 업데이트	`AwsCloudFrontDistribution` 에 뷰어 인증서 세부 정보가 추가되었습니다. `AwsCodeBuildProject` 에 추가 세부 정보가 추가되었습니다. `AwsElbV2LoadBalancer` 에 로드 밸런서 속성이 추가되었습니다. `AwsS3Bucket` 에 S3 버킷 소유자 계정 식별자가 추가되었습니다.	2021년 10월 8일
ASFF에 새 리소스 세부 정보 객체 추가	ASFF에 `AwsEc2VpcEndpointService` , `AwsEcrRepository` , `AwsEksCluster` , `AwsOpenSearchServiceDomain` , `AwsWafRateBasedRule` , `AwsWafRegionalRateBasedRule` , `AwsXrayEncryptionConfig` 새 리소스 세부 정보 객체 추가	2021년 10월 8일
Lambda.2 제어에서 더 이상 사용되지 않는 런타임 삭제	AWS 기본 보안 모범 사례 표준에서 [Lambda.2] Lambda 함수는 지원되는 **`dotnetcore2.1`** 런타임을 사용해야 합니다.	2021년 10월 6일
Check Point 통합에 새 이름	Check Point Dome9 Arc와의 통합은 이제 체크포인트 포스처 관리입니다. CloudGuard 통합 ARN은 변경되지 않았습니다.	2021년 10월 1일

Alcide와의 통합이 삭제	Alcide KAudit과의 통합이 중단되었습니다.	2021년 9월 30일
EC2.19의 심각도 변경	[EC2.19]의 보안 그룹의 경우 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다의 심각도는 중간에서 높음으로 변경되었습니다.	2021년 9월 30일
이제 중국 AWS Organizations 지역과의 통합이 지원됩니다.	이제 중국(베이징) 및 중국(닝샤)에서 Security Hub와 Organizations의 통합을 지원합니다.	2021년 9월 20일
S3.1 및 PCI.S3.6 컨트롤에 대한 새로운 AWS Config 규칙	S3.1 및 PCI.S3.6 모두 Amazon S3 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. 이러한 컨트롤의 AWS Config 규칙이 에서 로 변경되었습니다. `s3-account-level-public-access-blocks` `s3-account-level-public-access-blocks-periodic`	2021년 9월 14일
Lambda.2 제어에서 더 이상 사용되지 않는 런타임 삭제	AWS 기본 보안 모범 사례 표준에서 [Lambda.2] 에서 **`nodejs10.x`** 및 **`ruby2.5`** 런타임을 제거했습니다.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.	2021년 9월 13일

CIS 2.2 제어의 심각도 변경	CIS 재단 벤치마크 표준에서는 2.2의 심각도를 나타냅니다. AWS — CloudTrail 로그 파일 검증이 활성화되었는지 확인이 낮음에서 보통으로 변경되었는지 확인합니다.	2021년 9월 13일
기본 보안 모범 사례 표준의 ECS.1, Lambda.2 및 SSM.1이 업데이트되었습니다. AWS	AWS 기본 보안 모범 사례 표준에서 이제 ECS.1의 파라미터는 로 설정되어 있습니다. `SkipInactiveTaskDefinitions` `true` 이렇게 하면 제어가 활성 작업 정의만 점검할 수 있습니다. Lambda.2의 경우 런타임 목록에 Python 3.9를 추가. SSM.1은 이제 중지된 인스턴스와 실행 중인 인스턴스를 모두 점검합니다.	2021년 9월 7일
이제 PCI.Lambda.2 제어에서 Lambda @Edge 리소스가 제외됩니다.	이제 PCI DSS(지불 카드 산업 데이터 보안 표준) 표준에서는 이제 PCI.Lambda.2 제어에서 Lambda @Edge 리소스가 제외됩니다.	2021년 9월 7일
HackerOne Vulnerability Intelligence와의 통합 추가	Security Hub는 이제 HackerOne Vulnerability Intelligence와의 통합을 제공합니다. 이 통합에서 Security Hub로 조사 결과를 전송합니다.	2021년 9월 7일

ASFF에서 리소스 세부 정보 객체 업데이트	`AwsKmsKey` 에 대해 `KeyRotationStatus` 추가. `AwsS3Bucket` 에 대해 `AccessControlList` , `BucketLoggingConfiguration` , `BucketNotificationConfiguration` , `BucketWebsiteConfiguration` 추가.	2021년 9월 2일
ASFF에 새 리소스 세부 정보 객체 추가	ASFF에 `AwsAutoScalingLaunchConfiguration` , `AwsEc2VpnConnection` , `AwsEcrContainerImage` 새 리소스 세부 정보 객체가 추가되었습니다	2021년 9월 2일
ASFF에서 `Vulnerabilities` 객체에 세부 정보 추가	`Cvss`에서 `Adjustments` 및 `Source` 추가 `VulnerablePackages` 에서 파일 경로와 패키지 관리자 추가	2021년 9월 2일
Systems Manager 탐색기 및 OpsCenter 통합이 이제 중국 지역에서 지원됩니다.	Security OpsCenter Hub는 SSM Explorer와 통합되었으며 현재 중국 (베이징) 및 중국 (닝샤) 에서 지원됩니다.	2021년 8월 31일
Lambda.4 제어 사용 중지	Security Hub가 제어 [Lambda.4] Lambda 함수에는 DLQ(Dead Letter Queue)이 구성되어 있어야 합니다를 사용 중지합니다. 제어가 사용 중지되면 콘솔에 더 이상 표시되지 않으며 Security Hub는 이에 대한 점검을 수행하지 않습니다.	2021년 8월 31일

