구현 안내서

AWS의 자동 보안 응답

AWS의 자동 보안 응답: 구현 안내서

Table of Contents

AWS Security Hub에서 사전 정의된 대응 및 문제 해결 작업을 사용하여 보안 위협 자동 해결

이 구현 가이드는 AWS의 자동 보안 대응 솔루션, 참조 아키텍처 및 구성 요소, 배포 계획 고려 사항, AWS의 자동 보안 대응 솔루션을 Amazon Web Services(AWS) 클라우드에 배포하기 위한 구성 단계에 대한 개요를 제공합니다.

이 탐색 테이블을 사용하여 다음 질문에 대한 답을 빠르게 찾을 수 있습니다.

다음을 수행하려는 경우 . . .	읽기 . . .
이 솔루션 실행 비용 파악	비용
이 솔루션의 보안 고려 사항 이해	보안
이 솔루션의 할당량을 계획하는 방법 알아보기	할당량
이 솔루션에서 지원되는 AWS 리전 파악	지원되는 AWS 리전
이 솔루션에 포함된 AWS CloudFormation 템플릿을 보거나 다운로드하여이 솔루션의 인프라 리소스(“스택”)를 자동으로 배포합니다.	AWS CloudFormation 템플릿
소스 코드에 액세스하고 선택적으로 AWS 클라우드 개발 키트(AWS CDK)를 사용하여 솔루션을 배포합니다.	GitHub 리포지토리

보안이 지속적으로 발전하려면 데이터를 보호하기 위한 사전 예방 단계가 필요하므로 보안 팀이 대응하기 어렵고 비용이 많이 들고 시간이 많이 걸릴 수 있습니다. AWS의 자동 보안 대응 솔루션은 업계 규정 준수 표준 및 모범 사례를 기반으로 사전 정의된 대응 및 문제 해결 조치를 제공하여 보안 문제를 신속하게 해결하는 데 도움이 됩니다.

AWS의 자동 보안 대응은 AWS Security Hub와 협력하여 보안을 개선하고 워크로드를 Well-Architected Security 원칙 모범 사례(SEC10)에 맞게 조정하는 데 도움이 되는 AWS 솔루션입니다.SEC10 이 솔루션을 사용하면 AWS Security Hub 고객이 일반적인 보안 조사 결과를 더 쉽게 해결하고 AWS에서 보안 태세를 개선할 수 있습니다.

Security Hub 기본 계정에 배포할 특정 플레이북을 선택할 수 있습니다. 각 플레이북에는 단일 AWS 계정 내에서 또는 여러 계정에서 문제 해결 워크플로를 시작하는 데 필요한 사용자 지정 작업, Identity and Access Management(IAM) 역할, Amazon EventBridge 규칙, AWS AWS Systems Manager 자동화 문서, AWS AWS Lambda 함수 및 AWS Step Functions가 포함되어 있습니다. 해결은 AWS Security Hub의 작업 메뉴에서 작동하며 권한 있는 사용자가 단일 작업으로 모든 AWS Security Hub 관리 계정에서 결과를 해결할 수 있습니다. 예를 들어, AWS 리소스 보안을 위한 규정 준수 표준인 CIS(인터넷 보안 센터) AWS Foundations Benchmark의 권장 사항을 적용하여 암호가 90일 이내에 만료되도록 하고 AWS에 저장된 이벤트 로그의 암호화를 적용할 수 있습니다.

> **Note**
>
> 해결은 즉각적인 조치가 필요한 긴급 상황을 위한 것입니다. 이 솔루션은 AWS Security Hub Management 콘솔을 통해 사용자가 시작한 경우 또는 특정 제어에 대해 Amazon EventBridge 규칙을 사용하여 자동 문제 해결이 활성화된 경우에만 결과 해결을 변경합니다. 이러한 변경 사항을 되돌리려면 리소스를 수동으로 원래 상태로 되돌려야 합니다.
> CloudFormation 스택의 일부로 배포된 AWS 리소스를 수정할 때는 이로 인해 드리프트가 발생할 수 있습니다. 가능하면 스택 리소스를 정의하는 코드를 수정하고 스택을 업데이트하여 스택 리소스를 수정합니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 드리프트란 무엇입니까?를 참조하세요.

AWS의 자동 보안 대응에는 다음과 같이 정의된 보안 표준에 대한 플레이북 수정 사항이 포함됩니다.

- 인터넷 보안 센터(CIS) AWS 파운데이션 벤치마크 v1.2.0
- CIS AWS 파운데이션 벤치마크 v1.4.0
- CIS AWS 파운데이션 벤치마크 v3.0.0
- AWS 기본 보안 모범 사례(FSBP) v.1.0.0
- Payment Card Industry Data Security Standard(PCI-DSS) v3.2.1
- 미국 국립 표준 기술 연구소(NIST) SP 800-53 개정 5

이 솔루션에는 AWS Security Hub의 통합 제어 조사 결과 기능을 위한 보안 제어(SC) 플레이북도 포함되어 있습니다. 자세한 내용은 플레이북을 참조하세요.

이 구현 가이드에서는 AWS 클라우드에서 AWS의 자동 보안 대응 솔루션을 배포하기 위한 아키텍처 고려 사항 및 구성 단계에 대해 설명합니다. 여기에는 보안 및 가용성에 대한 AWS 모범 사례를 사용하여 AWS에서이 솔루션을 배포하는 데 필요한 AWS 컴퓨팅, 네트워크, 스토리지 및 기타 서비스를 시작, 구성 및 실행하는 AWS CloudFormation 템플릿에 대한 링크가 포함되어 있습니다.

이 가이드는 AWS 클라우드에서 설계한 실제 경험이 있는 IT 인프라 아키텍트, 관리자 및 DevOps 전문가를 대상으로 합니다.

기능 및 이점

AWS의 자동 보안 응답은 다음과 같은 기능을 제공합니다.

특정 컨트롤에 대한 조사 결과 자동 수정

제어에 대한 Amazon EventBridge 규칙을 활성화하여 AWS Security Hub에 표시된 즉시 해당 제어에 대한 조사 결과를 자동으로 수정합니다.

한 위치에서 여러 계정 및 리전의 문제 해결 관리

조직의 계정 및 리전의 집계 대상으로 구성된 AWS Security Hub 관리자 계정에서 솔루션이 배포된 모든 계정 및 리전의 결과에 대한 문제 해결을 시작합니다.

문제 해결 작업 및 결과에 대한 알림 받기

솔루션에서 배포한 Amazon SNS 주제를 구독하여 문제 해결이 시작될 때 알림을 받고 문제 해결이 성공했는지 여부를 확인합니다.

Jira 또는 ServiceNow와 같은 티켓 시스템과 통합

조직이 문제 해결(예: 인프라 코드 업데이트)에 대응할 수 있도록이 솔루션은 티켓을 외부 티켓팅 시스템으로 푸시할 수 있습니다.

GovCloud 및 중국 파티션에서 AWSConfigRemediations 사용

솔루션에 포함된 문제 해결 방법 중 일부는 상용 파티션에서 사용할 수 있지만 GovCloud 또는 중국에서는 사용할 수 없는 AWS 소유 AWSConfigRemediation 문서의 재패키지입니다. 이러한 문서를 파티션에서 사용하려면이 솔루션을 배포합니다.

사용자 지정 문제 해결 및 플레이북 구현으로 솔루션 확장

이 솔루션은 확장 가능하고 사용자 지정할 수 있도록 설계되었습니다. 대체 문제 해결 구현을 지정하려면 사용자 지정된 AWS Systems Manager 자동화 문서와 AWS IAM 역할을 배포합니다. 솔루션에서 구현하지 않은 전체 새 제어 세트를 지원하려면 사용자 지정 플레이북을 배포합니다.

사용 사례

조직의 계정 및 리전에서 표준에 대한 규정 준수 적용

제공된 수정 사항을 사용할 수 있도록 표준용 플레이북(예: AWS 기본 보안 모범 사례)을 배포합니다. 솔루션을 배포한 모든 계정 및 리전의 리소스에 대한 문제 해결을 자동으로 또는 수동으로 시작하여 규정을 준수하지 않는 리소스를 수정합니다.

조직의 규정 준수 요구 사항에 맞게 사용자 지정 문제 해결 또는 플레이북 배포

제공된 Orchestrator 구성 요소를 프레임워크로 사용합니다. 조직의 특정 요구 사항에 따라 out-of-compliance 리소스를 해결하기 위한 사용자 지정 문제 해결을 구축합니다.

개념 및 정의

이 섹션에서는 이 솔루션과 관련된 핵심 개념 및 용어에 대해 설명합니다.

문제 해결, 문제 해결 실행서

결과를 해결하는 단계 세트의 구현입니다. 예를 들어, 제어 보안 제어(SC) Lambda.1 "Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다"를 수정하면 퍼블릭 액세스를 허용하는 문을 제거하도록 관련 AWS Lambda 함수의 정책이 수정됩니다.

런북 제어

Orchestrator가 특정 제어에 대해 시작된 문제 해결을 올바른 문제 해결 실행서로 라우팅하는 데 사용하는 AWS Systems Manager(SSM) 자동화 문서 세트 중 하나입니다. 예를 들어 SC Lambda.1 및 AWS Foundational Security Best Practices(FSBP) Lambda.1에 대한 수정 사항은 동일한 수정 실행서로 구현됩니다. 오케스트레이터는 각 컨트롤에 대한 컨트롤 런북을 호출합니다. 컨트롤 런북의 이름은 각각 ASR-AFSBP_Lambda.1 및 ASR-SC_2.0.0_Lambda.1입니다. 각 컨트롤 런북은 동일한 문제 해결 런북을 호출합니다.이 경우 ASR-RemoveLambdaPublicAccess가 됩니다.

오케스트레이터

AWS Security Hub에서 결과 객체를 입력하고 대상 계정 및 리전에서 올바른 컨트롤 런북을 호출하는 솔루션에서 배포한 Step Functions입니다. 또한 Orchestrator는 문제 해결이 시작될 때와 문제 해결이 성공 또는 실패할 때 솔루션 SNS 주제에 알립니다.

표준

조직에서 규정 준수 프레임워크의 일부로 정의한 제어 그룹입니다. 예를 들어 AWS Security Hub에서 지원하는 표준 중 하나와이 솔루션은 AWS FSBP입니다.

제어

규정 준수를 위해 리소스가 보유해야 하거나 보유해서는 안 되는 속성에 대한 설명입니다. 예를 들어, 제어 AWS FSBP Lambda.1에는 AWS Lambda 함수가 퍼블릭 액세스를 금지해야 한다고 명시되어 있습니다. 퍼블릭 액세스를 허용하는 함수는이 제어에 실패합니다.

통합 제어 조사 결과, 보안 제어, 보안 제어 보기

AWS Security Hub의 기능으로, 활성화되면 특정 표준에 해당하는 IDs가 아닌 통합 제어 IDs로 조사 결과를 표시합니다. 예를 들어는 AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2 및 PCI-DSS v3.2.1 S3.1을 제어합니다. 모든 맵은 통합(SC) 제어 S3.2 "S3 버킷은 퍼블릭 읽기 액세스를 금지해야 합니다."에 매핑됩니다. 이 기능을 켜면 SC 실행서가 사용됩니다.

AWS 용어에 대한 일반적인 참조는 AWS 용어집을 참조하세요.

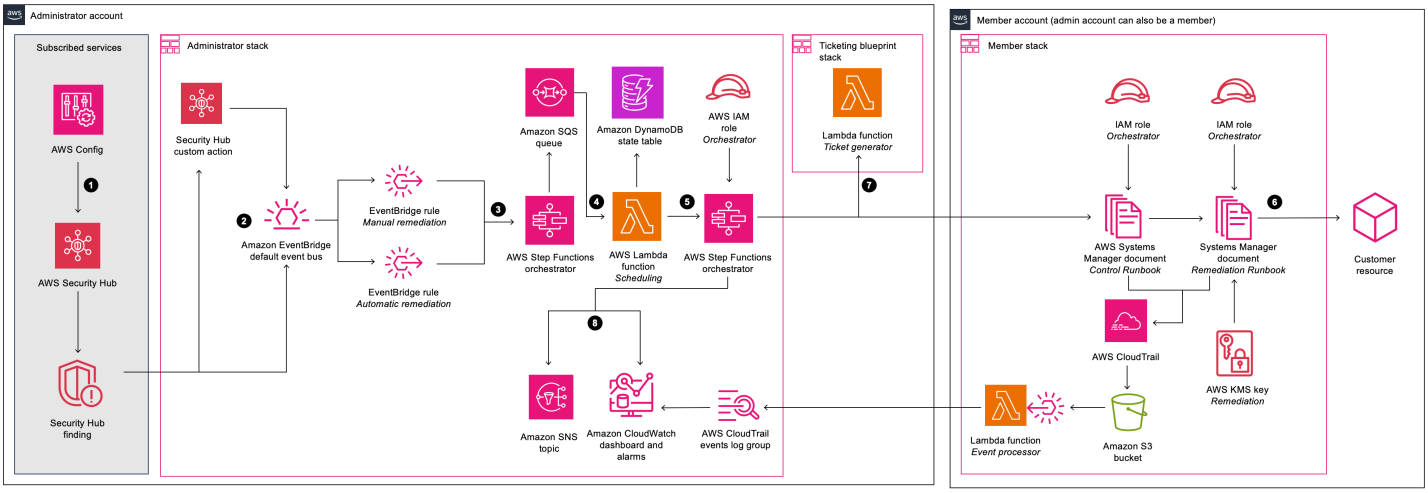
아키텍처 개요

이 섹션에서는 이 솔루션과 함께 배포된 구성 요소에 대한 참조 구현 아키텍처 다이어그램을 제공합니다.

아키텍처 다이어그램

이 솔루션을 기본 파라미터와 함께 배포하면 AWS 클라우드에서 다음 환경이 빌드됩니다.

AWS 아키텍처의 자동 보안 응답



> **Note**
>
> AWS CloudFormation 리소스는 AWS Cloud Development Kit(AWS CDK) 구문에서 생성됩니다.

AWS CloudFormation 템플릿과 함께 배포된 솔루션 구성 요소의 상위 수준 프로세스 흐름은 다음과 같습니다.

1. Detect: AWS Security Hub는 고객에게 AWS 보안 상태에 대한 포괄적인 보기를 제공합니다. 이를 통해 보안 업계 표준 및 모범 사례를 기준으로 환경을 측정할 수 있습니다. AWS Config, Amazon Guard Duty, AWS Firewall Manager와 같은 다른 AWS 서비스에서 이벤트와 데이터를 수집하는 방식으로 작동합니다. 이러한 이벤트 및 데이터는 CIS AWS Foundations Benchmark와 같은 보안 표준을 기준으로 분석됩니다. 예외는 AWS Security Hub 콘솔에서 조사 결과로 어설션됩니다. 새 결과는 Amazon EventBridge 이벤트로 전송됩니다.

2. 시작: 사용자 지정 작업을 사용하여 결과에 대해 이벤트를 시작할 수 있으며, 이로 인해 EventBridge 이벤트가 발생합니다. AWS Security Hub 사용자 지정 작업 및 EventBridge 규칙은 AWS 플레이북에서 자동 보안 응답을 시작하여 조사 결과를 해결합니다. 솔루션은 다음을 배포합니다.

   a. 사용자 지정 작업 이벤트와 일치하는 EventBridge 규칙 1개

   b. 실시간 조사 결과 이벤트와 일치하도록 지원되는 각 컨트롤(기본적으로 비활성화됨)에 대해 EventBridge 이벤트 규칙 1개

   Security Hub 콘솔의 사용자 지정 작업 메뉴를 사용하여 자동 문제 해결을 시작할 수 있습니다. 비프로덕션 환경에서 신중하게 테스트한 후 자동 문제 해결을 활성화할 수도 있습니다. 개별 문제 해결에 대해 자동화를 활성화할 수 있습니다. 모든 문제 해결에 대해 자동 시작을 활성화할 필요는 없습니다.

3. 사전 문제 해결: 관리자 계정에서 AWS Step Functions는 문제 해결 이벤트를 처리하고 예약할 준비를 합니다.

4. 일정: 솔루션은 예약 AWS Lambda 함수를 호출하여 Amazon DynamoDB 상태 테이블에 문제 해결 이벤트를 배치합니다.

5. 오케스트레이션: 관리자 계정에서 Step Functions는 교차 계정 AWS Identity and Access Management(IAM) 역할을 사용합니다. Step Functions는 보안 결과를 생성한 리소스가 포함된 멤버 계정에서 문제 해결을 호출합니다.

6. 해결 방법: 멤버 계정의 AWS Systems Manager Automation 문서는 Lambda 퍼블릭 액세스 비활성화와 같이 대상 리소스에 대한 조사 결과를 해결하는 데 필요한 작업을 수행합니다.

   선택적으로 EnableCloudTrailForASRActionLog 파라미터를 사용하여 멤버 스택에서 작업 로그 기능을 활성화할 수 있습니다. 이 기능은 멤버 계정에서 솔루션이 수행한 작업을 캡처하여 솔루션의 Amazon CloudWatch 대시보드에 표시합니다.

7. (선택 사항) 티켓 생성: TicketGenFunctionName 파라미터를 사용하여 관리자 스택에서 티켓팅을 활성화하면 솔루션이 제공된 티켓 생성기 Lambda 함수를 호출합니다. 이 Lambda 함수는 멤버 계정에서 문제 해결이 성공적으로 실행된 후 티켓팅 서비스에 티켓을 생성합니다. Jira 및 ServiceNow와의 통합을 위한 스택을 제공합니다.

8. 알림 및 로그: 플레이북은 결과를 CloudWatch 로그 그룹에 로깅하고, Amazon Simple Notification Service(Amazon SNS) 주제에 알림을 보내고, Security Hub 결과를 업데이트합니다. 이 솔루션은 결과 노트에 작업에 대한 감사 추적을 유지합니다.

AWS Well-Architected 설계 고려 사항

이 솔루션은 고객이 클라우드에서 안정적이고 안전하며 효율적이고 비용 효율적인 워크로드를 설계하고 운영할 수 있도록 지원하는 AWS Well-Architected Framework의 모범 사례를 바탕으로 설계되었습니다. 이 섹션에서는이 솔루션을 구축할 때 Well-Architected Framework의 설계 원칙과 모범 사례가 어떻게 적용되었는지 설명합니다.

운영 우수성

이 섹션에서는 운영 우수성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- CloudFormation을 사용하는 IaC로 정의된 리소스입니다.
- 가능한 경우 다음과 같은 특성으로 구현된 문제 해결:
  - 멱등성
  - 오류 처리 및 보고
  - 로깅
  - 장애 시 리소스를 알려진 상태로 복원

보안

이 섹션에서는 보안 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 인증 및 권한 부여에 사용한 IAM.
- 대부분의 경우 역할 권한 범위를 최대한 좁히도록 설정되었지만, 대부분의 경우 이 솔루션을 사용하려면 와일드카드 권한이 있어야 모든 리소스에 적용할 수 있습니다.

신뢰성

이 섹션에서는 신뢰성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- Security Hub는 조사 결과의 근본 원인이 해결되지 않은 경우 조사 결과를 계속 생성합니다.
- 서버리스 서비스를 사용하면 필요에 따라 솔루션의 규모를 조정할 수 있습니다.

성능 효율성

이 섹션에서는 성능 효율성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 오케스트레이션 및 권한을 직접 구현하지 않고도 확장할 수 있는 플랫폼으로 설계되었습니다.

비용 최적화

이 섹션에서는 비용 최적화 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 서버리스 서비스를 사용하면 사용한 만큼만 비용을 지불할 수 있습니다.
- 모든 계정에서 SSM 자동화를 위한 프리 티어 사용

지속 가능성

이 섹션에서는 지속 가능성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 서버리스 서비스를 사용하면 필요에 따라 스케일 업 또는 스케일 다운할 수 있습니다.

아키텍처 세부 정보

이 섹션에서는이 솔루션을 구성하는 구성 요소 및 AWS 서비스와 이러한 구성 요소가 함께 작동하는 방식에 대한 아키텍처 세부 정보를 설명합니다.

AWS Security Hub 통합

`automated-security-response-admin` 스택을 배포하면 AWS Security Hub의 사용자 지정 작업 기능과 통합됩니다. AWS Security Hub 콘솔 사용자가 문제 해결을 위해 조사 결과를 선택하면 솔루션은 AWS Step Functions.

교차 계정 권한 및 AWS Systems Manager 실행서는 `automated-security-response-member.template` 및 `automated-security-response-member-roles.template` CloudFormation 템플릿을 사용하여 모든 AWS Security Hub 계정(관리자 및 멤버)에 배포해야 합니다. 자세한 내용은 플레이북을 참조하세요. 이 템플릿을 사용하면 대상 계정에서 자동 문제 해결을 수행할 수 있습니다.