PCI.EC2.3 제어 사용 중지	Security Hub가 제어 [PCI.EC2.3] 사용하지 않는 EC2 보안 그룹은 삭제해야 합니다를 사용 중지합니다. 제어가 사용 중지되면 콘솔에 더 이상 표시되지 않으며 Security Hub는 이에 대한 점검을 수행하지 않습니다.	2021년 8월 27일
Security Hub에서 조사 결과를 사용자 지정 작업에 보내는 방식 변경	조사 결과를 사용자 지정 작업에 보내면 Security Hub는 이제 각 조사 결과를 별도의 Security Hub Findings - Custom Action 이벤트로 보냅니다.	2021년 8월 20일
사용자 지정 Lambda 런타임에 대한 새 규정 준수 상태 사유 코드 추가	새 `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` 규정 준수 상태 사유 코드 추가 이 사유 코드는 Security Hub가 사용자 지정 Lambda 런타임에 대해 점검을 수행할 수 없음을 나타냅니다.	2021년 8월 20일
AWS Firewall Manager 이제 중국 지역에서 통합이 지원됩니다.	이제 중국(베이징) 및 중국(닝샤)에서 Security Hub와 Firewall Manager의 통합을 지원합니다.	2021년 8월 19일
Caveonix Cloud 및 Forcepoint Cloud Security Gateway와의 새로운 통합	Security Hub는 이제 Caveonix Cloud 및 Forcepoint Cloud Security Gateway와의 통합을 제공합니다. 두 통합에서 Security Hub로 조사 결과를 전송합니다.	2021년 8월 10일

ASFF에 새 CompanyName , ProductName 및 Region 속성이 추가	ASFF의 최상위 레벨에 CompanyName , ProductName , 및 Region 필드 추가 이러한 필드는 자동으로 채워지며 사용자 지정 제품 통합을 제외하고 BatchImportFindings 또는 BatchUpdateFindings 를 사용하여 업데이트할 수 없습니다. 콘솔에서 조사 결과 필터는 이러한 새 필드를 사용합니다. API에서 CompanyName 및 ProductName 필터는 ProductFields 아래에 있는 속성을 사용합니다.	2021년 7월 23일
ASFF에서 리소스 세부 정보 객체 추가 및 업데이트	새 AwsRdsEventSubscription 리소스 유형 및 새 리소스 세부 정보가 추가되었습니다. AwsEcsService 리소스 유형에 대한 리소스 세부 정보가 추가되었습니다. AwsElasticsearchDomain 리소스 세부 정보 객체에 속성이 추가되었습니다.	2021년 7월 23일

AWS 기본 보안 모범 사례 표준에 제어 기능 추가	아마존 API 게이트웨이 (APIGateway.5), 아마존 EC2 (EC2.19), 아마존 ECS (ECS.2), 엘라스틱 로드 밸런싱 (ELB.7), 아마존 서비스 (ES.5~ES.8), 아마존 RDS (RDS.16~RDS.23), OpenSearch 아마존 레드시프트 (Redshift.4에 대한 새로운 제어 기능 추가), 아마존 SQS (SQS.1).	2021년 7월 20일
서비스 연결 역할 관리형 정책 내에서 권한 이동	관리형 정책 `AWSSecurityHubServiceRolePolicy` 내에서 `config:PutEvaluations` 권한을 이동함으로써, 모든 리소스에 적용됩니다.	2021년 7월 14일
AWS 기본 보안 모범 사례 표준에 제어 기능 추가	아마존 API 게이트웨이 (APIGateway.4), 아마존 (.5 및 CloudFront .6), CloudFront 아마존 EC2 CloudFront (EC2.17 및 EC2.18), 아마존 ECS (ECS.1), 아마존 서비스 (ES.4), (IAM.21), 아마존 RDS (RDS.15 OpenSearch), 아마존 S3 AWS Identity and Access Management (S3.8) 에 대한 새로운 컨트롤이 추가되었습니다.	2021년 7월 8일

제어 조사 결과에 대한 새 규정 준수 상태 사유 코드 추가	`INTERNAL_SERVICE_ERROR` 는 알 수 없는 오류가 발생했음을 나타냅니다. `SNS_TOPIC_CROSS_ACCOUNT` 는 SNS 주제를 다른 계정에서 소유하고 있음을 나타냅니다. `SNS_TOPIC_INVALID` 는 연결된 SNS 주제가 유효하지 않음을 나타냅니다.	2021년 7월 6일
와의 통합이 추가되었습니다. AWS Chatbot	와의 통합을 추가했습니다 AWS Chatbot. Security Hub는 조사 결과를 에 AWS Chatbot 전송합니다.	2021년 6월 30일
서비스 연결 역할 관리형 정책에 새 권한 추가	서비스 연결 역할이 평가 결과를 AWS Config에 제공할 수 있도록 허용하는 새 권한을 관리형 `AWSSecurityHubServiceRolePolicy` 정책에 추가했습니다.	2021년 6월 29일
ASFF에서 새로운 리소스 세부 정보 객체 추가 및 업데이트	ECS 클러스터 및 ECS 작업 정의에 대한 새 리소스 세부 정보 객체가 추가되었습니다. 연결된 네트워크 인터페이스를 나열하도록 EC2 인스턴스 객체가 업데이트되었습니다. API Gateway V2 단계에 대한 클라이언트 인증서 ID가 추가되었습니다. S3 버킷의 수명 주기 구성이 추가되었습니다.	2021년 6월 24일

집계된 제어 상태 및 표준 보안 점수 계산 업데이트	Security Hub는 이제 24시간마다 전체 제어 상태와 표준 보안 점수를 계산합니다. 관리자 계정의 경우 이제 각 계정에 대한 각 제어의 활성화 또는 비활성화 여부가 점수에 반영됩니다.	2021년 6월 23일
Security Hub 일시 중지된 계정 처리에 대한 정보 업데이트	Security Hub가 일시 중지된 계정을 처리하는 방법에 대한 정보를 AWS에 추가하였습니다.	2021년 6월 23일
개별 관리자 계정의 활성화된 컨트롤과 비활성화된 제어를 표시하는 탭 추가	관리자 계정의 경우 표준 세부 정보 페이지의 기본 탭에는 계정 전체에 대한 집계 정보가 포함됩니다. 새로 추가된 이 계정에 대해 활성화됨 및 이 계정에 대해 비활성화됨 탭에는 개별 관리자 계정에 대해 활성화되거나 비활성화된 계정이 나열됩니다.	2021년 6월 23일
`Lambda.2`에 대한 파라미터에 `java8.al2` 추가	AWS 기본 보안 모범 사례 표준에 제어를 `java8.al2` 위해 지원되는 런타임에 추가되었습니다. `Lambda.2`	2021년 6월 8일
NETSCOUT 사이버 조사관과의 MicroFocus ArcSight 새로운 통합	NETSCOUT 사이버 조사관과의 MicroFocus ArcSight 통합이 추가되었습니다. MicroFocus ArcSight Security Hub로부터 조사 결과를 받습니다. NETSCOUT Cyber Investigator는 Security Hub로 조사 결과를 보냅니다.	2021년 6월 7일

AWSSecurityHubServiceRolePolicy 에 대한 세부 정보 추가	Security Hub 서비스 연결 역할에서 사용하는 기존 관리형 정책 AWSSecurityHubServiceRolePolicy 에 대한 세부 정보를 추가하도록 관리형 정책 섹션을 업데이트했습니다.	2021년 6월 4일
Jira Service Management와의 새로운 통합	Jira용 AWS 서비스 관리 커넥터는 결과를 Jira로 보내고 이를 사용하여 Jira 이슈를 생성합니다. Jira 문제가 업데이트되면 Security Hub의 해당 조사 결과도 업데이트됩니다.	2021년 5월 26일
아시아 태평양(오사카) 리전에서 지원되는 제어 목록 업데이트	아시아 태평양 (오사카) 에서 지원되지 않는 제어 기능을 나타내도록 CIS AWS 재단 표준 및 PCI DSS (결제 카드 산업 데이터 보안 표준) 를 업데이트했습니다.	2021년 5월 21일
클라우드용 Sysdig Secure와의 새로운 통합	클라우드용 Sysdig Secure와의 통합이 추가되었습니다. 이 통합에서 Security Hub로 조사 결과를 전송합니다.	2021년 5월 14일

AWS 기본 보안 모범 사례 표준에 규제 항목을 추가했습니다.	아마존 API 게이트웨이 (APIGateway.2 및 APIGateway.3), (.4 및 CloudTrail .5) CloudTrail, 아마존 EC2 (EC2.15 및 EC2.16), (.1 AWS CloudTrail 및 .2), (람다.4), 아마존 RDS (RDS.12 — RDS.14), 아마존 레드시프트 (Redshift.7) ElasticBeanstalk 에 대한 새로운 제어 기능 추가 (.3 ElasticBeanstalk 및 .4 AWS Lambda), 그리고 (AWS Elastic Beanstalk WAF.1). AWS Secrets Manager SecretsManager SecretsManager AWS WAF	2021년 5월 10일
GuardDuty 및 Amazon RDS 컨트롤 업데이트	`GuardDuty.1` 및 `PCI.GuardDuty.1` 의 심각도를 중간에서 높음으로 변경했습니다. `RDS.8`에 `databaseEngines` 파라미터를 추가했습니다.	2021년 5월 4일
ASFF에 새 리소스 세부 정보 추가	`Resources.Details` 에서는 Amazon EC2 네트워크 ACL, Amazon EC2 서브넷 및 AWS Elastic Beanstalk 환경에 대한 새로운 리소스 세부 정보 객체가 추가되었습니다.	2021년 5월 3일
Amazon EventBridge 규칙의 필터 값을 제공하는 콘솔 필드 추가	Security Hub EventBridge 규칙의 사전 정의된 새 필터 패턴은 필터 값을 지정하는 데 사용할 수 있는 콘솔 필드를 제공합니다.	2021년 4월 30일

AWS Systems Manager Explorer와의 통합이 추가되었고 OpsCenter	Security Hub는 이제 Systems Manager 탐색기 및 와의 통합을 지원합니다 OpsCenter. 통합은 Security Hub로부터 조사 결과를 받고 Security Hub에서 이러한 조사 결과를 업데이트합니다.	2021년 4월 26일
제품 통합의 새로운 유형	새로운 통합 유형인 `UPDATE_FINDINGS_IN_SECURITY_HUB` 은 제품 통합이 Security Hub에서 받은 조사 결과를 업데이트한다는 것을 나타냅니다.	2021년 4월 22일
“마스터 계정”이 “관리자 계정”으로 변경	‘마스터 계정’이라는 용어가 ‘관리자 계정’으로 변경되었습니다. Security Hub 콘솔 및 API에서도 이 용어가 변경되었습니다.	2021년 4월 22일
HTTP를 Websocket으로 대체하도록 APIGateway.1을 업데이트	API Gateway.1의 제목, 설명 및 문제 해결을 업데이트했습니다. 이제 제어에서 HTTP API 실행 로깅 대신 Websocket API 실행 로깅에 대해 확인합니다.	2021년 4월 9일
Amazon GuardDuty 통합이 이제 베이징과 닝샤에서 지원됩니다	Security Hub GuardDuty 통합은 이제 중국 (베이징) 및 중국 (닝샤) 지역에서 지원됩니다.	2021년 4월 5일
Lambda.2 제어를 위해 지원되는 런타임에 `nodejs14.x` 추가	Foundational Security Best Practices 표준의 Lambda.2 제어가 이제 `nodejs14.x` 런타임을 지원합니다.	2021년 3월 30일