사용자는 Amazon CloudWatch 이벤트 규칙을 사용하여 문제 해결별로 자동 문제 해결을 자동으로 시작할 수 있습니다. 이 옵션은 결과가 AWS Security Hub에 보고되는 즉시 결과의 완전 자동 문제 해결을 활성화합니다. 기본적으로 자동 시작은 꺼져 있습니다. 이 옵션은 AWS Security Hub 관리자 계정에서 CloudWatch Events 규칙을 켜서 플레이북 설치 중 또는 설치 후에 언제든지 변경할 수 있습니다.

교차 계정 문제 해결

AWS의 자동 보안 응답은 교차 계정 역할을 사용하여 교차 계정 역할을 사용하는 기본 및 보조 계정에서 작업합니다. 이러한 역할은 솔루션 설치 중에 멤버 계정에 배포됩니다. 각 수정에는 개별 역할이 할당됩니다. 기본 계정의 수정 프로세스에는 수정이 필요한 계정의 수정 역할을 수임할 수 있는 권한이 부여됩니다. 수정은 수정이 필요한 계정에서 실행되는 AWS Systems Manager 실행서에 의해 수행됩니다.

플레이북

문제 해결 세트는 플레이북이라는 패키지로 그룹화됩니다. 플레이북은이 솔루션의 템플릿을 사용하여 설치, 업데이트 및 제거됩니다. 각 플레이북에서 지원되는 문제 해결에 대한 자세한 내용은 개발자 안내서 → 플레이북을 참조하세요. 이 솔루션은 현재 다음 플레이북을 지원합니다.

- Security Control은 2023년 2월 23일에 게시된 AWS Security Hub의 통합 제어 조사 결과 기능과 일치하는 플레이북입니다.

> **Important**
>
> Security Hub에서 통합 제어 조사 결과가 활성화된 경우 솔루션에서 활성화해야 하는 유일한 플레이북입니다.

- Center for Internet Security(CIS) Amazon Web Services Foundations 벤치마크, 버전 1.2.0, 2018년 5월 18일 게시.
- Center for Internet Security(CIS) Amazon Web Services Foundations 벤치마크, 버전 1.4.0, 2022년 11월 9일 게시.
- Center for Internet Security(CIS) Amazon Web Services Foundations 벤치마크, 버전 3.0.0, 2024년 5월 13일 게시.
- AWS Foundational Security Best Practices(FSBP) 버전 1.0.0, 2021년 3월 발행.
- Payment Card Industry Data Security Standards(PCI-DSS) 버전 3.2.1, 2018년 5월 게시.
- 미국 국립 표준 기술 연구소(NIST) 버전 5.0.0, 2023년 11월 발행.

중앙 집중식 로깅

단일 CloudWatch Logs 그룹인 SO0111-ASR에 대한 AWS 로그의 자동 보안 응답. 이러한 로그에는 솔루션의 문제 해결 및 관리를 위한 솔루션의 자세한 로깅이 포함되어 있습니다.

알림

이 솔루션은 Amazon Simple Notification Service(Amazon SNS) 주제를 사용하여 문제 해결 결과를 게시합니다. 이 주제에 대한 구독을 사용하여 솔루션의 기능을 확장할 수 있습니다. 예를 들어 이메일 알림을 보내고 문제 티켓을 업데이트할 수 있습니다.

- SO0111-ASR_Topic - 실행된 문제 해결과 관련된 일반적인 정보 및 오류 메시지를 보내는 데 사용됩니다.
- SO0111-ASR_Alarm_Topic - 솔루션의 경보 중 하나가 트리거될 때 이를 알리는 데 사용되며, 이는 솔루션이 예상대로 작동하지 않음을 나타냅니다.

이 솔루션의 AWS 서비스

솔루션은 다음 서비스를 사용합니다. 솔루션을 사용하려면 코어 서비스가 필요하며, 지원 서비스는 코어 서비스를 연결합니다.

AWS 서비스	설명
Amazon EventBridge	Core. 결과가 수정될 때 오케스트레이터 단계 함수를 시작하는 이벤트를 배포합니다.
AWS IAM	Core. 여러 역할을 배포하여 다양한 리소스에 대한 문제 해결을 허용합니다.
Lambda	Core. 단계 함수 오케스트레이터가 문제를 해결하는 데 사용할 여러 lambda 함수를 배포합니다.
AWS Security Hub	Core. 고객에게 AWS 보안 상태에 대한 포괄적인 보기를 제공합니다.
AWS Step Functions	Core. AWS Systems Manager API 호출을 통해 문제 해결 문서를 호출하는 오케스트레이터를 배포합니다.
AWS Systems Manager	Core. 실행할 문제 해결 로직이 포함된 System Manager 문서(문서에 대한 링크)를 배포합니다.
AWS CloudTrail	지원. AWS 리소스에 대한 솔루션의 변경 사항을 기록하고 CloudWatch 대시보드에 표시합니다.
Amazon CloudWatch	지원. 다른 플레이북이 결과를 로깅하는 데 사용할 로그 그룹을 배포합니다. 경보가 있는 사용자 지정 대시보드에 표시할 지표를 수집합니다.
AWS DynamoDB	지원. 문제 해결 일정을 최적화하기 위해 각 계정 및 리전에 마지막 실행 문제 해결을 저장합니다.
Amazon Simple Notification Service	지원. 수정이 완료되면 알림을 받는 SNS 주제를 배포합니다.
AWS SQS	지원. 솔루션이 문제 해결을 병렬로 실행할 수 있도록 문제 해결 예약을 지원합니다.

AWS 서비스	설명
AWS Key Management Service	지원. 문제 해결을 위해 데이터를 암호화하는 데 사용됩니다.
Config	지원. AWS Security Hub와 함께 사용할 모든 리소스를 기록합니다.

배포 계획

이 섹션에서는 솔루션을 배포하기 전에 발생하는 비용, 네트워크 보안, 지원되는 AWS 리전, 할당량 및 기타 고려 사항에 대해 설명합니다.

비용

이 솔루션을 실행하는 데 사용되는 AWS 서비스의 비용은 사용자의 책임입니다.

이번 개정부터 예상 월별 비용은 다음과 같습니다.

- 소규모 배포(계정 10개, 리전 1개 - 미국 동부/북부 버지니아): 매월 300건의 문제 해결에 대해 약 21.17 USD
- 중간 배포(100개 계정, 1개 리전 - 미국 동부/북부. 버지니아): 매월 3,000건의 문제 해결에 대해 약 134.86 USD
- 대규모 배포(1,000개 계정, 10개 리전): 매월 30,000건의 문제 해결에 대해 약 10,271.70 USD

> **Important**
>
> 요금은 변경될 수 있습니다. 자세한 내용은이 솔루션에 사용되는 각 AWS 서비스의 요금 페이지를 참조하세요.

> **Note**
>
> 많은 AWS 서비스에는 고객이 무료로 사용할 수 있는 서비스의 기준 금액인 프리 티어가 포함되어 있습니다. 실제 비용은 제공된 요금 예제보다 많거나 적을 수 있습니다.

비용 관리에 도움이 되도록 AWS Cost Explorer를 통해 예산을 생성하는 것이 좋습니다. 요금은 변경될 수 있습니다. 자세한 내용은이 솔루션에 사용되는 각 AWS 서비스의 요금 웹 페이지를 참조하세요.

샘플 비용 테이블

이 솔루션을 실행하는 데 드는 총 비용은 다음 요인에 따라 달라집니다.

- AWS Security Hub 멤버 계정 수
- 활성 자동 호출 문제 해결 수
- 문제 해결 빈도

이 솔루션은 구성에 따라 비용이 발생하는 다음 AWS 구성 요소를 사용합니다. 중소 규모 및 대규모 조직에 대한 요금 예제가 제공됩니다.

Service	프리 티어	요금 [USD]
AWS Systems Manager 자동화 - 단계 수	매월 계정당 100,000단계	프리 티어 외에도 각 기본 단계에는 단계당 0.002 USD가 부과됩니다. 다중 계정 자동화의 경우 모든 하위 계정에서 실행되는 단계를 포함한 모든 단계는 원래 계정에서만 계산됩니다.
AWS Systems Manager 자동화 - 단계 기간	매월 5,000초	프리 티어 외에도 각 aws:executeScript 작업 단계에는 월 5,000초의 프리 티어 후 초당 0.00003 USD가 부과됩니다.
AWS Systems Manager 자동화 - 스토리지	프리 티어 없음	매월 GB당 0.046 USD
AWS Systems Manager 자동화 - 데이터 전송	프리 티어 없음	전송된 GB당 0.900 USD(교차 계정 또는 out-of-Region)
AWS Security Hub - 보안 검사	프리 티어 없음	처음 100,000checks/account/Region/월 비용 검사당 0.0010 USD 다음 400,000checks/account/Region/월 비용은 검사당 0.0008 USD입니다.

Service	프리 티어	요금 [USD]
		500,000건 이상의 checks/account/Region/월 비용 검사당 0.0005 USD
AWS Security Hub - 수집 이벤트 찾기	처음 10,000events/account/Region/월은 무료입니다. Security Hub의 보안 검사와 관련된 수집 이벤트 찾기.	10,000개 이상의 events/account/Region/월 비용은 이벤트당 0.00003 USD입니다.
Amazon CloudWatch - 지표	기본 모니터링 지표(5분 빈도) 10개의 세부 모니터링 지표(1분 빈도) 1백만 개의 API 요청(GetMetricData 및 GetMetricWidgetImage에는 적용되지 않음)	첫 10,000개의 지표 비용은 월 0.30 USD입니다. 다음 240,000개의 지표 비용은 월 0.10 USD입니다. 다음 750,000개 지표 요금은 월 0.05 USD입니다. 1,000,000개 이상의 지표 비용은 월 0.02 USD입니다. API 호출 요금은 요청 1,000개당 0.01 USD입니다.
Amazon CloudWatch - 대시보드	매월 최대 50개의 지표에 대한 대시보드 3개	매월 대시보드당 3.00 USD

Service	프리 티어	요금 [USD]
Amazon CloudWatch - 경보	10 경보 지표(고분해능 경보에는 적용되지 않음)	표준 해상도(60초) 비용 경보당 0.10 USD 고해상도(10초) 비용은 경보 지표당 0.30 USD입니다. 경보당 표준 해결 이상 탐지 비용 0.30 USD 고분해능 이상 탐지 비용은 경보당 0.90 USD입니다. 경보당 복합 비용 0.50 USD
Amazon CloudWatch - 로그 컬렉션	5GB 데이터(수집, 아카이브 스토리지 및 Logs Insights 쿼리로 스캔한 데이터)	GB당 0.50 USD
Amazon CloudWatch - 로그 스토리지	5GB 데이터(수집, 아카이브 스토리지 및 Logs Insights 쿼리로 스캔한 데이터)	스캔한 데이터 GB당 0.005 USD
Amazon CloudWatch - 이벤트	사용자 지정 이벤트를 제외한 모든 이벤트가 포함됩니다.	사용자 지정 이벤트의 경우 이벤트 백만 개당 1.00 USD 교차 계정 이벤트의 경우 이벤트 백만 개당 1.00 USD
AWS Lambda - 요청	매월 1M 개의 무료 요청	1M 요청당 0.20 USD
AWS Lambda - 기간	매월 400,000GB-초의 컴퓨팅 시간	GB-초당 0.0000166667 USD. 기간 요금은 함수에 할당하는 메모리 양에 따라 달라집니다. 1MB 단위로 128MB에서 10,240MB 사이의 메모리를 함수에 할당할 수 있습니다. 1MB

Service	프리 티어	요금 [USD]
AWS Step Functions - 상태 전환	매월 4,000회의 무료 상태 전환	이후 상태 전환 1,000건당 0.025 USD
Amazon EventBridge	AWS 서비스에서 게시한 모든 상태 변경 이벤트는 무료입니다.	사용자 지정 이벤트는 게시된 사용자 지정 이벤트 백만 개당 1.00 USD의 비용이 듭니다. 타사(SaaS) 이벤트는 게시된 이벤트 백만 건당 1.00 USD의 비용이 듭니다. 교차 계정 이벤트는 전송된 백만 개의 교차 계정 이벤트당 1.00 USD의 비용이 듭니다.
Amazon SNS	매월 처음 1백만 개의 Amazon SNS 요청은 무료입니다.	이후 요청 1백만 건당 0.50 USD
Amazon SQS	매월 처음 1백만 개의 Amazon SQS 요청은 무료입니다.	이후 요청 1백만~1,000억 건당 0.40 USD
Amazon DynamoDB	처음 25GB의 스토리지는 무료입니다.	이후 1백만 개의 일관된 읽기 및 쓰기당 2.00 USD
AWS Key Management Service 요금	요청 20,000건/월	KMS 키 1개당 1.00 USD. 자동 또는 온디맨드 방식으로 교체하는 KMS 키의 경우 키의 첫 번째 및 두 번째 교체에 월 1 USD(시간당 비례 배분)의 비용이 추가됩니다.

요금 예제(월별)

예제 1: 매월 300건의 문제 해결

- 계정 10개, 리전 1개

- account/Region/month당 문제 해결 30건
- 월별 총 비용 21.17 USD

Service	가정	월별 요금[USD]
Systems Manager Automation	단계: ~4단계 * 문제 해결 300건 * 0.002 USD = 2.40 USD 기간: 10초 * 문제 해결 300건 * 0.00003 USD = 0.09 USD	2.49 USD
AWS Security Hub	청구 가능한 서비스를 사용하지 않음	$0
Amazon CloudWatch Logs	문제 해결 300건 * 0.000002 USD = 0.0006 USD $0.0006 * 0.03 = $0.000018	< 0.01 USD
AWS Lambda - 요청	문제 해결 300건 * 요청 6개 = 요청 1,800개 $0.20 * 1,000,000 요청 = $0.20	0.20 USD
AWS Lambda - 기간	256M: 1.875GB sec * 300개 문제 해결 * 0.0000167 USD = 0.009,375 USD	< 0.01 USD
Step Functions	상태 전환 17개 * 문제 해결 300개 = 5,100 $0.025 * (5,100/1,000) 상태 전환 = $0.15	0.15 USD
Amazon EventBridge 규칙	규칙에 대한 요금 없음	$0
AWS Key Management Service	키 1개 * 계정 10개 * 리전 1개 * $1 = $10	10.00 USD

Service	가정	월별 요금[USD]
Amazon DynamoDB	$2.00 * 1,000,000 읽기 및 쓰기 = $2.00	2.00 USD
Amazon SQS	$0.40 * 1,000,000 요청 = $0.40	0.40 USD
Amazon SNS	$0.50 * 1,000,000 알림 = $0.50	0.50 USD
Amazon CloudWatch - 지표	$0.30 * 7 사용자 지정 지표 = $2.10 $0.01 * (300 * 3 / 1,000) 풋 지표 API 호출 = $0.01	2.11 USD
Amazon CloudWatch - 대시보드	$3.00 * 대시보드 1개 = $3.00	3.00 USD
Amazon CloudWatch - 경보	$0.10 * 경보 3개 = $0.30	0.30 USD
합계		21.17 USD

예제 2: 매월 3,000건의 문제 해결

- 계정 100개, 리전 1개
- account/Region/month당 문제 해결 30건
- 월별 총 비용 134.86 USD

Service	가정	월별 요금[USD]
Systems Manager Automation	단계: ~4단계 * 문제 해결 3,000건 * 0.002 USD = 24.00 USD 기간: 10초 * 3,000건의 수정 사항 * 0.00003 USD = 0.90 USD	24.90 USD

Service	가정	월별 요금[USD]
AWS Security Hub	청구 가능한 서비스를 사용하지 않음	$0
Amazon CloudWatch Logs	문제 해결 3,000건 * 0.000002 USD = 0.006 USD $0.006 * 0.03 = $0.00018	< 0.01 USD
AWS Lambda - 요청	문제 해결 3,000건 * 요청 6건 = 요청 18,000건 $0.20 * 1,000,000 요청 = $0.20	0.20 USD
AWS Lambda - 기간	256M: 1.875GB 초 * 3,000건의 문제 해결 * 0.000167 USD = 0.09,375 USD	0.09 USD
Step Functions	상태 전환 17건 * 문제 해결 3,000건 = 51,000 $0.025 * (51,000/1,000) 상태 전환 = $1.275	1.28 USD
Amazon EventBridge 규칙	규칙에 대한 요금 없음	$0
AWS Key Management Service	키 1개 * 계정 100개 * 리전 1개 * $1 = $100	100 USD
Amazon DynamoDB	$2.00 * 1,000,000 읽기 및 쓰기 = $2.00	2.00 USD
Amazon SQS	$0.40 * 1,000,000 요청 = $0.40	0.40 USD
Amazon SNS	$0.50 * 1,000,000 알림 = $0.50	0.50 USD

Service	가정	월별 요금[USD]
Amazon CloudWatch - 지표	$0.30 * 7 사용자 지정 지표 = $2.10 $0.01 * (3000 * 3 / 1,000) 풋 지표 API 호출 = $0.09	2.19 USD
Amazon CloudWatch - 대시보드	$3.00 * 대시보드 1개 = $3.00	3.00 USD
Amazon CloudWatch - 경보	$0.10 * 경보 3개 = $0.30	0.30 USD
합계		134.86 USD

예제 3: 월별 30,000건의 문제 해결

- 계정 1,000개, 리전 10개
- account/Region/month당 문제 해결 30건
- 월별 총 비용 1,271.70 USD

Service	가정	월별 요금[USD]
Systems Manager Automation	단계: ~4단계 * 30,000건의 문제 해결 * 0.002 USD = 240.00 USD 기간: 10초 * 30,000건의 문제 해결 * 0.00003 USD = 9.00 USD	249.00 USD
AWS Security Hub	청구 가능한 서비스를 사용하지 않음	$0
Amazon CloudWatch Logs	30,000건의 문제 해결 * 0.000002 USD = 0.06 USD	< 0.01 USD

Service	가정	월별 요금[USD]
	$0.06 * 0.03 = $0.0018	
AWS Lambda - 요청	문제 해결 30,000건 * 요청 6건 = 요청 180,000건 $0.20 * 1,000,000 요청 = $0.20	0.20 USD
AWS Lambda - 기간	256M: 1.875GB sec * 30,000건의 문제 해결 * 0.000167 USD = 0.9375 USD	0.94 USD
Step Functions	상태 전환 17건 * 문제 해결 30,000건 = 510,000 $0.025 * (510,000/1,000) 상태 전환 = $12.75	12.75 USD
Amazon EventBridge 규칙	규칙에 대한 요금 없음	$0
AWS Key Management Service	(키 1개) 1 USD * 계정 1,000개 * 리전 10개 = 10,000 USD	10,000 USD
Amazon DynamoDB	$0.000002 * 1,000,000 읽기 및 쓰기 = $2.00	2.00 USD
Amazon SQS	$0.000004 * 요청 1,000,000개 = $0.40	0.40 USD
Amazon SNS	$0.000005 * 1,000,000 알림 = $0.50	0.50 USD
Amazon CloudWatch - 지표	0.30 USD * 사용자 지정 지표 6개 = 1.80 USD $0.01 * (30,000 * 3 / 1,000) 풋 지표 API 호출 = $0.90	2.70 USD

Service	가정	월별 요금[USD]
Amazon CloudWatch - 대시보드	$3.00 * 대시보드 1개 = $3.00	3.00 USD
Amazon CloudWatch - 경보	$0.10 * 경보 2개 = $0.20	0.20 USD
합계		10,271.70 USD

> **Important**
>
> KMS 키 교체 비용 AWS Key Management Service (KMS)는 교체가 활성화되면 고객 관리형 키를 1년에 한 번 자동으로 교체합니다. 각 교체에는 연간 키당 1.00 USD의 비용이 발생합니다. 예를 들어 단일 리전에 1,000개의 계정이 있는 경우 연간 1,000 USD(교체 1개 × 키 1,000개 × 1.00 USD)가 추가로 발생합니다.

선택적 기능에 대한 추가 비용

이 섹션에서는이 솔루션의 선택적 기능과 관련된 추가 비용을 설명합니다.

향상된 CloudWatch 지표

관리자 스택을 배포할 때 EnableEnhancedCloudWatchMetrics 파라미터에 `yes` 대해를 선택하면 솔루션은 각 제어 ID에 대해 사용자 지정 지표 2개와 경보 1개를 생성합니다. 비용은 수정하려는 제어 IDs 수에 따라 달라집니다. 다음 표에서는 비용 상한을 결정하기 위해 매월 96개의 서로 다른 제어 IDs를 모두 수정한다고 가정합니다.