아시아 태평양(오사카)에 Security Hub가 출시	이제 아시아 태평양(오사카) 리전에서 Security Hub를 사용할 수 있습니다.	2021년 3월 29일
조사 결과 세부 정보에 조사 결과 공급자 필드 추가	조사 결과 세부 정보 패널에서 새로운 공급자 필드 찾기 섹션에는 신뢰도, 중요도, 관련 조사 결과, 심각도 및 유형에 대한 조사 결과 제공자 값이 포함되어 있습니다.	2021년 3월 24일
Amazon Macie로부터 민감한 조사 결과를 받는 옵션 추가	이제 Macie와의 통합을 구성하여 민감한 조사 결과를 Security Hub로 보낼 수 있습니다.	2021년 3월 23일
계정 관리를 위해 전환 중 AWS Organizations	구성원 계정이 있는 기존 관리자 계정을 보유한 고객의 경우 초대를 통한 계정 관리에서 Organizations를 사용하여 계정을 관리하는 것으로 변경하는 방법에 대한 새로운 정보가 추가되었습니다.	2021년 3월 22일
Amazon S3 퍼블릭 액세스 블록 구성에 대한 정보에 대해 ASFF에서 새 객체	`Resources` 에서 새 `AwsS3AccountPublicAccessBlock` 리소스 유형 및 세부 정보 객체는 계정에 대한 Amazon S3 퍼블릭 액세스 블록 구성에 대한 정보를 제공합니다. `AwsS3Bucket` 리소스 세부 정보 객체에서 `PublicAccessBlockConfiguration` 객체는 S3 버킷에 퍼블릭 액세스 블록 구성을 제공합니다.	2021년 3월 18일

특정 필드를 업데이트할 조사 결과 공급자를 찾을 수 있도록 하는 ASFF의 새로운 객체	ASFF의 새 FindingProviderFields 객체는 Confidence , Criticality , RelatedFindings , Severity, Types에 대한 값을 제공하는 BatchImportFindings 에 사용됩니다. 원래 필드는 BatchUpdateFindings 를 사용해서만 업데이트해야 합니다.	2021년 3월 18일
ASFF에서 리소스에 대한 새 DataClassification 객체	ASFF에서 새 Resources.DataClassification 객체는 리소스에서 탐지된 민감한 데이터에 대한 정보를 제공하는 데 사용됩니다.	2021년 3월 18일
사용 가능한 규정 준수 상태 코드에 CONFIG_RETURNS_NOT_APPLICABLE 값 추가	NOT_AVAILABLE 규정 준수 상태의 경우 사유 코드 RESOURCE_NO_LONGER_EXISTS 를 삭제하고 사유 코드 CONFIG_RETURNS_NOT_APPLICABLE 를 추가했습니다.	2021년 3월 16일
통합을 위한 새로운 관리형 정책 AWS Organizations	새로운 관리형 정책 AWSSecurityHubOrganizationsAccess 은 조직 관리 계정과 위임된 Security Hub 관리자 계정에 필요한 Organizations 권한을 제공합니다.	2021년 3월 15일

관리형 정책 및 서비스 연결 역할 정보가 보안 장으로 이동	관리형 정책에 대한 정보가 개정 및 확장되었습니다. 관리형 정책 정보와 서비스 연결 역할에 대한 정보가 모두 보안 장으로 이동했습니다.	2021년 3월 15일
SecureCloudDB와의 새로운 통합	타사 통합 목록에 SecureCloud DB를 추가했습니다. SecureCloudDB는 내부 및 외부 보안 태세와 활동에 대한 포괄적인 가시성을 제공하는 클라우드 네이티브 데이터베이스 보안 도구입니다. SecureCloudDB는 조사 결과를 Security Hub에 전송합니다.	2021년 3월 4일
CIS 1.1 및 CIS 3.1 - CIS 3.14 제어에 대한 심각도 수정	CIS 1.1 및 CIS 3.1 - CIS 3.14 제어의 심각도가 낮음으로 변경되었습니다.	2021년 3월 3일
RDS.11 제어 삭제	Foundational Security Best Practices 표준에서 RDS.11 제어를 삭제했습니다.	2021년 3월 3일
Turbot에 대한 통합 업데이트	Turbot 통합이 조사 결과를 보내고 받을 수 있도록 업데이트되었습니다.	2021년 2월 26일

Foundational Security Best Practices 표준에 제어 추가	아마존 API 게이트웨이 (API Gateway.1), 아마존 EC2 (EC2.9 및 EC2.10), 아마존 엘라스틱 파일 시스템 (EFS.2), 아마존 서비스 (ES.2 및 ES.3), 엘라스틱 로드 밸런싱 (ELB.6), OpenSearch (KMS.3) 에 대한 새로운 컨트롤이 추가되었습니다. AWS Key Management Service AWS KMS	2021년 2월 11일
`DescribeProducts` API에 선택적 `ProductArn` 필터 추가	이제 `DescribeProducts` API 작업에 선택적 `ProductArn` 파라미터가 포함됩니다. `ProductArn` 파라미터는 세부 정보를 반환할 특정 제품 통합을 식별하는 데 사용됩니다.	2021년 2월 3일
Cloud Storage Security의 Amazon S3용 안티바이러스와의 새로운 통합	Amazon S3용 안티바이러스와의 통합은 바이러스 스캔 결과를 조사 결과로 Security Hub에 보냅니다.	2021년 1월 27일
관리자 계정의 보안 점수 계산 프로세스를 업데이트했습니다.	관리자 계정의 경우 Security Hub는 별도의 프로세스를 사용하여 보안 점수를 계산합니다. 새 프로세스를 통해 구성원 계정에는 활성화되지만 관리자 계정에서는 비활성화된 컨트롤이 점수에 포함되도록 합니다.	2021년 1월 21일

ASFF의 새 필드 및 객체	리소스에 대해 발생한 작업을 추적하는 새 `Action` 객체를 추가했습니다. DNS 이름과 IP 주소를 추적하는 필드를 `AwsEc2NetworkInterface` 객체에 추가했습니다. 리소스 세부 정보에 새 `AwsSsmPatchCompliance` 속성을 추가했습니다.	2021년 1월 21일
Foundational Security Best Practices 표준에 제어 추가	아마존 (CloudFront.1~.4), 아마존 다이나모DB CloudFront (CloudFrontDynamoDB.1 ~ DynamoDB.3), Elastic Load Balancing (ELB.3 ~ ELB.5), 아마존 RDS (RDS.9 ~ RDS.11), 아마존 레드시프트 (Redshift.1 ~ Redshift.3 및 Redshift.6), 아마존에 대한 새로운 컨트롤이 추가되었습니다. SNS (SNS.1).	2021년 1월 15일
워크플로우 상태는 기록 상태 또는 규정 준수 상태에 따라 재설정됩니다	Security Hub는 보관된 조사 결과가 활성화되거나 조사 결과의 규정 준수 상태가 `PASSED`에서 `FAILED`, `WARNING` 또는 `NOT_AVAILABLE` 중 하나로 변경되는 경우 워크플로우 상태를 `NOTIFIED` 또는 `RESOLVED`에서 `NEW`으로 자동으로 재설정합니다. 이러한 변경은 추가 조사가 필요함을 나타냅니다.	2021년 1월 7일

제어 기반 조사 결과에 `ProductFields` 정보 추가	제어에서 생성된 조사 결과의 경우 AWS 보안 조사 결과 형식(ASFF)의 `ProductFields` 객체의 콘텐츠에 대한 정보를 추가했습니다.	2020년 12월 29일
관리형 인사이트 업데이트	인사이트 5의 제목 변경. 의심스러운 활동이 있는 IAM 사용자를 점검하는 새 인사이트 32가 추가되었습니다.	2020년 12월 22일
IAM.7 및 Lambda.1 제어에 대한 업데이트	AWS 기본 보안 모범 사례 표준에서 IAM.7의 매개변수를 업데이트했습니다. Lambda.1의 제목과 설명을 업데이트했습니다.	2020년 12월 22일
ServiceNow ITSM과의 통합 확대	ServiceNow ITSM 통합을 통해 사용자는 Security Hub 검색 결과 수신 시 자동으로 인시던트 또는 문제를 생성할 수 있습니다. 이러한 인시던트 또는 문제가 업데이트되면 Security Hub의 조사 결과도 업데이트됩니다.	2020년 12월 11일
AWS Audit Manager와의 새로운 통합	Security Hub는 이제 AWS 감사 관리자와의 통합을 제공합니다. 통합을 통해 Audit Manager는 Security Hub로부터 제어 기반 조사 결과를 받을 수 있습니다.	2020년 12월 8일

Aqua Security Kube-bench와의 새로운 통합	Security Hub는 Aqua Security Kube-bench와의 통합 추가했습니다. 이 통합에서 Security Hub로 조사 결과를 전송합니다.	2020년 11월 24일
이제 중국 리전에서 Cloud Custodian을 사용할 수 있습니다	이제 중국(베이징) 및 중국(닝샤) 리전에서 Cloud Custodian과의 통합을 사용할 수 있습니다.	2020년 11월 24일
`BatchImportFindings` 는 이제 추가 필드를 업데이트하는 데 사용할 수 있습니다	이전에는, `Confidence` , `Criticality` , `RelatedFindings` , `Severity`, `Types` 필드를 업데이트하는 데 `BatchImportFindings` 을 사용할 수 없었습니다. 이제 이러한 필드를 `BatchUpdateFindings` 에 의해 업데이트하지 않은 경우 `BatchImportFindings` 로 업데이트할 수 있습니다. `BatchUpdateFindings` 에 의해 업데이트된 후에는 `BatchImportFindings` 로 업데이트할 수 없습니다.	2020년 11월 24일
Security Hub는 이제 다음과 통합되었습니다. AWS Organizations	이제 고객은 Organizations 계정 구성을 사용하여 구성원 계정을 관리할 수 있습니다. 조직 관리 계정은 Security Hub 관리자 계정으로 지정하고, 이 계정이 Security Hub에서 활성화할 조직 계정을 결정합니다. 조직의 일부가 아닌 계정에도 수동 초대 프로세스를 계속 사용할 수 있습니다.	2020년 11월 23일