Service	96IDs 가정 * 2 = 192개의 사용자 지정 지표	월별 요금[USD]
Amazon CloudWatch - 지표	$0.30 * 192 사용자 지정 지표 = $57.60	57.60 USD
Amazon CloudWatch - 경보	$0.10 * 96 경보 = $9.60	9.60 USD
합계		67.20 USD

CloudTrail 작업 로그

작업 로그 기능을 활성화하는 각 멤버 계정에서 솔루션은 모든 쓰기 관리 이벤트를 로깅하는 CloudTrail 추적을 생성합니다. Lambda 함수는 솔루션과 관련이 없는 이벤트를 필터링합니다. 즉, 솔루션과 관련이 없는 이벤트는 여전히 추적에서 캡처되고 Lambda 함수에서 처리되므로 비용은 계정의 총 관리 이벤트 수와 관련이 있습니다.

다음 표에서는 계정에서 매월 150,000개의 관리 이벤트를 가정합니다. 실제 비용은 계정의 실제 관리 이벤트 활동에 따라 달라집니다.

Service	가정	월별 요금[USD]
CloudTrail	150,000 * 2.00 USD/100,000 USD = 3.00 USD	3.00 USD
Lambda	150,000 * 0.2 * 0.125 = 3,750GB-초 3,750 * 0.0000166667 USD = 0.0625 USD 컴퓨팅 시간 비용 0.15 * 0.20 USD = 0.03 USD 요청 비용 $0.0625 + $0.03 = 총 Lambda 비용 $0.0952	$0.0925
합계		멤버 계정당 3.09 USD

보안

AWS 인프라에 시스템을 구축하면 사용자와 AWS 간에 보안 책임이 공유됩니다. AWS는 호스트 운영 체제, 가상화 계층 및 서비스가 운영되는 시설의 물리적 보안을 포함한 구성 요소를 운영, 관리 및 제어하므로이 공유 모델은 운영 부담을 줄입니다. AWS 보안에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오.

IAM 역할

AWS Identity and Access Management(IAM) 역할을 통해 고객은 AWS 클라우드의 서비스 및 사용자에게 세분화된 액세스 정책 및 권한을 할당할 수 있습니다. 이 솔루션은 솔루션의 자동화된 함수에 각 문제 해결과 관련된 좁은 범위의 권한 집합 내에서 문제 해결 작업을 수행할 수 있는 액세스 권한을 부여하는 IAM 역할을 생성합니다.

관리자 계정의 Step Function은 SO0111-ASR-Orchestrator-Admin 역할에 할당됩니다. 이 역할만 각 멤버 계정에서 SO0111-Orchestrator-Member를 수임할 수 있습니다. 각 수정 역할은 멤버 역할을 AWS Systems Manager 서비스에 전달하여 특정 수정 런북을 실행할 수 있습니다. 문제 해결 역할 이름은 SO0111로 시작하고 문제 해결 런북의 이름과 일치하는 설명이 이어집니다. 예를 들어 SO0111-RemoveVPCDefaultSecurityGroupRules는 ASR-RemoveVPCDefaultSecurityGroupRules 문제 해결 런북의 역할입니다.

지원되는 AWS 리전

리전 이름	리전 코드
미국 동부(오하이오)	us-east-2
미국 동부(버지니아 북부)	us-east-1
미국 서부(캘리포니아 북부)	us-west-1
미국 서부(오리건)	us-west-2
아프리카(케이프타운)	af-south-1
아시아 태평양(홍콩)	ap-east-1
아시아 태평양(하이데라바드)	ap-south-2
아시아 태평양(자카르타)	ap-southeast-3
아시아 태평양(멜버른)	ap-southeast-4
아시아 태평양(뭄바이)	ap-south-1
아시아 태평양(오사카)	ap-northeast-3

리전 이름	리전 코드
아시아 태평양(서울)	ap-northeast-2
아시아 태평양(싱가포르)	ap-southeast-1
아시아 태평양(시드니)	ap-southeast-2
아시아 태평양(도쿄)	ap-northeast-1
캐나다(중부)	ca-central-1
유럽(프랑크푸르트)	eu-central-1
유럽(아일랜드)	eu-west-1
유럽(런던)	eu-west-2
유럽(밀라노)	eu-south-1
유럽(파리)	eu-west-3
유럽(스페인)	eu-south-2
유럽(스톡홀름)	eu-north-1
유럽(취리히)	eu-central-2
중동(바레인)	me-south-1
중동(UAE)	me-central-1
남아메리카(상파울루)	sa-east-1
AWS GovCloud(US-East)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1
중국(베이징)	cn-north-1
중국(닝샤)	cn-northwest-1

리전 이름	리전 코드
이스라엘(텔아비브)	il-central-1
캐나다 서부(캘거리)	ca-west-1
멕시코(멕시코 시티)	mx-central-1
아시아 태평양(태국)	ap-southeast-7

> **Note**
>
> 목록에 없는 모든 새 AWS 리전은 로컬 배포를 통해 지원될 수 있지만 원클릭 배포는 지원되지 않습니다.

할당량

서비스 할당량(제한이라고도 함)은 AWS 계정의 최대 서비스 리소스 또는 작업 수입니다.

이 솔루션의 AWS 서비스에 대한 할당량

이 솔루션에 구현된 각 서비스의 할당량이 충분한지 확인하세요. 자세한 내용은 AWS 서비스 할당량을 참조하세요.

다음 링크를 사용하여 해당 서비스의 페이지로 이동합니다. 페이지를 전환하지 않고 설명서의 모든 AWS 서비스에 대한 Service Quotas 보려면 대신 PDF의 서비스 엔드포인트 및 할당량 페이지에서 정보를 확인합니다.

AWS CloudFormation 할당량

AWS 계정에는이 솔루션에서 스택을 시작할 때 알아야 할 AWS CloudFormation 할당량이 있습니다. 이러한 할당량을 이해하면 이 솔루션을 성공적으로 배포하지 못하는 제한 오류를 방지할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation 할당량을 참조하세요. AWS CloudFormation

AWS CloudWatch 할당량

AWS 계정에는 CloudWatch 리소스 정책에 연결된 AWS CloudWatch 할당량이 있습니다.이 할당량은 계정당 리전당 10개의 리소스 정책만 허용하며 할당량 증가에 대해서는 요청할 수 없습니다. AWS CloudWatch 사용 설명서의 AWS CloudWatch Logs 할당량을 참조하세요. CloudWatch 배포하기 전에 현재 사용량을 확인하여 솔루션을 배포할 때이 임계값을 초과하지 않는지 확인하세요.

Amazon EventBridge 규칙 할당량

AWS 계정에는 솔루션과 함께 배포할 플레이북을 선택할 때 알아야 할 Amazon EventBridge 규칙 할당량이 있습니다. 각 플레이북은 수정할 수 있는 각 컨트롤에 대해 EventBridge 규칙을 생성합니다. 여러 플레이북을 배포할 때 규칙 할당량에 도달할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 할당량을 참조하세요. EventBridge

AWS Security Hub 배포

AWS Security Hub 배포 및 구성은이 솔루션의 사전 조건입니다. AWS Security Hub 설정에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 AWS Security Hub 설정을 참조하세요.

최소한 기본 계정에 작동하는 Security Hub가 구성되어 있어야 합니다. 이 솔루션은 Security Hub 기본 계정과 동일한 계정(및 AWS 리전)에 배포할 수 있습니다. 또한 각 Security Hub 기본 및 보조 계정에서 솔루션의 AWS Step Functions에 AssumeRole 권한을 허용하는 멤버 템플릿을 배포하여 계정에서 문제 해결 런북을 실행해야 합니다.

Stack과 StackSets 배포 비교

스택 세트를 사용하면 단일 AWS CloudFormation 템플릿을 사용하여 AWS 리전의 AWS 계정에서 스택을 생성할 수 있습니다. 버전 1.4부터이 솔루션은 배포 위치와 방법에 따라 리소스를 분할하여 스택 세트 배포를 지원합니다. 다중 계정 고객, 특히 AWS Organizations를 사용하는 고객은 스택 세트를 사용하여 여러 계정에 배포할 수 있습니다. 솔루션을 설치하고 유지 관리하는 데 필요한 노력을 줄입니다. StackSets에 대한 자세한 내용은 AWS CloudFormation StackSets 사용을 참조하세요.

솔루션 배포

> **Important**
>
> Security Hub에서 통합 제어 조사 결과 기능이 켜져 있는 경우(새 배포에서는 기본값임) 이 솔루션을 배포할 때만 보안 제어(CS) 플레이북을 활성화합니다. 기능이 켜져 있지 않은 경우 Security Hub에서 활성화된 보안 표준에 대한 플레이북만 활성화합니다. 추가 플레이북을 활성화하면 EventBridge 규칙의 할당량에 도달할 수 있습니다.

이 솔루션은 AWS CloudFormation 템플릿 및 스택을 사용하여 배포를 자동화합니다. CloudFormation 템플릿은이 솔루션에 포함된 AWS 리소스와 해당 속성을 지정합니다. CloudFormation 스택은 템플릿에 설명된 리소스를 프로비저닝합니다.

솔루션이 작동하려면 세 개의 템플릿을 배포해야 합니다. 먼저 템플릿을 배포할 위치를 결정한 다음 배포 방법을 결정합니다.

이 개요에서는 템플릿과 템플릿을 배포할 위치와 방법을 결정하는 방법을 설명합니다. 다음 섹션에는 각 스택을 스택 또는 스택 StackSet.

각 스택을 배포할 위치 결정

세 가지 템플릿은 다음 이름으로 참조되며 다음 리소스를 포함합니다.

- 관리자 스택: 오케스트레이터 단계 함수, 이벤트 규칙 및 Security Hub 사용자 지정 작업.
- 멤버 스택: SSM 자동화 문서 수정.
- 멤버 역할 스택: 문제 해결을 위한 IAM 역할.

관리자 스택은 단일 계정 및 단일 리전에 한 번 배포해야 합니다. 조직의 Security Hub 조사 결과의 집계 대상으로 구성한 계정 및 리전에 배포해야 합니다. 작업 로그 기능을 사용하여 관리 이벤트를 모니터링하려면 조직의 관리 계정 또는 위임된 관리자 계정에 관리자 스택을 배포해야 합니다.

솔루션은 Security Hub 조사 결과에서 작동하므로 해당 계정 또는 리전이 Security Hub 관리자 계정 및 리전의 조사 결과를 집계하도록 구성되지 않은 경우 특정 계정 및 리전의 조사 결과에서 작동할 수 없습니다.

예를 들어, 조직에는 리전 `us-east-1` 및에서 운영되는 계정이 있으며`us-west-2`, 계정은 리전의 Security Hub 위임된 관리자`111111111111`입니다`us-east-1`. `222222222222` 및 계정은 위

임된 관리자 계정의 Security Hub 멤버 계정이어야 333333333333 합니다111111111111. 에서 로 결과를 집계us-west-2하도록 세 계정을 모두 구성해야 합니다us-east-1. 관리자 스택은 111111111111의 계정에 배포해야 합니다us-east-1.

집계 결과에 대한 자세한 내용은 Security Hub 위임된 관리자 계정 및 교차 리전 집계 설명서를 참조하세요.

멤버 계정에서 허브 계정으로 신뢰 관계를 생성할 수 있도록 멤버 스택을 배포하기 전에 관리자 스택이 먼저 배포를 완료해야 합니다.

결과를 수정하려는 모든 계정 및 리전에 멤버 스택을 배포해야 합니다. 여기에는 이전에 ASR 관리자 스택을 배포한 Security Hub 위임된 관리자 계정이 포함될 수 있습니다. SSM 자동화에 프리 티어를 사용하려면 자동화 문서가 멤버 계정에서 실행되어야 합니다.

이전 예제를 사용하여 모든 계정 및 리전의 결과를 해결하려면 멤버 스택을 세 계정(,111111111111 222222222222및 333333333333)과 두 리전(us-east-1 및) 모두에 배포해야 합니다us-west-2.

멤버 역할 스택은 모든 계정에 배포해야 하지만 계정당 한 번만 배포할 수 있는 글로벌 리소스(IAM 역할)가 포함되어 있습니다. 멤버 역할 스택을 배포하는 리전은 중요하지 않으므로 간소화를 위해 관리자 스택이 배포되는 동일한 리전에 배포하는 것이 좋습니다.

이전 예제를 사용하여의 세 계정(, 222222222222및 111111111111333333333333) 모두에 멤버 역할 스택을 배포하는 것이 좋습니다us-east-1.

각 스택을 배포하는 방법 결정

스택 배포 옵션은 다음과 같습니다.

- CloudFormation StackSet(자체 관리형 권한)
- CloudFormation StackSet(서비스 관리형 권한)
- CloudFormation 스택

서비스 관리형 권한이 있는 StackSets는 자체 역할을 배포할 필요가 없으며 조직의 새 계정에 자동으로 배포할 수 있으므로 가장 편리합니다. 안타깝게도이 방법은 관리자 스택과 멤버 스택 모두에서 사용하는 중첩 스택을 지원하지 않습니다. 이러한 방식으로 배포할 수 있는 유일한 스택은 멤버 역할 스택입니다.

전체 조직에 배포할 때는 조직 관리 계정이 포함되지 않으므로 조직 관리 계정의 조사 결과를 수정하려면이 계정에 별도로 배포해야 합니다.

멤버 스택은 모든 계정 및 리전에 배포해야 하지만 중첩 스택이 포함되어 있으므로 서비스 관리형 권한이 있는 StackSets를 사용하여 배포할 수 없습니다. 따라서 자체 관리형 권한이 있는 StackSets를 사용하여이 스택을 배포하는 것이 좋습니다.

관리자 스택은 한 번만 배포되므로 단일 계정 및 리전에 자체 관리형 권한이 있는 일반 CloudFormation 스택 또는 StackSet로 배포할 수 있습니다.

통합 제어 조사 결과

Security Hub의 통합 제어 조사 결과 기능을 켜거나 끄면 조직의 계정을 구성할 수 있습니다. AWS Security Hub 사용 설명서의 통합 제어 조사 결과를 참조하세요.

> **Important**
>
> 활성화된 경우 솔루션의 v2.0.0 이상을 사용해야 합니다. 또한 "SC" 또는 "보안 제어" 표준에 대한 관리자 및 멤버 중첩 스택을 모두 배포해야 합니다. 그러면이 기능이 켜져 있을 때 생성된 통합 제어 IDs와 함께 사용할 자동화 문서 및 EventBridge 규칙이 배포됩니다. 이 기능을 사용할 때 특정 표준(예: AWS FSBP)에 대해 관리자 또는 멤버 중첩 스택을 배포할 필요가 없습니다.

AWS CloudFormation 템플릿

View template

automated-security-response-admin.template -이 템플릿을 사용하여 AWS에서 자동 보안 응답을 시작합니다. 템플릿은 솔루션의 핵심 구성 요소, AWS Step Functions 로그에 대한 중첩 스택, 활성화하도록 선택한 각 보안 표준에 대한 중첩 스택 하나를 설치합니다.

사용되는 서비스에는 Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions, Amazon CloudWatch Logs, Amazon S3 및 AWS Systems Manager가 포함됩니다.

관리자 계정 지원

다음 템플릿은 AWS Security Hub 관리자 계정에 설치되어 지원하려는 보안 표준을 켭니다. 를 설치할 때 설치할 다음 템플릿 중 하나를 선택할 수 있습니다`automated-security-response-admin.template`.

automated-security-response-orchestrator-log.template - Orchestrator Step Function에 대한 CloudWatch 로그 그룹을 생성합니다.

AFSBPStack.template - AWS 기본 보안 모범 사례 v1.0.0 규칙.

CIS120Stack.template - CIS Amazon Web Services Foundations 벤치마크, v1.2.0 규칙.

CIS140Stack.template - CIS Amazon Web Services Foundations 벤치마크, v1.4.0 규칙.

CIS300Stack.template - CIS Amazon Web Services Foundations 벤치마크, v3.0.0 규칙.

PCI321Stack.template - PCI-DSS v3.2.1 규칙.

NISTStack.template - NIST(National Institute of Standards and Technology), v5.0.0 규칙.

SCStack.template - Security Controls v2.0.0 규칙.

멤버 역할

View template

automated-security-response-member-roles.template - 각 AWS Security Hub 멤버 계정에 필요한 수정 역할을 정의합니다.

멤버 계정

View template

automated-security-response-member.template - 코어 솔루션을 설정한 후이 템플릿을 사용하여 각 AWS Security Hub 멤버 계정(관리자 계정 포함)에 AWS Systems Manager 자동화 런북 및 권한을 설치합니다. 이 템플릿을 사용하면 설치할 보안 표준 플레이북을 선택할 수 있습니다.

는 선택한 항목에 따라 다음 템플릿을 `automated-security-response-member.template` 설치합니다.

automated-security-response-remediation-runbooks.template - 하나 이상의 보안 표준에서 사용하는 일반적인 문제 해결 코드입니다.

AFSBPMemberStack.template - AWS 기본 보안 모범 사례 v1.0.0 설정, 권한 및 문제 해결 런북.

CIS120MemberStack.template - CIS Amazon Web Services Foundations 벤치마크, 버전 1.2.0 설정, 권한 및 문제 해결 런북.

CIS140MemberStack.template - CIS Amazon Web Services Foundations 벤치마크, 버전 1.4.0 설정, 권한 및 문제 해결 런북.

CIS300MemberStack.template - CIS Amazon Web Services Foundations 벤치마크, 버전 3.0.0 설정, 권한 및 문제 해결 런북.

PCI321MemberStack.template - PCI-DSS v3.2.1 설정, 권한 및 문제 해결 런북.

NISTMemberStack.template - NIST(National Institute of Standards and Technology), v5.0.0 설정, 권한 및 문제 해결 런북.

SCMemberStack.template - 보안 제어 설정, 권한 및 문제 해결 런북.

automated-security-response-member-cloudtrail.template - 작업 로그 기능에서 및 서비스 활동을 추적하고 감사하는 데 사용됩니다.

티켓 시스템 통합

다음 템플릿 중 하나를 사용하여 티켓팅 시스템과 통합합니다.

View template

JiraBlueprintStack.template - Jira를 티켓팅 시스템으로 사용하는 경우 배포합니다.

View template

ServiceNowBlueprintStack.template - ServiceNow를 티켓팅 시스템으로 사용하는 경우 배포합니다.

다른 외부 티켓팅 시스템을 통합하려는 경우 이러한 스택 중 하나를 청사진으로 사용하여 자체 사용자 지정 통합을 구현하는 방법을 이해할 수 있습니다.

자동 배포 - StackSets

> **Note**
>
> StackSets를 사용하여 배포하는 것이 좋습니다. 그러나 단일 계정 배포 또는 테스트 또는 평가 목적의 경우 스택 배포 옵션을 고려하세요.

솔루션을 시작하기 전에이 가이드에서 설명하는 아키텍처, 솔루션 구성 요소, 보안 및 설계 고려 사항을 검토하세요. 이 섹션의 step-by-step 지침에 따라 솔루션을 구성하고 AWS Organizations에 배포합니다.

배포 시간: StackSet 파라미터에 따라 계정당 약 30분.

사전 조건

AWS Organizations는 다중 계정 AWS 환경 및 리소스를 중앙에서 관리하고 관리하는 데 도움이 됩니다. StackSets는 AWS Organizations에서 가장 잘 작동합니다.

이전에이 솔루션의 v1.3.x 이하를 배포한 경우 기존 솔루션을 제거해야 합니다. 자세한 내용은 솔루션 업데이트를 참조하세요.

이 솔루션을 배포하기 전에 AWS Security Hub 배포를 검토합니다.

- AWS Organization에는 위임된 Security Hub 관리자 계정이 있어야 합니다.
- Security Hub는 리전 간에 조사 결과를 집계하도록 구성해야 합니다. 자세한 내용은 AWS Security Hub 사용 설명서의 리전 간 조사 결과 집계를 참조하세요.
- AWS를 사용하는 각 리전에서 조직에 대해 Security Hub를 활성화해야 합니다.

이 절차에서는 AWS Organizations를 사용하는 계정이 여러 개 있고 AWS Organizations 관리자 계정과 AWS Security Hub 관리자 계정을 위임했다고 가정합니다.

배포 개요

> **Note**
>
> 이 솔루션의 StackSets 배포는 서비스 관리형 및 자체 관리형 StackSets의 조합을 사용합니다. 자체 관리형 StackSets 서비스 관리형 StackSets 아직 지원되지 않는 중첩된 StackSets 사용하므로 현재 사용해야 합니다.

AWS Organizations의 위임된 관리자 계정에서 StackSets를 배포합니다. https://docs.aws.amazon.com/organizations/latest/userguide/services-that-can-integrate-cloudformation.html AWS Organizations

계획

다음 양식을 사용하여 StackSets 배포를 지원합니다. 데이터를 준비한 다음 배포 중에 값을 복사하여 붙여넣습니다.

```
AWS Organizations admin account ID: _________________
Security Hub admin account ID: _________________
CloudTrail Logs Group: ____________________________
Member account IDs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
AWS Organizations OUs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
```

(선택 사항) 0단계: 티켓팅 통합 스택 배포

- 티켓팅 기능을 사용하려는 경우 먼저 티켓팅 통합 스택을 Security Hub 관리자 계정에 배포합니다.
- 이 스택에서 Lambda 함수 이름을 복사하여 관리자 스택에 입력으로 제공합니다(1단계 참조).