대용량 제어에 대한 별도의 조사 결과 목록 형식 삭제.	조사 결과가 매우 많으면 제어의 조사 결과 목록에서 더 이상 조사 결과 페이지 형식을 사용하지 않습니다.	2020년 11월 19일
신규 및 업데이트된 타사 통합	Security Hub는 이제 cloudtamer.io, 3CoreSec, Prowler 및 쿠버네티스 시큐리티와의 통합을 지원합니다. StackRox IBM QRadar는 더 이상 조사 결과를 전송하지 않습니다. 이는 조사 결과를 수신만 합니다.	2020년 10월 30일
제어 세부 정보 페이지에서 조사 결과를 다운로드하는 옵션이 추가되었습니다.	제어 세부 정보 페이지에서 새 다운로드 옵션을 사용하여 조사 결과 목록을 .csv 파일로 다운로드할 수 있습니다. 다운로드한 목록은 목록에 있는 모든 필터를 따릅니다. 특정 조사 결과를 선택한 경우 다운로드한 목록에는 해당 조사 결과만 포함됩니다.	2020년 10월 26일
표준 세부 정보 페이지에서 제어 목록을 다운로드하는 옵션이 추가되었습니다.	표준 세부 정보 페이지에서 새 다운로드 옵션을 사용하여 제어 목록을 .csv 파일로 다운로드할 수 있습니다. 다운로드한 목록은 목록에 있는 모든 필터를 따릅니다. 특정 제어를 선택한 경우 다운로드한 목록에는 해당 제어만 포함됩니다.	2020년 10월 26일

신규 및 업데이트된 파트너 통합	Security Hub는 이제 와 ThreatModeler 통합되었습니다. 새 제품 이름을 반영하도록 다음 파트너 통합을 업데이트했습니다. Twistlock Enterprise Edition은 이제 Palo Alto Networks - Prisma Cloud Compute입니다. 또한 Palo Alto Networks에서 Demisto는 이제 Cortex XSOAR이고 Redlock은 이제 Prisma Cloud Enterprise입니다.	2020년 10월 23일
Security Hub가 중국(베이징) 및 중국(닝샤)에서 출시	이제 중국(베이징) 및 중국(닝샤) 리전에서 Security Hub를 사용할 수 있습니다.	2020년 10월 21일
ASFF 속성 및 타사 통합에 대한 형식 수정	ASFF 속성 및 파트너 통합 목록은 이제 표 대신 목록 기반 형식을 사용합니다. ASFF 구문, 속성 및 유형 분류는 이제 별도의 주제에 있습니다.	2020년 10월 15일
새롭게 디자인된 표준 세부 정보 페이지	활성화된 표준에 대한 표준 세부 정보 페이지에 이제 제어 탭 목록이 표시됩니다. 탭은 제어 상태를 기반으로 제어 목록을 필터링합니다.	2020년 10월 7일
CloudWatch 이벤트를 다음으로 대체했습니다. EventBridge	아마존 CloudWatch 이벤트에 대한 참조를 Amazon으로 EventBridge 대체했습니다.	2020년 10월 1일

Blue Hexagon AWS, Alcide KAudit 및 팔로 알토 네트웍스 VM 시리즈와 새롭게 통합되었습니다.	Security Hub는 이제 Alcide KAudit 및 팔로 알토 AWS네트웍스 VM 시리즈용 블루 헥사곤과 통합되었습니다. 파란색 육각형 AWS 창과 KAudit는 조사 결과를 Security Hub로 보냅니다. VM-Series가 Security Hub에서 조사 결과를 받습니다.	2020년 9월 30일
ASFF에서 새로운 리소스 세부 정보 객체 추가 및 업데이트	`AwsApiGatewayRestApi` , `AwsApiGatewayStage` , `AwsApiGatewayV2Api` , `AwsApiGatewayV2Stage` , `AwsCertificateManagerCertificate` , `AwsElbLoadBalancer` , `AwsIamGroup` , `AwsRedshiftCluster` 에 대한 새 `Resources.Details` 객체를 추가하였습니다. `AwsCloudFrontDistribution` , `AwsIamRole` 및 `AwsIamAccessKey` 객체에 세부 정보가 추가되었습니다.	2020년 9월 30일
리소스가 행위자인지 대상인지 추적하기 위한 ASFF의 리소스에 대한 새 `ResourceRole` 속성.	리소스에 대한 `ResourceRole` 속성은 리소스가 조사 결과 활동의 대상인지 또는 조사 결과 활동의 가해자인지를 나타냅니다. 유효 값은 `ACTOR`와 `TARGET`입니다.	2020년 9월 30일

사용 가능한 서비스 통합에 AWS Systems Manager 패치 관리자를 추가했습니다. AWS	AWS Systems Manager 패치 관리자는 이제 Security Hub와 통합되었습니다. Patch Manager는 고객의 플릿에 있는 인스턴스가 패치 규정 준수 표준을 위반하는 경우 Security Hub에 조사 결과를 보냅니다.	2020년 9월 22일
AWS 기본 보안 모범 사례 표준에 새로운 컨트롤이 추가되었습니다.	아마존 EC2 (EC2.7 및 EC2.8), 아마존 EMR (EMR.1), IAM (IAM.8), 아마존 RDS (RDS.4 ~ RDS.8), 아마존 S3 (S3.6), (.1 및 .2) 서비스에 대한 새로운 컨트롤이 추가되었습니다. AWS Secrets Manager SecretsManager SecretsManager SecretsManager	2020년 9월 15일
BatchUpdateFindings 필드에 대한 액세스를 제어하는 IAM 정책에 대한 새로운 컨텍스트 키	이제 BatchUpdateFindings 사용 시 필드 및 필드 값에 대한 액세스를 제한하도록 IAM 정책을 구성할 수 있습니다.	2020년 9월 10일
구성원 계정에 대한 BatchUpdateFindings 의 액세스 확대	이제 기본적으로 BatchUpdateFindings 멤버 계정은 관리자 계정과 동일한 액세스 권한을 가집니다.	2020년 9월 10일
기본 보안 모범 사례 AWS KMS 표준의 새로운 제어	Foundational Security Best Practices 표준에 두 가지 새로운 제어(KMS.1 및 KMS.2)를 추가했습니다. 새 컨트롤은 IAM 정책이 암호 해독 작업에 대한 액세스를 AWS KMS 제한하는지 여부를 확인합니다.	2020년 9월 9일