1단계: 위임된 Security Hub 관리자 계정에서 관리자 스택 시작

- 자체 관리형 StackSet를 사용하여 `automated-security-response-admin.template` AWS CloudFormation 템플릿을 Security Hub 관리자와 동일한 리전의 AWS Security Hub 관리자 계정으로 시작합니다. 이 템플릿은 중첩 스택을 사용합니다.
- 설치할 보안 표준을 선택합니다. 기본적으로 SC만 선택됩니다(권장).
- 사용할 기존 Orchestrator 로그 그룹을 선택합니다. 이전 설치에서 `SO0111-ASR- Orchestrator` 이미 존재하는 `Yes` 경우를 선택합니다.

자체 관리형 StackSets에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 자체 관리형 권한 부여를 참조하세요.

2단계: 각 AWS Security Hub 멤버 계정에 문제 해결 역할 설치

2단계의 템플릿이 1단계에서 생성한 IAM 역할을 참조하므로 1단계에서 배포가 완료될 때까지 기다립니다.

- 서비스 관리형 StackSet를 사용하여 `automated-security-response-member-roles.template` AWS Organizations의 각 계정에서 AWS CloudFormation 템플릿을 단일 리전으로 시작합니다. AWS Organizations
- 새 계정이 조직에 가입하면이 템플릿을 자동으로 설치하도록 선택합니다.
- AWS Security Hub 관리자 계정의 계정 ID를 입력합니다.

3단계: 각 AWS Security Hub 멤버 계정 및 리전에서 멤버 스택 시작

- 자체 관리형 StackSets를 사용하여 동일한 Security Hub 관리자가 관리하는 `automated-security-response-member.template` AWS Organization의 모든 계정에 AWS 리소스가 있는 모든 리전에서 AWS CloudFormation 템플릿을 시작합니다.

> **Note**
>
> 서비스 관리형 StackSets 중첩 스택을 지원할 때까지 조직에 가입하는 모든 새 계정에 대해 이 단계를 수행해야 합니다.

- 설치할 보안 표준 플레이북을 선택합니다.
- CloudTrail 로그 그룹의 이름을 입력합니다(일부 수정 사항에서 사용).
- AWS Security Hub 관리자 계정의 계정 ID를 입력합니다.

(선택 사항) 0단계: 티켓 시스템 통합 스택 시작

1. 티켓팅 기능을 사용하려는 경우 먼저 각 통합 스택을 시작합니다.
2. Jira 또는 ServiceNow에 대해 제공된 통합 스택을 선택하거나 이를 블루프린트로 사용하여 사용자 지정 통합을 구현합니다.

   Jira 스택을 배포하려면:

   a. 스택의 이름을 입력합니다.

   b. Jira 인스턴스에 URI를 제공합니다.

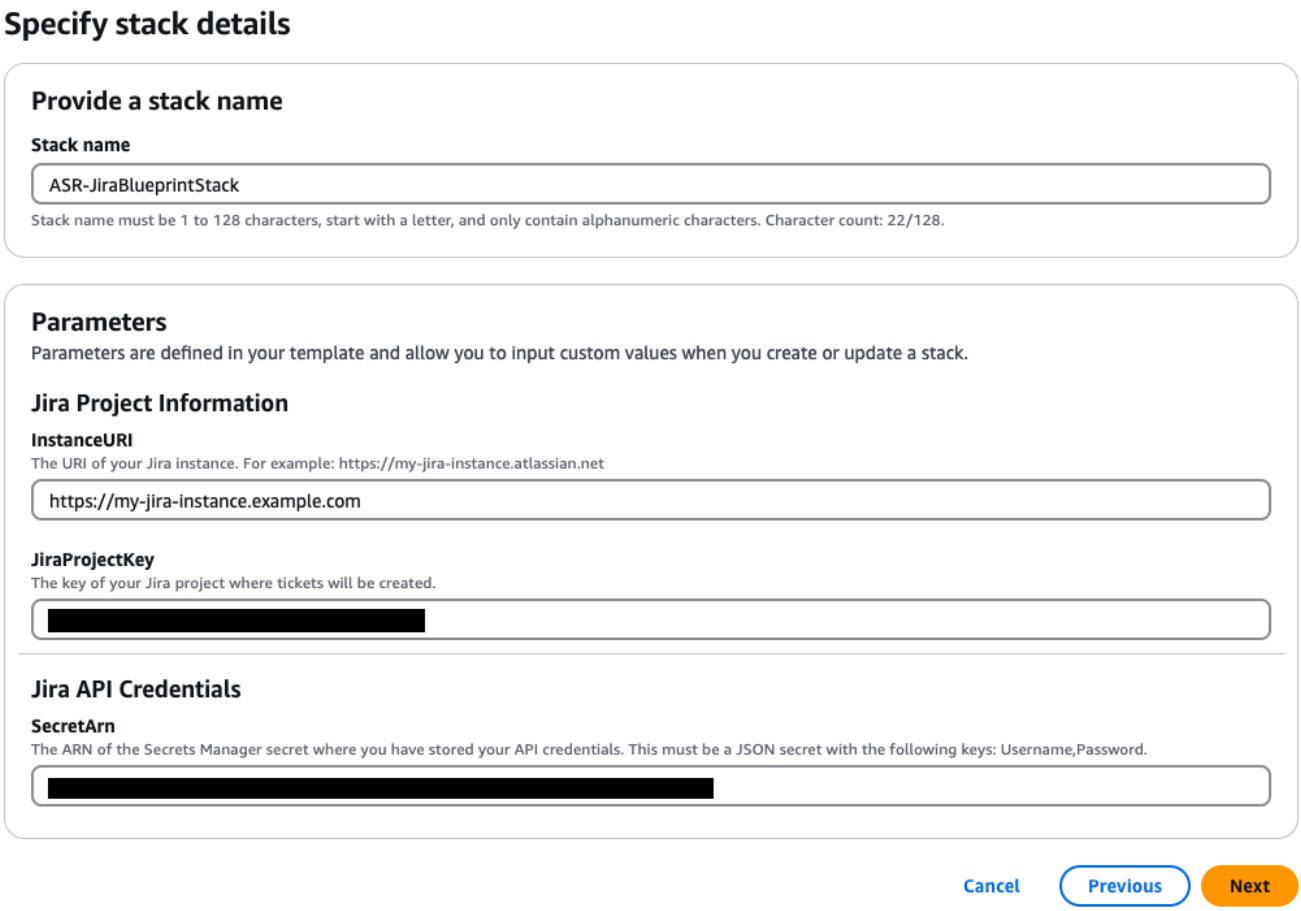
   c. 티켓을 보내려는 Jira 프로젝트의 프로젝트 키를 제공합니다.

d. Secrets Manager에서 Jira `Username` 및를 포함하는 새 키-값 보안 암호를 생성합니다.`Password`.

> **Note**
>
> 사용자 이름을 로`Username`, API 키를 로 제공하여 암호 대신 Jira API 키를 사용하도록 선택할 수 있습니다`Password`.

e. 이 보안 암호의 ARN을 스택에 입력으로 추가합니다.

스택 이름 Jira 프로젝트 정보와 Jira API 자격 증명을 제공합니다.



ServiceNow 스택을 배포하려면:

f. 스택의 이름을 입력합니다.

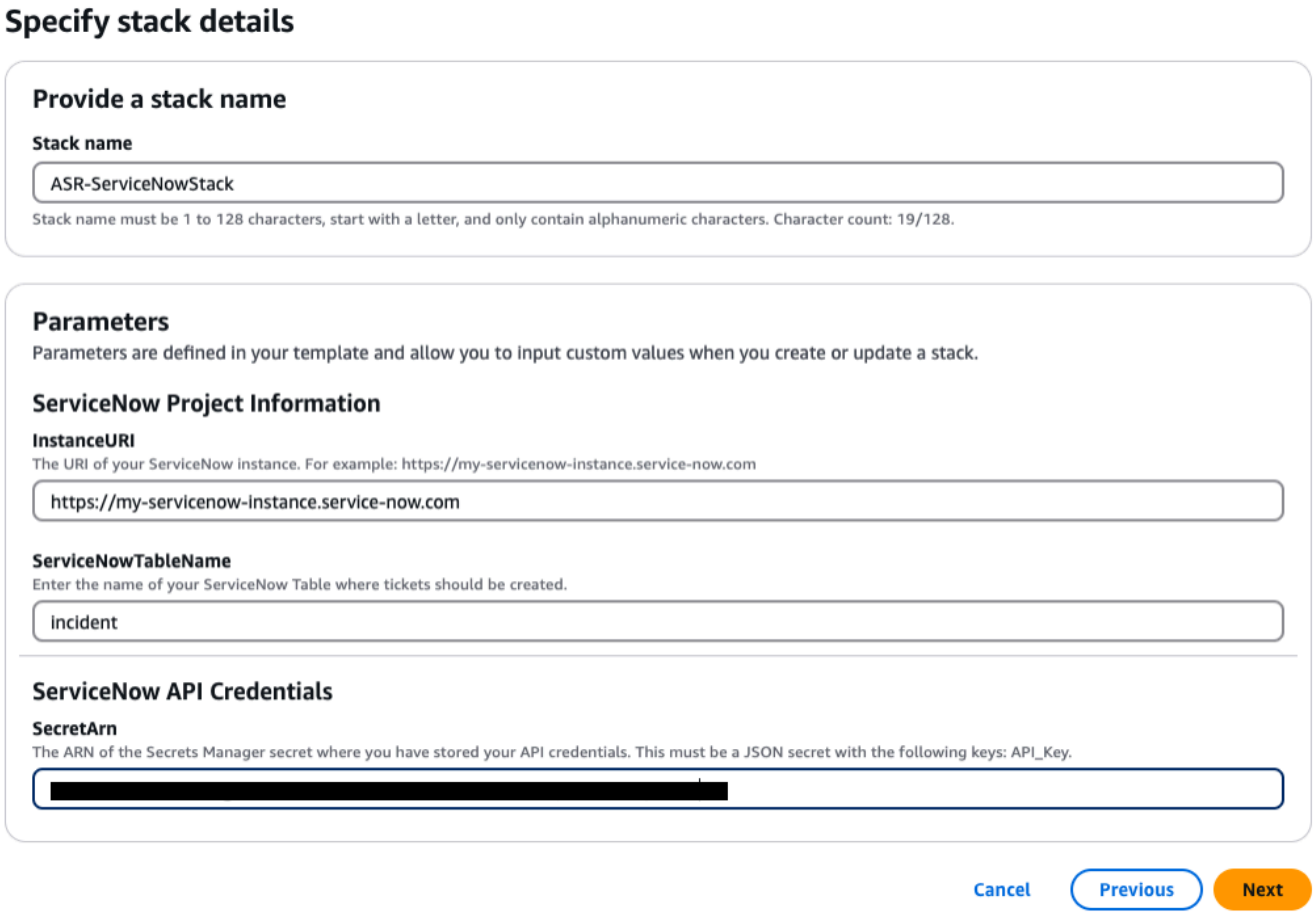
g. ServiceNow 인스턴스의 URI를 제공합니다.

h. ServiceNow 테이블 이름을 입력합니다.

i. 작성하려는 테이블을 수정할 수 있는 권한이 있는 API 키를 ServiceNow에 생성합니다.

j. 키를 사용하여 Secrets Manager에서 보안 암호를 `API_Key` 생성하고 보안 암호 ARN을 스택에 대한 입력으로 제공합니다.

스택 이름 ServiceNow 프로젝트 정보와 ServiceNow API 자격 증명을 제공합니다.

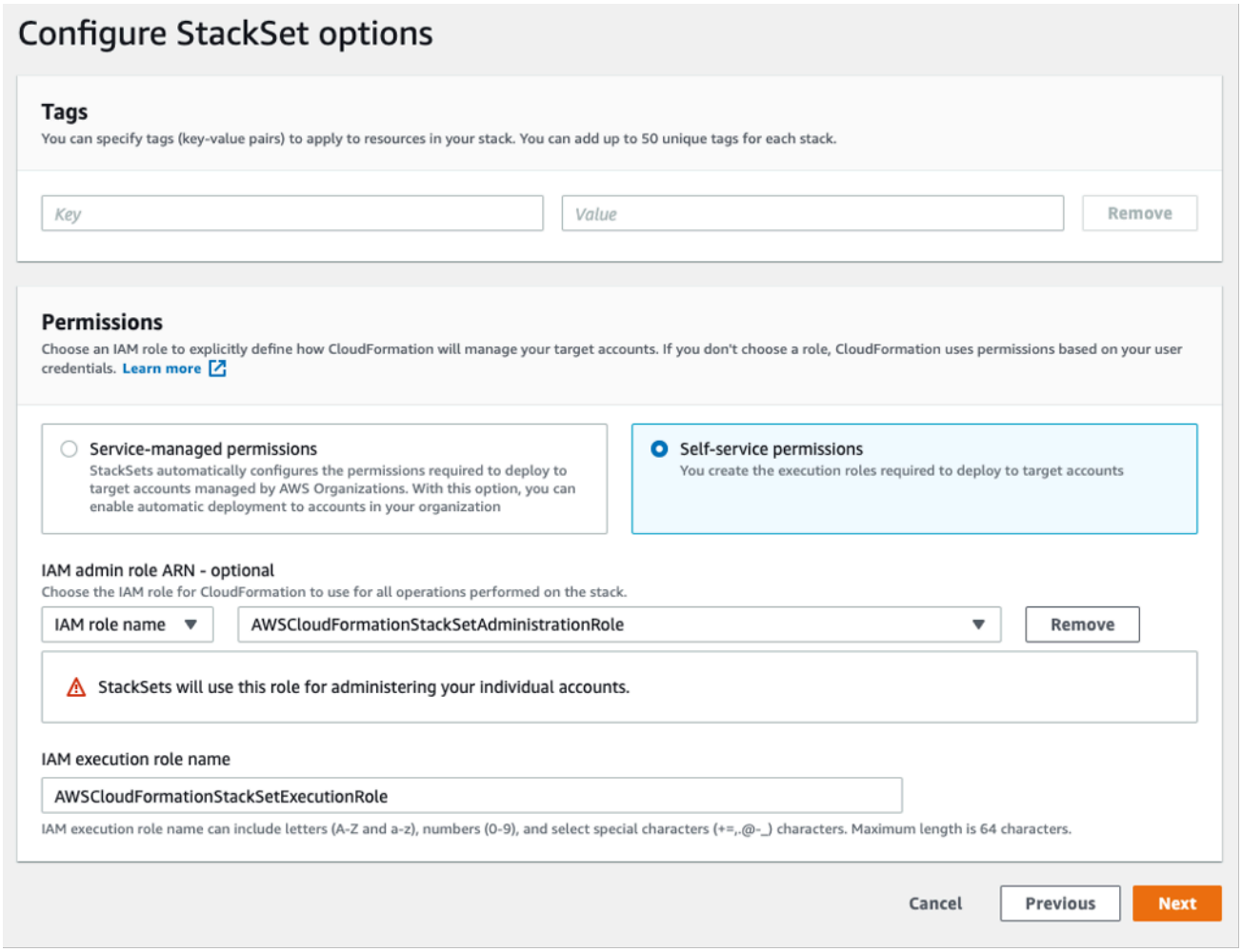


사용자 지정 통합 스택을 생성하려면: 솔루션 오케스트레이터 Step Functions가 각 문제 해결에 대해 호출할 수 있는 Lambda 함수를 포함합니다. Lambda 함수는 Step Functions에서 제공하는 입력을 받아 티켓팅 시스템의 요구 사항에 따라 페이로드를 구성하고 시스템에 티켓을 생성하도록 요청해야 합니다.

1단계: 위임된 Security Hub 관리자 계정에서 관리자 스택 시작

1. Security Hub 관리자 계정으로 관리자 스택 `automated-security-response-admin.template`를 시작합니다. 일반적으로 단일 리전의 조직당 하나씩. 이 스택은 중첩 스택을 사용하므로이 템플릿을 자체 관리형 StackSet로 배포해야 합니다.

StackSet 옵션 구성



2. 계정 번호 파라미터에 AWS Security Hub 관리자 계정의 계정 ID를 입력합니다.
3. 리전 지정 파라미터에서 Security Hub 관리자가 켜져 있는 리전만 선택합니다. 2단계로 넘어가기 전에이 단계가 완료될 때까지 기다립니다.

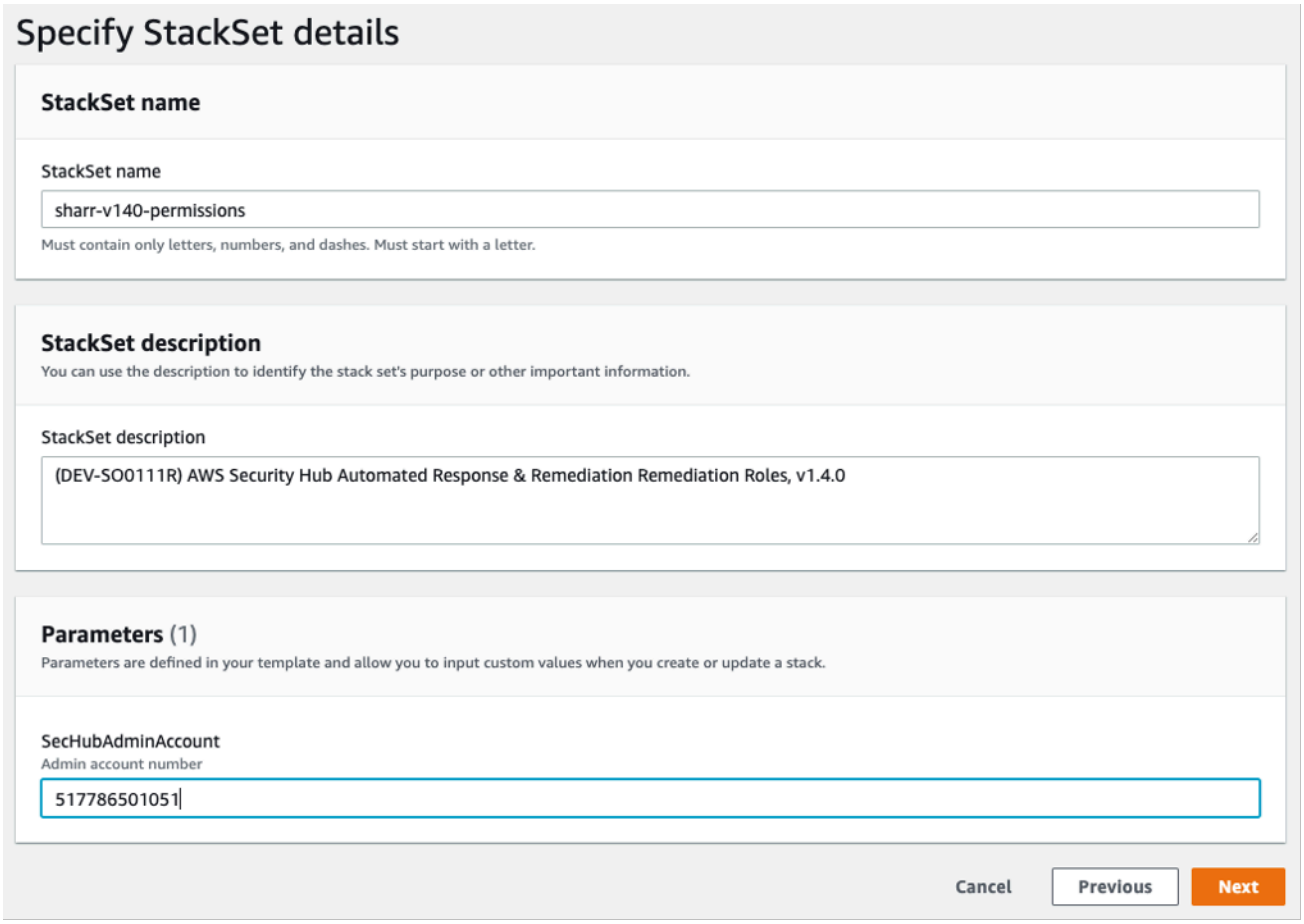
2단계: 각 AWS Security Hub 멤버 계정에 문제 해결 역할 설치

서비스 관리형 StackSets를 사용하여 멤버 역할 템플릿인를 배포합니다`automated-security-response-member-roles.template`. 이 StackSet는 멤버 계정당 하나의 리전에 배포해야 합니다. ASR Orchestrator 단계 함수에서 교차 계정 API 호출을 허용하는 전역 역할을 정의합니다.

1. 조직 정책에 따라 전체 조직(일반) 또는 조직 단위에 배포합니다.
2. AWS Organizations의 새 계정이 이러한 권한을 받도록 자동 배포를 켭니다.

3. 리전 지정 파라미터에서 단일 리전을 선택합니다. IAM 역할은 전역적입니다. 이 StackSet가 배포되는 동안 3단계로 계속 진행할 수 있습니다.

StackSet 세부 정보 지정



3단계: 각 AWS Security Hub 멤버 계정 및 리전에서 멤버 스택 시작

멤버 스택은 중첩 스택을 사용하기 때문에 자체 관리형 StackSet로 배포해야 합니다. AWS Organization의 새 계정에 대한 자동 배포는 지원하지 않습니다.

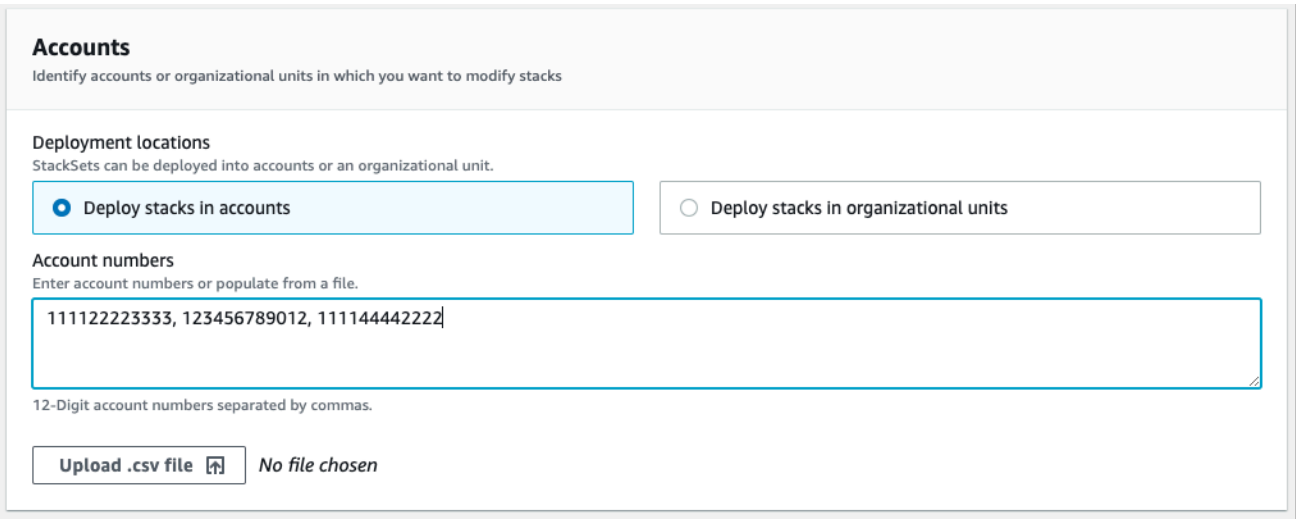
파라미터

LogGroup 구성: CloudTrail 로그를 수신하는 로그 그룹을 선택합니다. 존재하지 않거나 로그 그룹이 계정마다 다른 경우 편리한 값을 선택합니다. 계정 관리자는 CloudTrail 로그에 대한 CloudWatch Logs 그룹을 생성한 후 Systems Manager - Parameter Store /Solutions/SO0111/Metrics_LogGroupName 파라미터를 업데이트해야 합니다. 이는 API 호출 시 지표 경보를 생성하는 문제 해결에 필요합니다.

표준: 멤버 계정에 로드할 표준을 선택합니다. 이렇게 하면 AWS Systems Manager 런북만 설치되며 보안 표준은 활성화되지 않습니다.

SecHubAdminAccount: 솔루션의 관리자 템플릿을 설치한 AWS Security Hub 관리자 계정의 계정 ID를 입력합니다.

Accounts(계정)



배포 위치: 계정 번호 또는 조직 단위 목록을 지정할 수 있습니다.

리전 지정: 조사 결과를 수정할 모든 리전을 선택합니다. 계정 및 리전 수에 맞게 배포 옵션을 조정할 수 있습니다. 리전 동시성은 병렬일 수 있습니다.

자동 배포 - 스택

> **Note**
>
> 다중 계정 고객의 경우 StackSets를 사용하여 배포하는 것이 좋습니다.

솔루션을 시작하기 전에이 가이드에서 설명하는 아키텍처, 솔루션 구성 요소, 보안 및 설계 고려 사항을 검토하세요. 이 섹션의 step-by-step 지침에 따라 솔루션을 구성하고 계정에 배포합니다.

배포 시간: 약 30분

사전 조건

이 솔루션을 배포하기 전에 AWS Security Hub가 기본 및 보조 계정과 동일한 AWS 리전에 있는지 확인합니다. 이전에이 솔루션을 배포한 경우 기존 솔루션을 제거해야 합니다. 자세한 내용은 솔루션 업데이트를 참조하세요.

배포 개요

다음 단계에 따라이 솔루션을 AWS에 배포합니다.

(선택 사항) 0단계: 티켓 시스템 통합 스택 시작

- 티켓팅 기능을 사용하려는 경우 먼저 티켓팅 통합 스택을 Security Hub 관리자 계정에 배포합니다.
- 이 스택에서 Lambda 함수 이름을 복사하여 관리자 스택에 입력으로 제공합니다(1단계 참조).

1단계: 관리자 스택 시작

- `automated-security-response-admin.template` AWS Security Hub 관리자 계정으로 AWS CloudFormation 템플릿을 시작합니다.
- 설치할 보안 표준을 선택합니다.
- 사용할 기존 Orchestrator 로그 그룹을 선택합니다(이전 설치에서 `SO0111-ASR-Orchestrator` 이미 존재하는 `Yes` 경우 선택).

2단계: 각 AWS Security Hub 멤버 계정에 문제 해결 역할 설치

- `automated-security-response-member-roles.template` AWS CloudFormation 템플릿을 멤버 계정당 하나의 리전으로 시작합니다.
- AWS Security Hub 관리자 계정의 12자리 계정 IG를 입력합니다.

3단계: 멤버 스택 시작

- CIS 3.1-3.14 문제 해결에 사용할 CloudWatch Logs 그룹의 이름을 지정합니다. CloudTrail 로그를 수신하는 CloudWatch Logs 로그 그룹의 이름이어야 합니다.
- 문제 해결 역할을 설치할지 여부를 선택합니다. 이러한 역할은 계정당 한 번만 설치합니다.
- 설치할 플레이북을 선택합니다.
- AWS Security Hub 관리자 계정의 계정 ID를 입력합니다.

[4단계: (선택 사항) 사용 가능한 수정 사항 조정]

- 멤버 계정별로 수정 사항을 제거합니다. 이 단계는 선택 사항입니다.

(선택 사항) 0단계: 티켓 시스템 통합 스택 시작

1. 티켓팅 기능을 사용하려는 경우 먼저 각 통합 스택을 시작합니다.
2. Jira 또는 ServiceNow에 대해 제공된 통합 스택을 선택하거나 이를 블루프린트로 사용하여 사용자 지정 통합을 구현합니다.

   Jira 스택을 배포하려면:

   a. 스택의 이름을 입력합니다.

   b. Jira 인스턴스에 URI를 제공합니다.

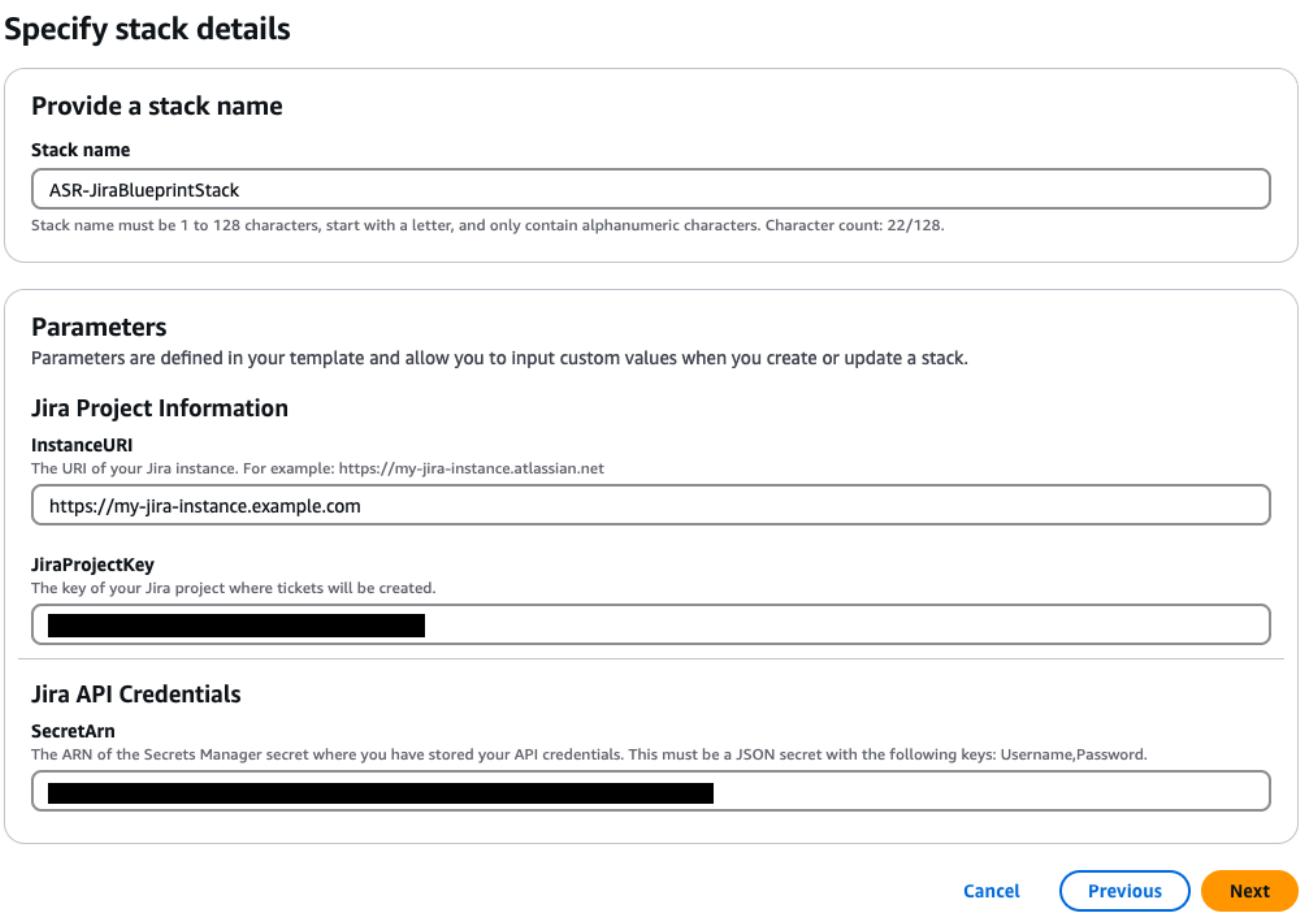
   c. 티켓을 보내려는 Jira 프로젝트의 프로젝트 키를 제공합니다.

   d. Secrets Manager에서 Jira `Username` 및를 포함하는 새 키-값 보안 암호를 생성합니다`Password`.

   > **Note**
   >
   > 사용자 이름을 로`Username`, API 키를 로 제공하여 암호 대신 Jira API 키를 사용하도록 선택할 수 있습니다`Password`.

   e. 이 보안 암호의 ARN을 스택에 입력으로 추가합니다.

   “스택 이름 Jira 프로젝트 정보와 Jira API 자격 증명을 제공합니다.



ServiceNow 스택을 배포하려면:

f. 스택의 이름을 입력합니다.

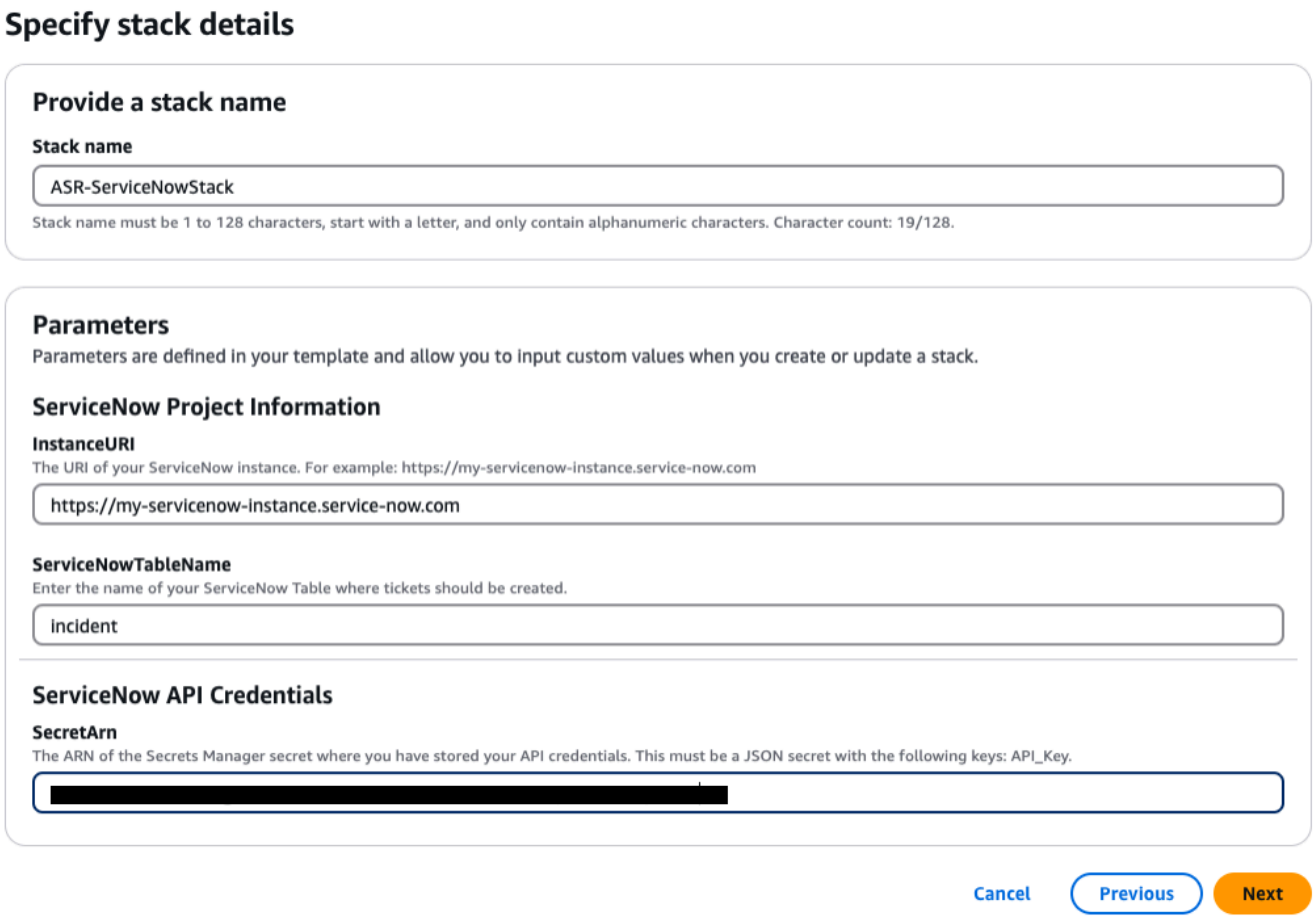
g. ServiceNow 인스턴스의 URI를 제공합니다.

h. ServiceNow 테이블 이름을 입력합니다.

i. 작성하려는 테이블을 수정할 수 있는 권한이 있는 API 키를 ServiceNow에 생성합니다.

j. 키를 사용하여 Secrets Manager에서 보안 암호를 `API_Key` 생성하고 보안 암호 ARN을 스택에 대한 입력으로 제공합니다.

스택 이름 ServiceNow 프로젝트 정보와 ServiceNow API 자격 증명을 제공합니다.



사용자 지정 통합 스택을 생성하려면: 솔루션 오케스트레이터 Step Functions가 각 문제 해결에 대해 호출할 수 있는 Lambda 함수를 포함합니다. Lambda 함수는 Step Functions에서 제공하는 입력을 받아 티켓팅 시스템의 요구 사항에 따라 페이로드를 구성하고 시스템에 티켓을 생성하도록 요청해야 합니다.

1단계: 관리자 스택 시작

> **Important**
>
> 이 솔루션에는 익명화된 운영 지표를 AWS로 전송하는 옵션이 포함되어 있습니다. 당사는 이 데이터를 사용하여 고객이 이 솔루션과 관련 서비스 및 제품을 어떻게 사용하는지 더 잘 이해합니다. AWS는이 설문 조사를 통해 수집된 데이터를 소유합니다. 데이터 수집에는 AWS 개인 정보 보호 고지가 적용됩니다.

이 기능을 옵트아웃하려면 템플릿을 다운로드하고 AWS CloudFormation 매핑 섹션을 수정한 다음 AWS CloudFormation 콘솔을 사용하여 템플릿을 업로드하고 솔루션을 배포합니다. 자세한 내용은이 가이드의 익명화된 데이터 수집 섹션을 참조하세요.

이 자동화된 AWS CloudFormation 템플릿은 AWS 클라우드의 AWS 솔루션에서 자동 보안 응답을 배포합니다. 스택을 시작하기 전에 Security Hub를 활성화하고 사전 조건을 완료해야 합니다.

> **Note**
>
> 이 솔루션을 실행하는 동안 사용되는 AWS 서비스의 비용은 사용자의 책임입니다. 자세한 내용은이 가이드의 비용 섹션을 참조하고이 솔루션에 사용되는 각 AWS 서비스의 요금 웹 페이지를 참조하세요.

1. AWS Security Hub가 현재 구성된 계정에서 AWS Management Console에 로그인하고 아래 버튼을 사용하여 `automated-security-response-admin.template` AWS CloudFormation 템플릿을 시작합니다.

   Launch solution

   또한 구현의 시작점으로 사용할 템플릿을 다운로드할 수도 있습니다.
2. 이 템플릿은 기본적으로 미국 동부(버지니아 북부) 리전에서 시작됩니다. 다른 AWS 리전에서이 솔루션을 시작하려면 AWS Management Console 탐색 모음에서 리전 선택기를 사용합니다.

   > **Note**
   >
   > 이 솔루션은 현재 특정 AWS 리전에서만 사용할 수 있는 AWS Systems Manager를 사용합니다. 이 솔루션은이 서비스를 지원하는 모든 리전에서 작동합니다. 리전별 최신 가용성은 AWS 리전 서비스 목록을 참조하세요.
3. 스택 생성 페이지에서 Amazon S3 URL 텍스트 상자에 올바른 템플릿 URL이 있는지 확인한 후 다음을 선택합니다.
4. 스택 세부 정보 지정 페이지에서 솔루션 스택 이름을 할당합니다. 문자 제한 이름 지정에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 및 STS 제한을 참조하세요.
5. 파라미터 페이지에서 다음을 선택합니다.

파라미터	Default	설명
SC 관리자 스택 로드	yes	SC 제어의 자동 문제 해결을 위해 관리자 구성 요소를 설치할지 여부를 지정합니다.
AFSBP 관리자 스택 로드	no	FSBP 제어의 자동 문제 해결을 위해 관리자 구성 요소를 설치할지 여부를 지정합니다.
CIS120 관리자 스택 로드	no	CIS120 제어의 자동 문제 해결을 위해 관리자 구성 요소를 설치할지 여부를 지정합니다.
CIS140 관리자 스택 로드	no	CIS140 제어의 자동 문제 해결을 위해 관리자 구성 요소를 설치할지 여부를 지정합니다.
CIS300 관리자 스택 로드	no	CIS300 제어의 자동 문제 해결을 위해 관리자 구성 요소를 설치할지 여부를 지정합니다.
PC1321 관리자 스택 로드	no	PC1321 제어의 자동 문제 해결을 위해 관리자 구성 요소를 설치할지 여부를 지정합니다.
NIST 관리자 스택 로드	no	NIST 제어의 자동 문제 해결을 위해 관리자 구성 요소를 설치할지 여부를 지정합니다.

파라미터	Default	설명
오케스트레이터 로그 그룹 재사용	no	기존 SO0111-ASR-Orchestrator CloudWatch Logs 그룹을 재사용할지 여부를 선택합니다. 이렇게 하면 이전 버전의 로그 데이터가 손실되지 않고 재설치 및 업그레이드가 간소화됩니다. 이 계정의 이전 배포에서가 Orchestrator Log Group 여전히 존재하는 yes 경우 기존 Orchestrator Log Group 선택을 재사용하고, 그렇지 않으면를 재사용합니다no. v2.3.0 이전 버전에서 스택 업데이트를 수행하는 경우 no
CloudWatch 지표 사용	yes	솔루션 모니터링을 위해 CloudWatch 지표를 활성화할지 여부를 지정합니다. 그러면 지표를 볼 수 있는 CloudWatch 대시보드가 생성됩니다.
CloudWatch 지표 경보 사용	yes	솔루션에 대해 CloudWatch 지표 경보를 활성화할지 여부를 지정합니다. 이렇게 하면 솔루션에서 수집한 특정 지표에 대한 경보가 생성됩니다.