제어에 대한 계정 수준의 조사 결과 삭제	Security Hub는 더 이상 제어에 대한 계정 수준의 조사 결과를 생성하지 않습니다. 리소스 수준 조사 결과만 생성됩니다.	2020년 9월 1일
ASFF에서 새 PatchSummary 객체	`PatchSummary` 객체를 ASFF에 추가했습니다. `PatchSummary` 객체는 선택한 규정 준수 표준과 관련된 리소스의 패치 규정 준수에 대한 정보를 제공합니다.	2020년 9월 1일
새롭게 디자인된 제어 세부 정보 페이지	제어의 세부 정보 페이지가 새롭게 디자인되었습니다. 제어 조사 결과 목록은 규정 준수 상태를 기반으로 목록을 빠르게 필터링할 수 있는 탭을 제공합니다. 또한 숨겨진 조사 결과를 빠르게 확인할 수 있습니다. 각 항목은 검색 리소스, AWS Config 규칙 및 검색 기록에 대한 추가 세부 정보에 대한 액세스를 제공합니다.	2020년 8월 28일
조사 결과에 대한 새 필터 옵션	조사 결과 필터의 경우 is not 필터를 사용하여 필드 값이 필터 값과 같지 않은 조사 결과를 찾을 수 있습니다. does not start with를 사용하여 필드 값이 지정된 필터 값으로 시작하지 않는 조사 결과를 찾을 수 있습니다.	2020년 8월 28일

ASFF에서 새로운 리소스 세부 정보 객체	`AwsDynamoDbTable` , `AwsEc2Eip` , `AwsIamPolicy` , `AwsIamUser` , `AwsRdsDbCluster` , `AwsRdsDbClusterSnapshot` , `AwsRdsDbSnapshot` , `AwsSecretsManagerSecret` 리소스 유형에 대해 새 `Resources.Details` 객체 추가	2020년 8월 18일
RSA Archer와의 새로운 통합	이제 Security Hub는 RSA Archer와 통합되었습니다. RSA Archer가 Security Hub에서 조사 결과를 받습니다.	2020년 8월 18일
에 대한 새 설명 필드 AwsKmsKey	`Resources.Details` 에 있는 `AwsKmsKey` 객체에 `Description` 필드를 추가했습니다.	2020년 8월 18일
에 필드 추가 AwsRdsDbInstance	`Resources.Details` 에 있는 `AwsRdsDbInstance` 객체에 몇 가지 속성을 추가했습니다.	2020년 8월 18일
Security Hub에서 제어의 전체 상태를 결정하는 방법 업데이트	조사 결과가 없는 제어의 경우 상태는 알 수 없음 대신 데이터 없음입니다. 제어 상태에는 계정 수준 및 리소스 수준 조사 결과가 모두 포함됩니다. 제어 상태는 숨겨진 조사 결과를 무시하는 경우를 제외하고는 조사 결과의 워크플로우 상태를 사용하지 않습니다.	2020년 8월 13일

Security Hub에서 표준에 대한 보안 점수를 계산하는 방식 업데이트	이제 Security Hub에서 표준에 대한 보안 점수를 계산할 때 데이터 없음 상태인 제어를 무시합니다. 보안 점수는 데이터가 없는 제어를 제외하고, 통과된 제어와 활성화된 제어의 비율입니다.	2020년 8월 13일
활성화된 표준에서 새 제어를 자동으로 활성화하는 새로운 옵션	활성화된 표준에서 새 제어를 자동으로 활성화하는 설정 옵션이 추가되었습니다. `UpdateSecurityHubConfiguration` API 작업을 사용하여 이 옵션을 구성할 수도 있습니다.	2020년 7월 31일
PCI DSS(지불 카드 산업 데이터 보안 표준)에 대한 새 컨트롤	PCI DSS 표준에 새 제어를 추가했습니다. 새 컨트롤의 식별자는 PCI.DMS.1, PCI.EC2.5, PCI.EC2.6, PCI.ELBV2.1, PCI입니다. GuardDuty 1., PCI.IAM.7, PCI.IAM.8, PCI.S3.5, PCI.S3.6, PCI.SageMaker1., PCI.SSM.2, PCI.SSM.3.	2020년 7월 29일
Foundational Security Best Practices 표준에 대한 새로운 및 업데이트된 제어	Foundational Security Best Practices 표준에 새 제어 추가 새 컨트롤의 식별자는 .1, DMS.1, EC2.4, EC2.6, S3.5 및 SSM.3입니다 AutoScaling. ACM.1의 제목을 업데이트하고 `daysToExpiration` 파라미터 값을 30으로 변경했습니다.	2020년 7월 29일