파라미터	Default	설명
RemediationFailure AlarmThreshold	5	제어 ID당 문제 해결 실패 비율에 대한 임계값을 지정합니다. 예를 들어를 입력하면 지정된 날짜에 제어 ID가 문제 해결의 5% 이상 실패하면 경보가 5발생합니다. 이 파라미터는 경보가 생성된 경우에만 작동합니다 (CloudWatch 지표 경보 사용 파라미터 참조).
EnableEnhancedClou dWatchMetrics	no	yes인 경우는 추가 CloudWatch 지표를 생성하여 CloudWatch 대시보드에서 모든 제어 IDs 개별적으로 추적하고 CloudWatch 경보로 추적합니다. 이 경우 발생하는 추가 비용을 이해하려면 비용 섹션을 참조하세요.
TicketGenFunctionName	(선택 사항 입력)	선택 사항. 티켓팅 시스템을 통합하지 않으려면 비워 둡니다. 그렇지 않으면 0단계의 스택 출력에서 Lambda 함수 이름을 입력합니다. 예: `SO0111-ASR-Service Now-TicketGenerato r .`

파라미터	Default	설명
TargetAccountIDs	ALL	자동 문제 해결 범위를 제어하는 AWS 계정 IDs. "ALL"을 사용하여 조직의 모든 계정을 대상으로 지정합니다. 또는 12자리 AWS 계정 IDs의 쉼표로 구분된 목록을 제공합니다. 예: "123456789012,098765432109"
TargetAccountIDsStrategy	INCLUDE	솔루션이 TargetAccountIDs 목록을 기반으로 자동 문제 해결을 적용하는 방법을 정의합니다. INCLUDE: 나열된 계정에 대해서만 자동 문제 해결을 실행합니다. EXCLUDE: 나열된 계정을 제외한 모든 계정에 대해 자동 문제 해결을 실행합니다.

> **Note**
>
> 솔루션의 CloudFormation 스택을 배포하거나 업데이트한 후 관리자 계정에서 자동 문제 해결을 수동으로 활성화해야 합니다.

1. 스택 옵션 구성 페이지에서 다음을 선택합니다.
2. 검토 페이지에서 설정을 검토하고 확인합니다. 템플릿이 AWS Identity and Access Management(IAM) 리소스를 생성할 것임을 확인하는 확인란을 선택합니다.
3. [스택 생성(Create stack)]을 선택하여 스택을 배포합니다.

AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 볼 수 있습니다. 약 15분 후에 CREATE_COMPLETE 상태를 받게 됩니다.

2단계: 각 AWS Security Hub 멤버 계정에 문제 해결 역할 설치

`automated-security-response-member-roles.template` StackSet는 멤버 계정당 하나의 리전에만 배포해야 합니다. ASR Orchestrator 단계 함수에서 교차 계정 API 호출을 허용하는 전역 역할을 정의합니다.

1. 각 AWS Security Hub 멤버 계정(멤버이기도 한 관리자 계정 포함)의 AWS Management Console에 로그인합니다. 버튼을 선택하여 `automated-security-response-member-roles.template` AWS CloudFormation 템플릿을 시작합니다. 또한 구현의 시작점으로 사용할 템플릿을 다운로드할 수도 있습니다.

   Launch solution

2. 이 템플릿은 기본적으로 미국 동부(버지니아 북부) 리전에서 시작됩니다. 다른 AWS 리전에서이 솔루션을 시작하려면 AWS Management Console 탐색 모음에서 리전 선택기를 사용합니다.
3. 스택 생성 페이지에서 Amazon S3 URL 텍스트 상자에 올바른 템플릿 URL이 있는지 확인한 후 다음을 선택합니다.
4. 스택 세부 정보 지정 페이지에서 솔루션 스택 이름을 할당합니다. 문자 제한 이름 지정에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 및 STS 제한을 참조하세요.
5. 파라미터 페이지에서 다음 파라미터를 지정하고 다음을 선택합니다.

파라미터	Default	설명
네임스페이스	`<## ##>`	최대 9자의 소문자 영숫자로 구성된 문자열을 입력합니다. 수정 IAM 역할 이름에 접미사로 추가할 고유한 네임스페이스입니다. 멤버 역할 및 멤버 스택에서 동일한 네임스페이스를 사용해야 합니다. 이 문자열은 각 솔루션 배포마다 고유해야 하지만 스택 업데이트 중에는 변경할 필요가 없습니

파라미터	Default	설명
		다. 네임스페이스 값은 멤버 계정별로 고유할 필요가 없습니다.
Sec Hub 계정 관리자	<## ##>	AWS Security Hub 관리자 계정의 12자리 계정 ID를 입력합니다. 이 값은 관리자 계정의 솔루션 역할에 권한을 부여합니다.

6. 스택 옵션 구성 페이지에서 다음을 선택합니다.
7. 검토 페이지에서 설정을 검토하고 확인합니다. 템플릿이 AWS Identity and Access Management(IAM) 리소스를 생성할 것임을 확인하는 확인란을 선택합니다.
8. [스택 생성(Create stack)]을 선택하여 스택을 배포합니다.

   AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 볼 수 있습니다. 약 5분 후에 CREATE_COMPLETE 상태를 받게 됩니다. 이 스택이 로드되는 동안 다음 단계를 계속할 수 있습니다.

3단계: 멤버 스택 시작

> **Important**
>
> 이 솔루션에는 익명화된 운영 지표를 AWS로 전송하는 옵션이 포함되어 있습니다. 당사는 이 데이터를 사용하여 고객이 이 솔루션과 관련 서비스 및 제품을 어떻게 사용하는지 더 잘 이해합니다. AWS는이 설문 조사를 통해 수집된 데이터를 소유합니다. 데이터 수집에는 AWS 개인 정보 취급방침이 적용됩니다.
>
> 이 기능을 옵트아웃하려면 템플릿을 다운로드하고 AWS CloudFormation 매핑 섹션을 수정한 다음 AWS CloudFormation 콘솔을 사용하여 템플릿을 업로드하고 솔루션을 배포합니다. 자세한 내용은이 가이드의 운영 지표 수집 섹션을 참조하세요.

`automated-security-response-member` 스택은 각 Security Hub 멤버 계정에 설치해야 합니다. 이 스택은 자동 문제 해결을 위한 실행서를 정의합니다. 각 멤버 계정의 관리자는이 스택을 통해 사용할 수 있는 문제 해결을 제어할 수 있습니다.

1. 각 AWS Security Hub 멤버 계정(멤버이기도 한 관리자 계정 포함)의 AWS Management Console에 로그인합니다. 버튼을 선택하여 `automated-security-response-member.template` AWS CloudFormation 템플릿을 시작합니다.

템플릿을 자체 구현의 시작점으로 다운로드할 수도 있습니다. 이 템플릿은 기본적으로 미국 동부(버지니아 북부) 리전에서 시작됩니다. 다른 AWS 리전에서이 솔루션을 시작하려면 AWS Management Console 탐색 모음에서 리전 선택기를 사용합니다.

+

> **Note**
>
> 이 솔루션은 현재 대부분의 AWS 리전에서 사용할 수 있는 AWS Systems Manager를 사용합니다. 이 솔루션은 이러한 서비스를 지원하는 모든 리전에서 작동합니다. 리전별 최신 가용성은 AWS 리전 서비스 목록을 참조하세요.

1. 스택 생성 페이지에서 Amazon S3 URL 텍스트 상자에 올바른 템플릿 URL이 있는지 확인한 후 다음을 선택합니다.
2. 스택 세부 정보 지정 페이지에서 솔루션 스택 이름을 할당합니다. 문자 제한 이름 지정에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 및 STS 제한을 참조하세요.
3. 파라미터 페이지에서 다음 파라미터를 지정하고 다음을 선택합니다.

파라미터	Default	설명
지표 필터 및 경보를 생성하는 데 사용할 LogGroup의 이름을 입력합니다.	`<## ##>`	CloudTrail이 API 호출을 로깅하는 CloudWatch Logs 그룹의 이름을 지정합니다. CloudTrail 이는 CIS 3.1-3.14 문제 해결에 사용됩니다.
SC 멤버 스택 로드	`yes`	SC 제어의 자동 문제 해결을 위해 멤버 구성 요소를 설치할지 여부를 지정합니다.

파라미터	Default	설명
AFSBP 멤버 스택 로드	no	FSBP 제어의 자동 문제 해결을 위해 멤버 구성 요소를 설치할지 여부를 지정합니다.
CIS120 멤버 스택 로드	no	CIS120 제어의 자동 문제 해결을 위해 멤버 구성 요소를 설치할지 여부를 지정합니다.
CIS140 멤버 스택 로드	no	CIS140 제어의 자동 문제 해결을 위해 멤버 구성 요소를 설치할지 여부를 지정합니다.
CIS300 멤버 스택 로드	no	CIS300 제어의 자동 문제 해결을 위해 멤버 구성 요소를 설치할지 여부를 지정합니다.
PC1321 멤버 스택 로드	no	PC1321 제어의 자동 문제 해결을 위해 멤버 구성 요소를 설치할지 여부를 지정합니다.
NIST 멤버 스택 로드	no	NIST 제어의 자동 문제 해결을 위해 멤버 구성 요소를 설치할지 여부를 지정합니다.
Redshift 감사 로깅을 위한 S3 버킷 생성	no	FSBP RedShift.4 문제 해결을 위해 S3 버킷을 생성해야 하는지 `yes` 선택합니다. S3 버킷 및 문제 해결에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 Redshift.4 문제 해결을 참조하세요.
Sec Hub 관리자 계정	`<## ##>`	AWS Security Hub 관리자 계정의 12자리 계정 ID를 입력합니다.

파라미터	Default	설명
네임스페이스	*<## ##>*	최대 9자의 소문자 영숫자로 구성된 문자열을 입력합니다. 이 문자열은 IAM 역할 이름 및 작업 로그 S3 버킷의 일부가 됩니다. 멤버 스택 배포와 멤버 역할 스택 배포에 동일한 값을 사용합니다. 문자열은 각 솔루션 배포마다 고유해야 하지만 스택 업데이트 중에는 변경할 필요가 없습니다.
EnableCloudTrailForASRActionLog	no	CloudWatch 대시보드에서 솔루션에서 수행한 관리 이벤트를 모니터링할yes지 선택합니다. 솔루션은를 선택하는 각 멤버 계정에 CloudTrail 추적을 생성합니다yes. 이 기능을 활성화하려면 AWS Organization에 솔루션을 배포해야 합니다. 이 경우 발생하는 추가 비용을 이해하려면 비용 섹션을 참조하세요.

4. 스택 옵션 구성 페이지에서 다음을 선택합니다.
5. 검토 페이지에서 설정을 검토하고 확인합니다. 템플릿이 AWS Identity and Access Management(IAM) 리소스를 생성할 것임을 확인하는 확인란을 선택합니다.
6. [스택 생성(Create stack)]을 선택하여 스택을 배포합니다.

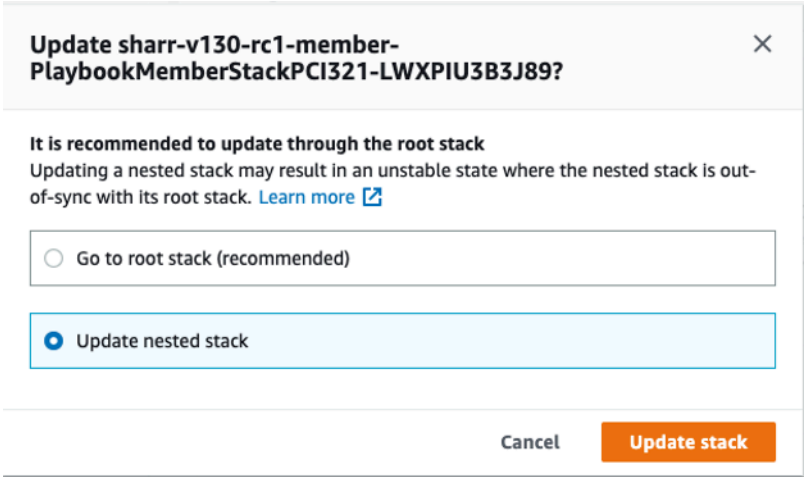
AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 볼 수 있습니다. 약 15분 후에 CREATE_COMPLETE 상태를 받게 됩니다.

4단계: (선택 사항) 사용 가능한 수정 사항 조정

멤버 계정에서 특정 수정 사항을 제거하려면 보안 표준에 대한 중첩 스택을 업데이트하면 됩니다. 간소화를 위해 중첩 스택 옵션은 루트 스택으로 전파되지 않습니다.

1. AWS CloudFormation 콘솔에 로그인하고 중첩 스택을 선택합니다.
2. 업데이트를 선택합니다.
3. 중첩 스택 업데이트를 선택하고 스택 업데이트를 선택합니다.

   중첩 스택 업데이트



4. 현재 템플릿 사용을 선택하고 다음을 선택합니다.
5. 사용 가능한 수정 사항을 조정합니다. 원하는 컨트롤의 값을 로 변경`Available`하고 원치 않는 컨트롤의 값을 로 변경합니다`Not available`.

> **Note**
>
> 문제 해결을 끄면 보안 표준 및 제어에 대한 솔루션 문제 해결 런북이 제거됩니다.

6. 스택 옵션 구성 페이지에서 다음을 선택합니다.
7. 검토 페이지에서 설정을 검토하고 확인합니다. 템플릿이 AWS Identity and Access Management(IAM) 리소스를 생성할 것임을 확인하는 확인란을 선택합니다.
8. 스택 업데이트를 선택합니다.

AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 볼 수 있습니다. 약 15분 후에 CREATE_COMPLETE 상태를 받게 됩니다.

Control Tower(CT) 배포

Customizations for AWS Control Tower(CfCT) 가이드는 회사 및 고객을 위해 AWS Control Tower 환경을 사용자 지정하고 확장하려는 관리자, DevOps 전문가, 독립 소프트웨어 개발 판매 회사, IT 인프라

아키텍트 및 시스템 통합 사업자를 위한 것입니다. 이 가이드는 CfCT 사용자 지정 패키지를 사용하여 AWS Control Tower 환경을 사용자 지정하고 확장하는 방법에 대한 정보를 제공합니다.

배포 시간: 약 30분

사전 조건

이 솔루션을 배포하기 전에 AWS Control Tower 관리자를 위한 솔루션인지 확인합니다.

AWS Control Tower 콘솔 또는 APIs를 사용하여 랜딩 존을 설정할 준비가 되면 다음 단계를 따르세요.

AWS Control Tower를 시작하려면 AWS Control Tower 시작하기를 참조하세요.

랜딩 존을 사용자 지정하는 방법을 알아보려면 다음을 참조하세요. 랜딩 존 사용자 지정

랜딩 존을 시작하고 배포하려면 랜딩 존 배포 가이드를 참조하세요.

배포 개요

다음 단계에 따라이 솔루션을 AWS에 배포합니다.

1단계: S3 버킷 빌드 및 배포

> **Note**
>
> S3 버킷 구성 - ADMIN 전용입니다. 이 단계는 일회성 설정 단계이므로 최종 사용자가 반복해서는 안 됩니다. S3 버킷은 ASR을 실행하는 데 필요한 AWS CloudFormation 템플릿 및 Lambda 코드를 포함하여 배포 패키지를 저장합니다. 이러한 리소스는 CfCt 또는 StackSet를 사용하여 배포됩니다.

1. S3 버킷 구성

배포 패키지를 저장하고 제공하는 데 사용할 S3 버킷을 설정합니다.

2. 환경 설정

빌드 및 배포 프로세스에 필요한 환경 변수, 자격 증명 및 도구를 준비합니다.

3. S3 버킷 정책 구성

적절한 버킷 정책을 정의하고 적용하여 액세스 및 권한을 제어합니다.

4. 빌드 준비

배포를 위해 애플리케이션 또는 자산을 컴파일, 패키징 또는 준비합니다.

5. S3에 패키지 배포

준비된 빌드 아티팩트를 지정된 S3 버킷에 업로드합니다.

2단계: AWS Control Tower에 배포 스택

1. ASR 구성 요소에 대한 빌드 매니페스트 생성

모든 ASR 구성 요소, 해당 버전, 종속성 및 빌드 지침을 나열하는 빌드 매니페스트를 정의합니다.

2. CodePipeline 업데이트

ASR 구성 요소를 배포하는 데 필요한 새 빌드 단계, 아티팩트 또는 단계를 포함하도록 AWS CodePipeline 구성을 수정합니다.

1단계: S3 버킷 빌드 및 배포

AWS 솔루션은 HTTPS를 통해 액세스하는 템플릿에 대한 글로벌 액세스를 위한 버킷과 Lambda 코드와 같은 리전 내 자산에 액세스하기 위한 리전 버킷이라는 두 개의 버킷을 사용합니다.

1. S3 버킷 구성

asr-staging과 같은 고유한 버킷 이름을 선택합니다. 터미널에 두 개의 환경 변수를 설정합니다. 하나는 참조가 접미사이고 다른 하나는 의도한 배포 리전이 접미사인 기본 버킷 이름이어야 합니다.

```
export BASE_BUCKET_NAME=asr-staging-$(date +%s)
export TEMPLATE_BUCKET_NAME=$BASE_BUCKET_NAME-reference
export REGION=us-east-1
export ASSET_BUCKET_NAME=$BASE_BUCKET_NAME-$REGION
```

2. 환경 설정

AWS 계정에서 asr-staging-reference 및 asr-staging-us-east-1과 같은 이름으로 두 개의 버킷을 생성합니다. (참조 버킷에는 CloudFormation 템플릿이 저장되고 리전 버킷에는 Lambda 코드 번들과 같은 다른 모든 자산이 저장됩니다.) 버킷은 암호화되어야 하며 퍼블릭 액세스를 허용하지 않아야 합니다.

```
aws s3 mb s3://$TEMPLATE_BUCKET_NAME/
```

```
aws s3 mb s3://$ASSET_BUCKET_NAME/
```

> **Note**
>
> 버킷을 생성할 때 버킷에 공개적으로 액세스할 수 없는지 확인합니다. 무작위 버킷 이름을 사용합니다. 퍼블릭 액세스를 비활성화합니다. KMS 암호화를 사용합니다. 그리고 업로드하기 전에 버킷 소유권을 확인합니다.

3. S3 버킷 정책 설정

실행 계정 ID에 대한 PutObject 권한을 포함하도록 $TEMPLATE_BUCKET_NAME S3 버킷 정책을 업데이트합니다. 버킷에 쓸 수 있는 권한이 있는 실행 계정 내의 IAM 역할에이 권한을 할당합니다. 이 설정을 사용하면 관리 계정에서 버킷을 생성하지 않아도 됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::<template bucket name>/*",
                "arn:aws:s3:::<template bucket name>"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "<org id>"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::<template bucket name>/*",
                "arn:aws:s3:::<template bucket name>"
            ],
            "Condition": {
                "ArnLike": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
            }
        }
    ]
}
```

권한을 포함하도록 자산 S3 버킷 정책을 변경합니다. 버킷에 쓸 수 있는 권한이 있는 실행 계정 내의 IAM 역할에이 권한을 할당합니다. 각 리전 자산 버킷(예: asr-staging-us-east-1, asr-staging-eu-west-1 등)에 대해이 설정을 반복하여 관리 계정에서 버킷을 생성할 필요 없이 여러 리전에 배포할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "<org id>"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
            "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
```

```
            }
        }
    ]
}
```

4. 빌드 준비

- 사전 조건:
  - AWS CLI v2
  - pip가 있는 Python 3.11 이상
  - AWS CDK 2.171.1 이상
  - npm을 사용하는 Node.js 20 이상
  - 내보낼 플러그인이 있는 Poetry v2
- Git 복제본 https://github.com/aws-solutions/automated-security-response-on-aws.git

먼저 소스 폴더에 npm 설치를 실행했는지 확인합니다.

복제된 리포지토리의 배포 폴더 옆에서 build-s3-dist.sh 실행하여 버킷의 루트 이름(예: mybucket)과 빌드 중인 버전(예: v1.0.0)을 전달합니다. GitHub에서 다운로드한 버전(예: GitHub: v1.0.0, 빌드: v1.0.0.mybuild)

```
chmod +x build-s3-dist.sh
export SOLUTION_NAME=automated-security-response-on-aws
export SOLUTION_VERSION=v1.0.0.mybuild
./build-s3-dist.sh -b $BASE_BUCKET_NAME -v $SOLUTION_VERSION
```

5. S3에 패키지 배포

```
cd deployment
aws s3 cp global-s3-assets/  s3://$TEMPLATE_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
aws s3 cp regional-s3-assets/  s3://$ASSET_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
```

2단계: AWS Control Tower에 배포 스택

1. ASR 구성 요소에 대한 매니페스트 빌드

S3 버킷에 ASR 아티팩트를 배포한 후 Control Tower 파이프라인 매니페스트를 업데이트하여 새 버전을 참조한 다음 파이프라인 실행을 트리거합니다. controltower 배포를 참조하세요.

> **Important**
>
> ASR 솔루션을 올바르게 배포하려면 CloudFormation 템플릿 개요 및 파라미터 설명에 대한 자세한 내용은 공식 AWS 설명서를 참조하세요. 아래 정보 링크: CloudFormation 템플릿 파라미터 개요 가이드

ASR 구성 요소의 매니페스트는 다음과 같습니다.

```
region: us-east-1 #<HOME_REGION_NAME>
version: 2021-03-15

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDsStrategy
        parameter_value: "INCLUDE"
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
```

```
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDs
        parameter_value: "ALL"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

  - name:  <ROLE MEMBER STACK NAME>
    resource_file: s3://<ROLE MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
    deploy_method: stack_set
    deployment_targets:
      organizational_units:
        - <ORG UNIT>

  - name:  <MEMBER STACK NAME>
    resource_file: s3://<MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: LoadCIS120MemberStack
        parameter_value: "no"
      - parameter_key: LoadNIST80053MemberStack
        parameter_value: "no"
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
      - parameter_key: CreateS3BucketForRedshiftAuditLogging
        parameter_value: "no"
      - parameter_key: LoadAFSBPMemberStack
        parameter_value: "no"
      - parameter_key: LoadSCMemberStack
```

```
      parameter_value: "yes"
    - parameter_key: LoadPCI321MemberStack
      parameter_value: "no"
    - parameter_key: LoadCIS140MemberStack
      parameter_value: "no"
    - parameter_key: EnableCloudTrailForASRActionLog
      parameter_value: "no"
    - parameter_key: LogGroupName
      parameter_value: <LOG_GROUP_NAME>
    - parameter_key: LoadCIS300MemberStack
      parameter_value: "no"
  deploy_method: stack_set
  deployment_targets:
   accounts: # :type: list
      - <ACCOUNT_NAME> # and/or
      - <ACCOUNT_NUMBER>
  organizational_units:
    - <ORG UNIT>
  regions: # :type: list
    - <REGION_NAME>
```

2. 코드 파이프라인 업데이트

custom-control-tower-configuration.zip에 매니페스트 파일을 추가하고 CodePipeline을 실행합니다. 코드 파이프라인 개요를 참조하세요.

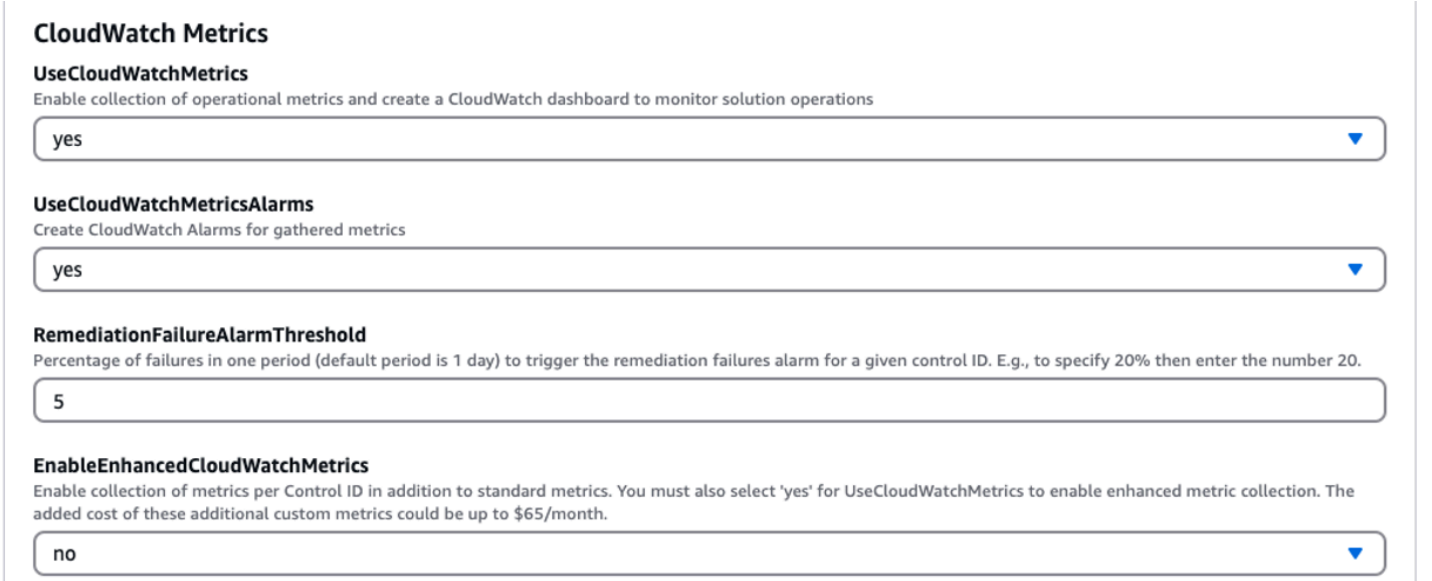
Amazon CloudWatch 대시보드를 사용하여 솔루션 작업 모니터링

이 솔루션에는 Amazon CloudWatch 대시보드에 표시되는 사용자 지정 지표 및 경보가 포함되어 있습니다.

CloudWatch 대시보드 및 경보는 잠재적인 문제가 있을 때 솔루션의 운영 및 알림을 모니터링합니다.

CloudWatch 지표, 경보 및 대시보드 활성화

CloudWatch 기능에는 네 가지 CloudFormation 템플릿 파라미터가 있습니다. CloudWatch



1. UseCloudWatchMetrics -이 값을 로 설정하면 운영 지표를 수집할 yes 수 있으며 CloudWatch 대시보드를 생성하여 이러한 지표를 볼 수 있습니다.
2. UseCloudWatchAlarms - 솔루션의 기본 경보를 yes 활성화하도록 설정합니다.
3. RemediationFailureAlarmThreshold - 경보를 발생시키기 위해 일정 기간 동안 해결에 실패한 비율입니다.
4. EnableEnhancedCloudWatchMetrics - 제어 ID당 개별 지표를 수집yes하려면이 파라미터를 로 설정합니다. 기본적으로이 파라미터는 로 설정no되므로 모든 제어 IDs의 총 문제 해결 수에 대한 지표만 수집됩니다. 제어 ID당 개별 지표 및 경보에는 추가 비용이 발생합니다.

CloudWatch 대시보드 사용

대시보드를 보려면

1. Amazon CloudWatch로 이동한 다음 대시보드로 이동합니다.
2. "ASR-Remediation-Metrics-Dashboard"라는 대시보드를 선택합니다.

CloudWatch 대시보드에는 다음 섹션이 포함되어 있습니다.

1. 총 성공적인 해결 - 솔루션으로 성공적으로 해결된 Security Hub 조사 결과 수에 대한 통찰력을 제공합니다.
2. 문제 해결 실패 - 총 및에서 실패한 문제 해결 횟수와 실패 원인을 백분율로 표시합니다. 실패 횟수가 많으면 솔루션의 기술적 문제를 더 자세히 조사해야 할 수 있습니다.
3. 제어 ID별 문제 해결 성공/실패 - 배포 시 향상된 지표를 활성화한 경우이 섹션에서는 제어 ID별로 문제 해결 결과를 나열합니다. 일반적으로 문제 해결 실패 섹션에 높은 실패율이 표시되면이 섹션에서는 실패가 여러 제어 IDs에 분산되어 있는지 또는 특정 제어 IDs만 실패하고 있는지 여부를 보여줍니다.
4. 실행서 역할 수임 실패 - 솔루션 멤버 역할이 설치되지 않은 계정의 문제 해결 시도로 인해 발생한 실패 수를 표시합니다. 역할 누락으로 인한 자동 문제 해결 시도로 인해 반복적으로 실패하면 불필요한 비용이 발생합니다. 관련 계정에 멤버 역할 스택을 설치하거나, 솔루션에서 생성한 모든 EventBridge 규칙을 비활성화하거나, Security Hub에서 계정의 연결을 해제하여 이를 완화합니다.
5. ASR별 Cloud Trail 관리 작업 - 배포 시 EnableCloudTrailForASRActionLog 파라미터를 사용하여 작업 로그를 활성화한 모든 멤버 계정의 솔루션별로 관리 작업을 나열합니다. AWS 계정에서 예기치 않은 리소스 변경이 관찰되면이 위젯을 통해 리소스가 솔루션에 의해 수정되었는지 파악할 수 있습니다.

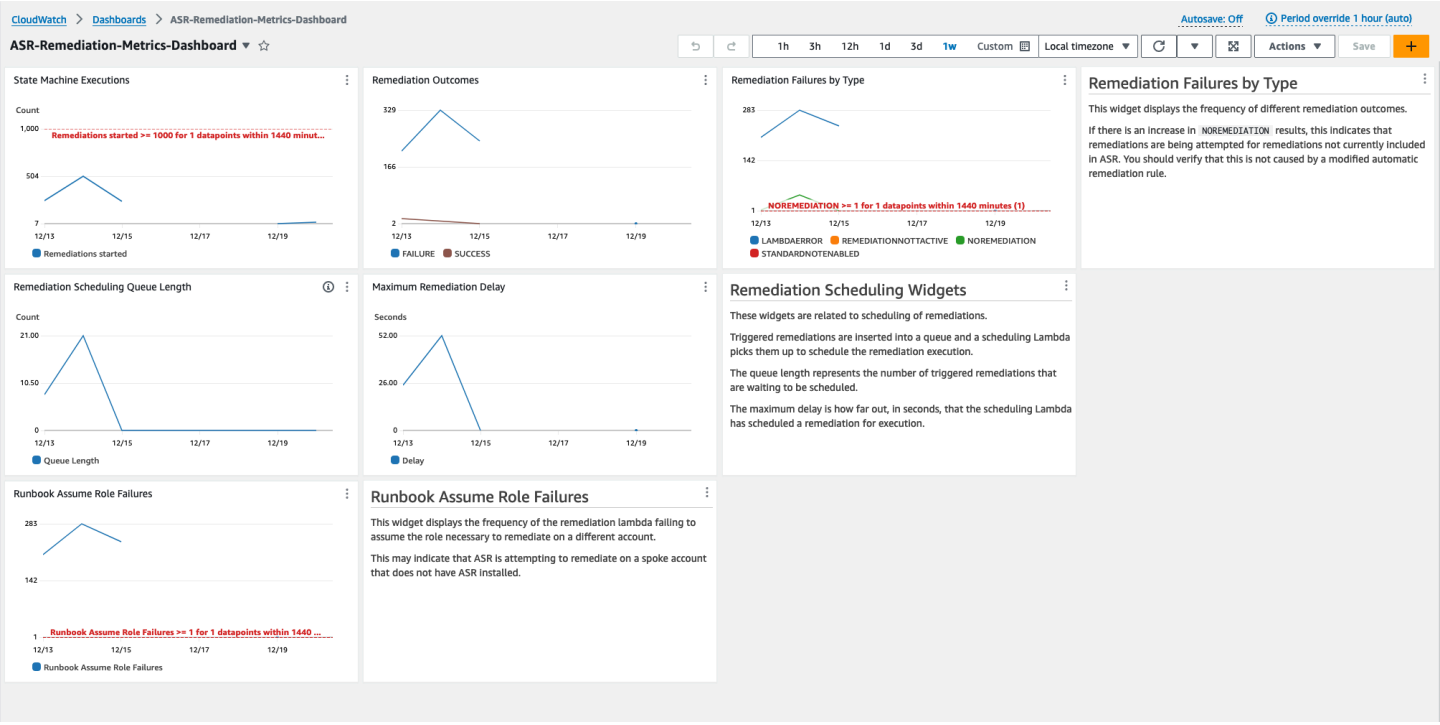
CloudWatch 대시보드에는 일반적인 운영 오류를 경고하는 사전 정의된 경보도 함께 제공됩니다.

1. 상태 시스템 실행은 24시간 동안 > 1000입니다.
   a. 문제 해결 실행이 크게 급증하면 이벤트 규칙이 의도한 것보다 더 자주 시작되고 있음을 나타낼 수 있습니다.
   b. CloudFormation 파라미터를 사용하여 임계값을 변경할 수 있습니다.
2. 유형별 문제 해결 실패 = 문제 해결 > 0
   a. ASR에 포함되지 않은 수정에 대한 수정을 시도하고 있습니다. 이는 이벤트 규칙이 의도한 문제 해결보다 더 많이 포함되도록 수정되었음을 나타낼 수 있습니다.

3. 런북 역할 수임 실패 > 0

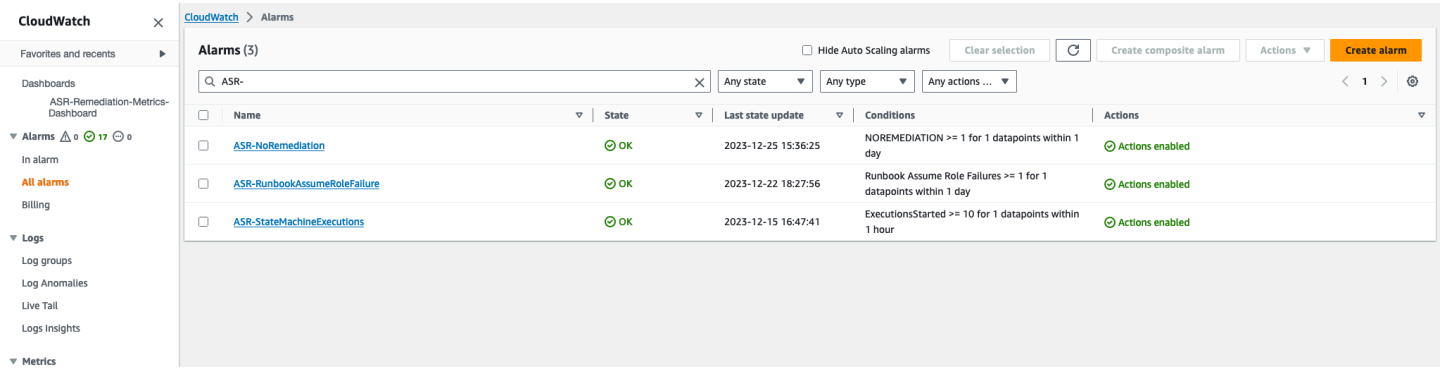
   a. 솔루션이 제대로 배포되지 않은 계정 또는 리전에서 문제 해결을 시도하고 있습니다. 이는 이벤트 규칙이 의도한 것보다 많은 계정을 포함하도록 수정되었음을 나타낼 수 있습니다.

모든 경보 임계값은 개별 배포 요구 사항에 맞게 수정할 수 있습니다.

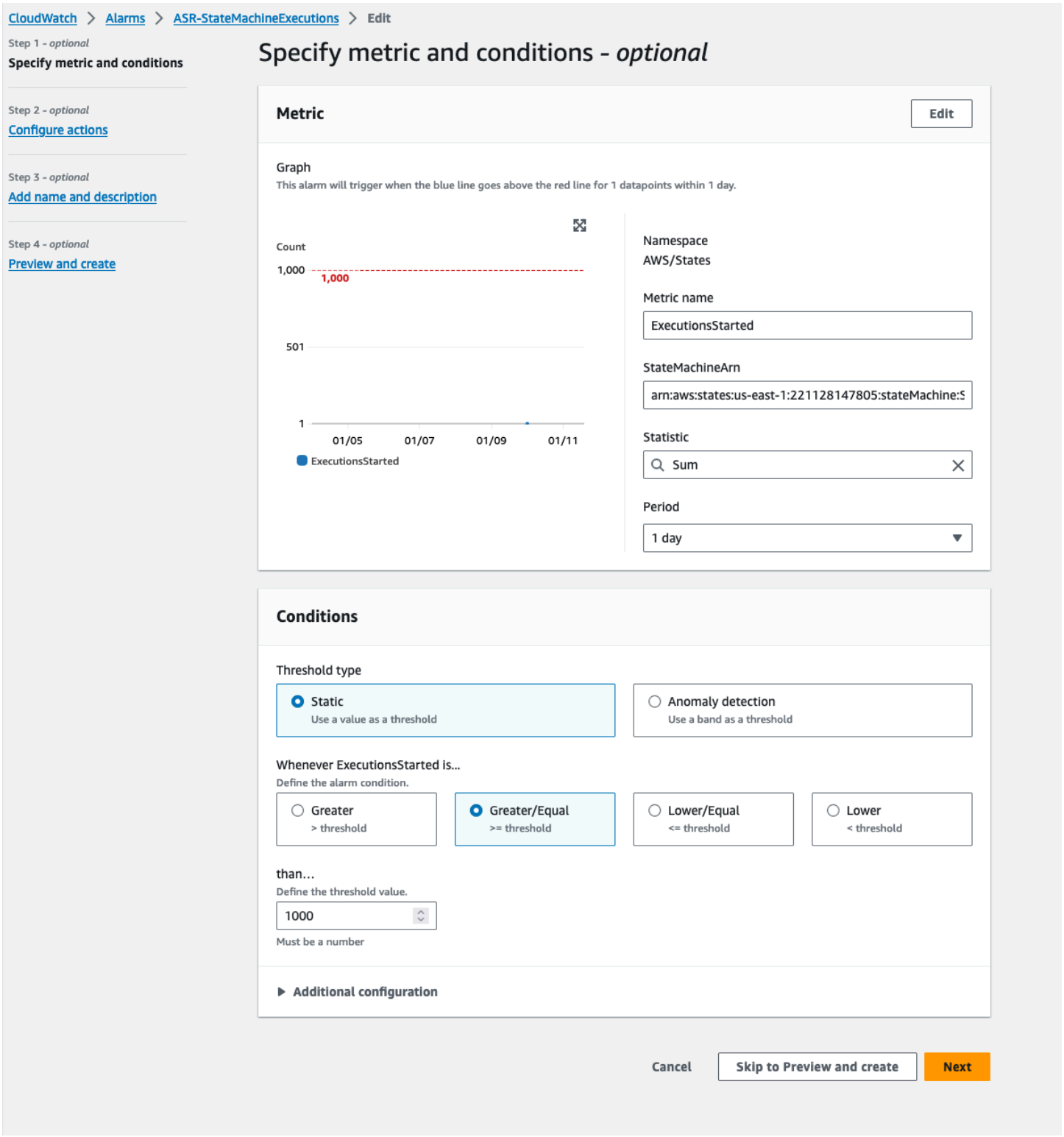


경보 임계값 수정

1. Amazon CloudWatch → 경보 → 모든 경보로 이동합니다.
2. 수정하려는 경보를 선택한 다음 작업 → 편집을 선택합니다.



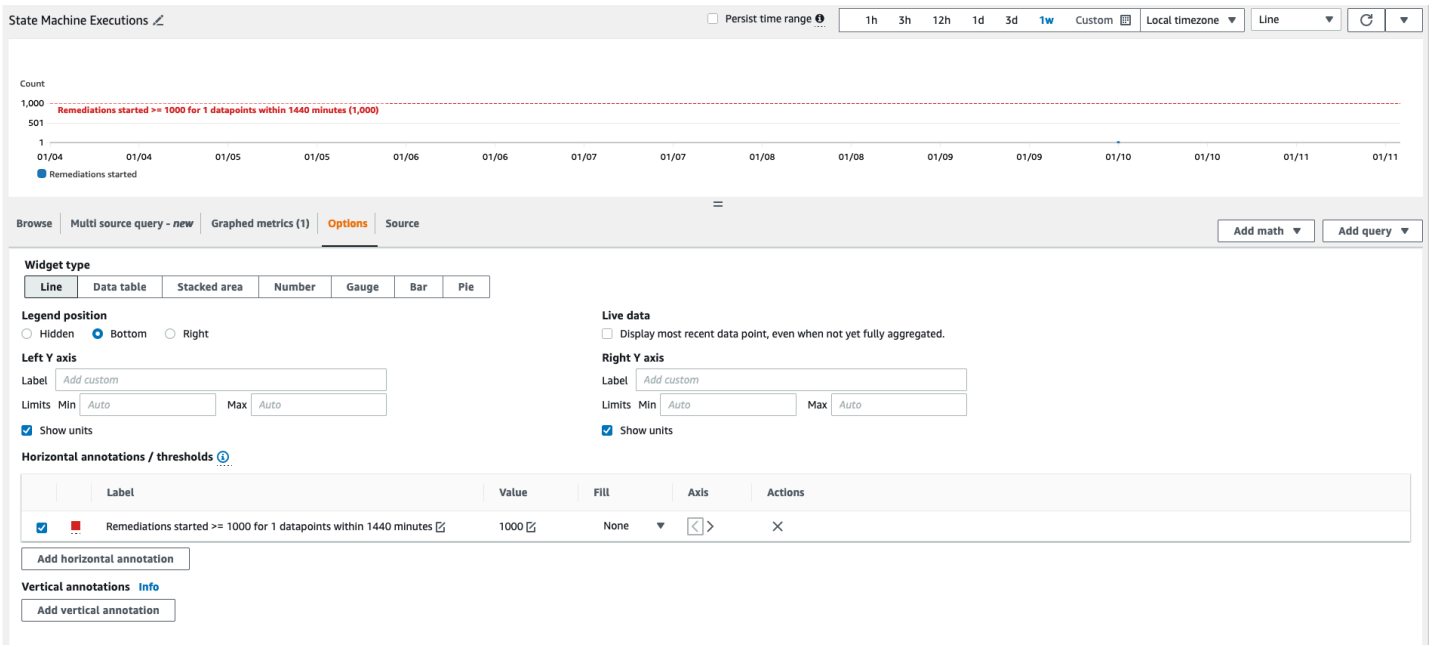
1. 임계값을 원하는 값으로 변경하고 저장합니다.