ASFF에서 새 Vulnerabilities 객체	조사 결과와 관련된 취약성에 대한 정보를 제공하는 Vulnerabilities 객체가 추가되었습니다.	2020년 7월 1일
Auto Scaling 그룹, EC2 볼륨 및 EC2 VPC에 대한 ASFF의 새 Resource.Details 객체	Resource.Details 에 AwsAutoScalingAutoScalingGroup , AWSEc2Volume 및 AwsEc2Vpc 객체가 추가되었습니다.	2020년 7월 1일
ASFF에서 새 NetworkPath 객체	조사 결과와 관련된 네트워크 경로에 대한 정보를 제공하는 NetworkPath 객체가 추가되었습니다.	2020년 7월 1일
Compliance.Status 이 PASSED인 경우 조사 결과를 자동으로 해결합니다	제어의 조사 결과(있는 경우)의 경우 Compliance.Status 가 PASSED인 경우 Security Hub는 자동으로 Workflow.Status 를 RESOLVED로 설정합니다.	2020년 6월 24일
AWS Command Line Interface 예제	여러 Security Hub 작업에 대한 AWS CLI 구문 및 예제가 추가되었습니다. Security Hub 활성화, 인사이트 관리, 표준 및 제어 관리, 제품 통합 관리, Security Hub 비활성화가 포함됩니다.	2020년 6월 24일
ASFF의 새로운 Severity.Original 속성	결과 공급자의 원래 심각도인 Severity.Original 속성을 추가했습니다. 이는 더 이상 사용되지 않는 Severity.Product 속성을 대체합니다.	2020년 5월 20일

컨트롤 상태에 대한 세부 정보를 제공하는 ASFF의 새로운 Compliance.StatusReasons 객체	제어의 현재 상태에 대한 추가 컨텍스트를 제공하는 Compliance.StatusReasons 객체를 추가했습니다.	2020년 5월 20일
새로운 AWS 기본 보안 모범 사례 표준	배포된 계정과 리소스가 보안 모범 사례에서 벗어나는 경우 이를 탐지하는 제어 집합인 새로운 AWS 기본 보안 모범 사례 표준이 추가되었습니다.	2020년 4월 22일
결과에 대한 워크플로우 상태를 업데이트하는 새로운 콘솔 옵션	Security Hub 콘솔 또는 API를 사용하여 조사 결과의 워크플로우 상태를 설정하는 데 필요한 정보가 추가되었습니다.	2020년 4월 16일
조사 결과에 대한 고객 업데이트를 위한 새로운 BatchUpdateFindings API	결과 조사 프로세스와 관련된 정보를 업데이트하기 위해 BatchUpdateFindings 를 사용하는 방법에 대한 정보가 추가되었습니다. BatchUpdateFindings 가 UpdateFindings 로 대체되며, 이는 더 이상 사용되지 않습니다.	2020년 4월 16일

AWS 보안 탐지 형식 (ASFF) 업데이트	여러 가지 새로운 리소스 유형이 추가되었습니다. `Severity` 객체에 새 `Label` 속성이 추가되었습니다. `Label`은 `Normalized` 필드를 대체하기 위한 것입니다. 결과 조사 과정을 추적하기 위해 새로운 `Workflow` 객체가 추가되었습니다. `Workflow`에는 기존 `Workflowstate` 속성을 대체하는 `Status` 속성이 포함되어 있습니다.	2020년 3월 12일
통합 페이지에 대한 업데이트	통합 페이지에 변경 사항을 반영하도록 업데이트되었습니다. 이제 각 통합에 대해 페이지에 통합 범주가 표시되고 각 통합에서 Security Hub의 조사 결과를 보내는지 또는 수신하는지 여부가 표시됩니다. 또한 각 통합을 활성화하는 데 필요한 특정 단계를 제공합니다.	2020년 2월 26일
새로운 타사 제품 통합	클라우드 커스토디안, FireEye 헬릭스, 포스포인트 CASB, 포스포인트 DLP, 포스포인트 NGFW, 랙스페이스 클라우드 네이티브 시큐리티, Vectra.ai Cognito Detect와 같은 신제품 통합이 추가되었습니다.	2020년 2월 21일

PCI DSS(지불 카드 산업 데이터 보안 표준)에 대한 새로운 보안 표준	PCI DSS(지불 카드 산업 데이터 보안 표준)에 대한 Security Hub 보안 표준이 추가되었습니다. 이 표준이 활성화되면 Security Hub는 PCI DSS 요구 사항과 관련된 제어에 대해 자동화된 점검을 수행합니다.	2020년 2월 13일
보안 탐지 형식 (ASFF) 업데이트 AWS	표준 제어의 관련 요구 사항에 대한 필드가 추가되었습니다. 새 리소스 유형 및 새 리소스 세부 정보가 추가되었습니다. 또한 ASFF를 사용하면 이제 최대 32개의 리소스를 제공할 수 있습니다.	2020년 2월 5일
개별 보안 표준 제어를 비활성화하는 새로운 옵션	각 개별 보안 표준 제어가 활성화되는지 여부를 제어하는 방법에 대한 정보가 추가되었습니다.	2020년 1월 15일
용어 및 개념 업데이트	용어 및 개념에 일부 설명이 업데이트되었고 새로운 용어가 추가되었습니다.	2019년 9월 21일
AWS Security Hub 일반 공급 릴리스	미리 보기 기간 동안 Security Hub의 개선 사항을 반영하여 콘텐츠를 업데이트합니다.	2019년 6월 25일
CIS AWS 재단 검사에 대한 수정 단계가 추가되었습니다.	Security Hub에서 AWS 지원되는 보안 표준에 수정 단계를 추가했습니다.	2019년 4월 15일
AWS Security Hub의 프리뷰 릴리즈	AWS Security Hub 사용 설명서의 미리 보기 릴리스 버전을 게시했습니다.	2018년 11월 18일

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