1. CloudWatch 대시보드로 이동하여 새 설정과 일치하도록 차트를 수정합니다.
   a. 해당 위젯의 오른쪽 상단에 있는 줄임표를 선택합니다.
   b. 편집을 선택합니다.

c. 옵션 탭으로 변경합니다.

d. 새 설정과 일치하도록 경보 주석을 수정합니다.



경보 알림 구독

관리자 계정에서 관리자 스택인 SO0111-ASR_Alarm_Topic에서 생성한 Amazon SNS 주제를 구독합니다. 그러면 경보가 ALARM 상태가 되면 알림을 받게 됩니다.

솔루션 업데이트

v1.4 이전 버전에서 업그레이드

이전에 v1.4.x 이전에 솔루션을 배포한 경우 제거한 다음 최신 버전을 설치합니다.

1. 이전에 배포한 솔루션을 제거합니다. 솔루션 제거를 참조하세요.
2. 최신 템플릿을 시작합니다. 솔루션 배포를 참조하세요.

> **Note**
>
> v1.2.1 이하에서 v1.3.0 이상으로 업그레이드하는 경우 기존 Orchestrator 로그 그룹 사용을로 설정합니다No. v1.3.0 이상을 다시 설치하는 경우이 옵션에 `Yes` 대해를 선택할 수 있습니다. 이 옵션을 사용하면 Orchestrator Step Functions에 대해 동일한 로그 그룹에 계속 로그인할 수 있습니다.

v1.4 이상에서 업그레이드

v1.4.x에서 업그레이드하는 경우 다음과 같이 모든 스택 또는 StackSets를 업데이트합니다.

1. 최신 템플릿을 사용하여 Security Hub 관리자 계정에서 스택을 업데이트합니다.
2. 각 멤버 계정에서 최신 템플릿의 권한을 업데이트합니다.
3. 현재 배포된 모든 리전의 각 멤버 계정에서 최신 템플릿에서 멤버 스택을 업데이트합니다.

v2.0.x에서 업그레이드

v2.0.x에서 업그레이드하는 경우 v2.1.2 이상으로 업그레이드합니다. v2.1.0 - v2.1.1로 업데이트하면 CloudFormation에서 실패합니다.

> **Note**
>
> - 솔루션을 업데이트할 때 관리자 계정에서 자동 문제 해결 규칙을 수동으로 다시 활성화해야 할 수 있습니다. 완전 자동화 문제 해결 활성화를 참조하세요.

- `Reuse Orchestrator Log Group` 파라미터를 사용하여 로그를 보존하는 경우 로그 그룹 재생성 또는 로그 보존 설정 손실을 방지하기 위해 스택 업데이트 중에 적절하게 설정되었는지 확인합니다. 솔루션 배포를 참조하세요. 이전 버전에서 v2.3.0+로 스택 업데이트를 수행하는 경우 "아니요"를 선택합니다.

문제 해결

알려진 문제 해결은 알려진 오류를 완화하기 위한 지침을 제공합니다. 이러한 지침으로 문제가 해결되지 않는 경우 AWS Support에 문의하세요.이 솔루션에 대한 AWS Support 사례를 개설하기 위한 지침을 제공합니다.

솔루션 로그

이 섹션에는이 솔루션에 대한 문제 해결 정보가 포함되어 있습니다. 주제는 왼쪽 탐색을 참조하세요.

이 솔루션은 AWS Systems Manager에서 실행되는 문제 해결 실행서의 출력을 수집하고 결과를 AWS Security Hub 관리자 계정S00111-ASR의 CloudWatch Logs 그룹에 로깅합니다. 하루에 제어당 하나의 스트림이 있습니다.

Orchestrator Step Functions는 AWS Security Hub 관리자 계정의 S00111-ASR-Orchestrator CloudWatch Logs 그룹으로의 모든 단계 전환을 기록합니다. 이 로그는 Step Functions의 각 인스턴스에 대한 상태 전환을 기록하는 감사 추적입니다. Step Functions 실행당 하나의 로그 스트림이 있습니다.

두 로그 그룹 모두 AWS KMS 고객 관리자 키(CMK)를 사용하여 암호화됩니다.

다음 문제 해결 정보는 S00111-ASR 로그 그룹을 사용합니다. 이 로그와 AWS Systems Manager Automation 콘솔, 자동화 실행 로그, Step Function 콘솔 및 Lambda 로그를 사용하여 문제를 해결합니다.

문제 해결에 실패하면 다음과 유사한 메시지가 표준, 제어 및 날짜에 대한 로그 스트림의 S00111-ASR에 로깅됩니다. 예: CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

다음 메시지는 추가 세부 정보를 제공합니다. 이 출력은 보안 표준 및 제어를 위한 ASR 실행서에서 가져온 것입니다. 예: ASR-CIS_1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

이 정보는 실패를 가리킵니다.이 경우 멤버 계정에서 실행되는 하위 자동화였습니다. 이 문제를 해결하려면 멤버 계정의 AWS Management Console에 로그인하고(위의 메시지에서), AWS Systems Manager로 이동하여 자동화로 이동하여 실행 ID에 대한 로그 출력을 검사해야 합니다`eecdef79-9111-4532-921a-e098549f525`.

알려진 문제 해결

- 문제: Amazon CloudWatch에서 리소스를 이미 사용할 수 있다는 오류와 함께 솔루션 배포가 실패합니다.

  해결 방법: CloudFormation 리소스/이벤트 섹션에서 로그 그룹이 이미 있음을 나타내는 오류 메시지가 있는지 확인합니다. ASR 배포 템플릿을 사용하면 기존 로그 그룹을 재사용할 수 있습니다. 재사용을 선택했는지 확인합니다.
- 문제: EventBridge 규칙이 생성되지 않는 플레이북 중첩 스택에 오류가 발생하여 솔루션이 배포되지 않음

  해결 방법: 배포된 플레이북 수와 함께 EventBridge 규칙의 할당량에 도달했을 수 있습니다. 이 솔루션의 SC 플레이북과 페어링된 Security Hub의 통합 제어 조사 결과를 사용하거나, 사용된 표준에 대한 플레이북만 배포하거나, EventBridge 규칙 할당량 증가를 요청하여 이를 방지할 수 있습니다.
- 문제: 동일한 계정의 여러 리전에서 Security Hub를 실행합니다. 이 솔루션을 여러 리전에 배포하려고 합니다.

  해결 방법: Security Hub 관리자와 동일한 계정 및 리전에 관리자 스택을 배포합니다. Security Hub 멤버가 구성된 각 계정 및 리전에 멤버 템플릿을 설치합니다. Security Hub에서 집계를 활성화합니다.
- 문제: 배포 직후 SO0111-ASR-Orchestrator가 Get Automation Document State에서 실패하고 502 오류가 발생했습니다. "`Lambda가 KMS 액세스가 거부되어 환경 변수를 해독할 수 없습니다. 함수의 KMS 키 설정을 확인하세요. KMS 예외: UnrecognizedClientExceptionKMS 메시지: 요청에 포함된 보안 토큰이 잘못되었습니다. (서비스: AWSLambda, 상태 코드: 502, 오류 코드: KMSAccessDeniedException, 요청 ID: ... `"

  해결 방법: 문제 해결을 실행하기 전에 솔루션이 안정화될 때까지 약 10분 정도 기다립니다. 문제가 계속되면 지원 티켓 또는 GitHub 문제를 엽니다.
- 문제: 조사 결과를 해결하려고 했지만 아무 일도 발생하지 않았습니다.

해결 방법: 조사 결과의 메모에서 해결되지 않은 이유를 확인합니다. 일반적인 원인은 결과에 자동 수정이 없기 때문입니다. 현재로서는 메모 이외의 해결 방법이 없는 경우 사용자에게 직접 피드백을 제공할 방법이 없습니다. 솔루션 로그를 검토합니다. 콘솔에서 CloudWatch Logs를 엽니다. SO0111-ASR CloudWatch Logs 그룹을 찾습니다. 가장 최근에 업데이트된 스트림이 먼저 표시되도록 목록을 정렬합니다. 실행을 시도한 결과의 로그 스트림을 선택합니다. 여기에서 오류를 찾아야 합니다. 실패의 몇 가지 이유는 조사 결과 제어와 문제 해결 제어 간의 불일치, 교차 계정 문제 해결(아직 지원되지 않음) 또는 조사 결과가 이미 해결된 경우일 수 있습니다. 실패 이유를 확인할 수 없는 경우 로그를 수집하고 지원 티켓을 여십시오.

- 문제: 문제 해결을 시작한 후 Security Hub 콘솔의 상태가 업데이트되지 않았습니다.

  해결 방법: Security Hub 콘솔은 자동으로 업데이트되지 않습니다. 현재 보기를 새로 고칩니다. 조사 결과의 상태가 업데이트되어야 합니다. 조사 결과가 실패에서 통과로 전환되는 데 몇 시간이 걸릴 수 있습니다. 결과는 AWS Config와 같은 다른 서비스에서 AWS Security Hub로 전송한 이벤트 데이터에서 생성됩니다. 규칙이 재평가되기까지의 시간은 기본 서비스에 따라 다릅니다. 이렇게 해도 문제가 해결되지 않으면 "`결과를 해결하려고 했지만 아무 일도 발생하지 않았습니다."에 대한 앞의 해결 방법을 참조하세요.

- 문제: 자동화 문서 상태 가져오기: AssumeRole 작업을 호출할 때 오류 발생(AccessDenied)에서 오케스트레이터 단계 함수가 실패합니다.

  해결 방법: ASR이 결과 해결을 시도하는 멤버 계정에 멤버 템플릿이 설치되지 않았습니다. 멤버 템플릿 배포 지침을 따릅니다.

- 문제: 레코더 또는 전송 채널이 이미 있으므로 Config.1 실행서가 실패합니다.

  해결 방법: AWS Config 설정을 주의 깊게 검사하여 Config가 올바르게 설정되었는지 확인합니다. 경우에 따라 자동 수정으로 기존 AWS Config 설정을 수정할 수 없습니다.

- 문제: 해결에 성공했지만 메시지를 반환합니다. `"No output available yet because the step is not successfully executed."`

  해결 방법:이 릴리스에서는 특정 문제 해결 실행서가 응답을 반환하지 않는 알려진 문제입니다. 문제 해결 실행서는 제대로 실패하고 작동하지 않으면 솔루션에 신호를 보냅니다.

- 문제: 해결에 실패하여 스택 추적을 전송했습니다.

  해결 방법: 때때로 오류 메시지가 아닌 스택 추적으로 이어지는 오류 조건을 처리할 기회를 놓치기도 합니다. 추적 데이터에서 문제를 해결하려고 시도합니다. 도움이 필요한 경우 지원 티켓을 엽니다.

- 문제: 사용자 지정 작업 리소스에서 v1.3.0 스택 제거에 실패했습니다.

해결 방법: 사용자 지정 작업 제거 시 관리자 템플릿을 제거하지 못할 수 있습니다. 이는 다음 릴리스에서 해결될 알려진 문제입니다. 이 경우:

a. AWS Security Hub 관리 콘솔에 로그인합니다.

b. 관리자 계정에서 설정으로 이동합니다.

c. 사용자 지정 작업 탭을 선택합니다.

d. ASR로 문제 해결 항목을 수동으로 삭제합니다.

e. 스택을 다시 삭제합니다.

- 문제: 관리자 스택을 재배포한 후에서 단계 함수가 실패합니다`AssumeRole`.

  해결 방법: 관리자 스택을 재배포하면 관리자 계정의 관리자 역할과 멤버 계정의 멤버 역할 간의 신뢰 연결이 끊어집니다. 모든 멤버 계정에서 멤버 역할 스택을 재배포해야 합니다.

- 문제: 24시간이 `PASSED` 지나면 CIS 3.x 수정 사항이 표시되지 않습니다.

  해결 방법: 멤버 계정에 `SO0111-ASR_LocalAlarmNotification` SNS 주제에 대한 구독이 없는 경우 일반적으로 발생합니다.

특정 문제 해결

AccessDenied 오류와 함께 SetSSLBucketPolicy 실패

관련 제어: AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI.S3.5, CIS v1.4.0 2.1.2, SC v2.0.0 S3.5

문제: AccessDenied 오류와 함께 SetSSLBucketPolicy가 실패합니다.

PutBucketPolicy 작업: 액세스 거부를 호출할 때 오류 발생(AccessDenied)

버킷에 대해 퍼블릭 액세스 차단 설정이 활성화된 경우는이 오류와 함께 퍼블릭 액세스를 허용하는 문이 포함된 버킷 정책을 입력하려고 시도합니다. 이러한 문이 포함된 버킷 정책을 적용한 다음 해당 버킷에 대한 퍼블릭 액세스 블록을 활성화하여이 상태에 도달할 수 있습니다.

ConfigureS3BucketPublicAccessBlock 문제 해결(관련 제어: AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI.S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2)도 버킷 정책을 변경하지 않고 퍼블릭 액세스 블록 설정을 설정하기 때문에 버킷을이 상태로 만들 수 있습니다.

SetSSLBucketPolicy는 버킷 정책에 문을 추가하여 SSL을 사용하지 않는 요청을 거부합니다. 정책의 다른 문은 수정하지 않으므로 퍼블릭 액세스를 허용하는 문이 있는 경우 수정은 해당 문이 여전히 포함된 수정된 버킷 정책 적용을 시도하지 못합니다.

해결 방법: 버킷의 퍼블릭 액세스 차단 설정과 충돌하여 퍼블릭 액세스를 허용하는 문을 제거하도록 버킷 정책을 수정합니다.

PutS3BucketPolicyDeny 실패

관련 제어: AWS FSBP v1.0.0 S3.6, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

문제: 다음 오류가 있는 PutS3BucketPolicyDeny:

```
Unable to create an explicit deny statement for {bucket_name}.
```

대상 버킷의 모든 정책에 대한 보안 주체가 "*"인 경우 솔루션은 모든 보안 주체에 대한 모든 버킷 작업을 차단하므로 대상 버킷에 거부 정책을 추가할 수 없습니다.

해결 방법: "*" 보안 주체를 사용하는 대신 특정 계정에 대한 작업을 허용하고 거부된 작업을 제한하도록 버킷 정책을 수정합니다.

솔루션을 비활성화하는 방법

인시던트가 발생하는 경우 인프라를 제거하지 않고 솔루션을 비활성화해야 할 수 있습니다. 이러한 시나리오에서는 솔루션에서 다양한 구성 요소를 비활성화하는 방법을 자세히 설명합니다.

시나리오 1: 단일 컨트롤에 대한 자동 문제 해결을 비활성화합니다.

1. AWS CloudFormation 콘솔에서 EventBridge로 이동합니다.
2. 사이드바에서 규칙을 선택합니다.
3. 기본 이벤트 버스를 선택하고 비활성화하려는 컨트롤을 검색합니다.
4. 규칙에서를 선택하고 비활성화 버튼을 선택합니다.

시나리오 2: 모든 제어에 대한 자동 문제 해결을 비활성화합니다.

1. 콘솔에서 EventBridge로 이동합니다.
2. 사이드바에서 규칙을 선택합니다.
3. "기본" 이벤트 버스를 선택하고 아래의 모든 규칙을 선택합니다.
4. "비활성화" 버튼에서를 선택합니다. 여러 규칙 페이지에 대해이 작업을 수행해야 할 수 있습니다.

시나리오 3: 계정에 대한 수동 문제 해결 비활성화

1. 콘솔에서 EventBridge로 이동합니다.
2. 사이드바에서 규칙을 선택합니다.
3. "기본" 이벤트 버스를 선택하고 "Remediate_with_ASR_CustomAction"을 검색합니다.
4. 규칙에서를 선택하고 "비활성화" 버튼을 선택합니다.

Support에 문의하세요.

AWS 개발자 지원, AWS 비즈니스 지원 또는 AWS 엔터프라이즈 지원이 있는 경우 지원 센터를 사용하여이 솔루션에 대한 전문가 지원을 받을 수 있습니다. 이후 단원에서는 그 방법에 대해서 설명합니다.

사례 생성

1. 지원 센터에 로그인합니다.
2. 사례 생성을 선택합니다.

어떻게 도와드릴까요?

1. 기술을 선택합니다.
2. 서비스에서 솔루션을 선택합니다.
3. 범주에서 기타 솔루션을 선택합니다.
4. 심각도에서 사용 사례에 가장 적합한 옵션을 선택합니다.
5. 서비스, 범주 및 심각도를 입력하면 인터페이스가 일반적인 문제 해결 질문에 대한 링크를 채웁니다. 이러한 링크로 질문을 해결할 수 없는 경우 다음 단계: 추가 정보를 선택합니다.

추가 정보

1. 제목에 질문 또는 문제를 요약하는 텍스트를 입력합니다.
2. 설명에서 문제를 자세히 설명합니다.
3. 파일 연결을 선택합니다.
4. Support에서 요청을 처리하는 데 필요한 정보를 첨부합니다.

사례를 더 빠르게 해결할 수 있도록 지원

1. 요청된 정보를 입력합니다.
2. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.

지금 해결하거나 문의하기

1. 지금 해결 솔루션을 검토합니다.
2. 이러한 솔루션과 관련된 문제를 해결할 수 없는 경우 문의하기를 선택하고 요청된 정보를 입력한 다음 제출을 선택합니다.

솔루션 제거

다음 절차에 따라 AWS Management Console을 사용하여 솔루션을 제거합니다.

V1.0.0-V1.2.1

릴리스 v1.0.0~v1.2.1의 경우 Service Catalog를 사용하여 CIS 및/또는 FSBP 플레이북을 제거합니다. v1.3.0에서는 Service Catalog가 더 이상 사용되지 않습니다.

1. AWS CloudFormation 콘솔에 로그인하고 Security Hub 기본 계정으로 이동합니다.
2. 서비스 카탈로그를 선택하여 프로비저닝된 플레이북을 종료하고 보안 그룹, 역할 또는 사용자를 제거합니다.
3. Security Hub 멤버 계정에서 스포크 `CISPermissions.template` 템플릿을 제거합니다.
4. Security Hub 관리자 및 멤버 계정에서 스포크 `AFSBPMemberStack.template` 템플릿을 제거합니다.
5. Security Hub 기본 계정으로 이동하여 솔루션의 설치 스택을 선택한 다음 삭제를 선택합니다.

> **Note**
>
> CloudWatch Logs 그룹 로그는 유지됩니다. 조직의 로그 보존 정책에 따라 이러한 로그를 보존하는 것이 좋습니다.

V1.3.x

1. 각 멤버 계정`automated-security-response-member.template`에서를 제거합니다.
2. 관리자 계정`automated-security-response-admin.template`에서를 제거합니다.

> **Note**
>
> v1.3.0에서 관리자 템플릿을 제거하면 사용자 지정 작업 제거 시 실패할 수 있습니다. 이는 다음 릴리스에서 해결될 알려진 문제입니다. 이 문제를 해결하려면 다음 지침을 따르십시오.
>
> 1. AWS Security Hub 관리 콘솔에 로그인합니다.
> 2. 관리자 계정에서 설정으로 이동합니다.

3. 사용자 지정 작업 탭을 선택합니다.
4. ASR로 문제 해결 항목을 수동으로 삭제합니다.
5. 스택을 다시 삭제합니다.

V1.4.0 이상

스택 배포

1. 각 멤버 계정`automated-security-response-member.template`에서를 제거합니다.
2. 관리자 계정`automated-security-response-admin.template`에서를 제거합니다.

StackSet 배포

각 StackSet에 대해 스택을 제거한 다음 배포의 역순으로 StackSet를 제거합니다.

템플릿`automated-security-response-member-roles.template`이 제거되더라도의 IAM 역할은 유지됩니다. 이렇게 하면 이러한 역할을 사용한 문제 해결이 계속 작동합니다. 이러한 SO0111-* 역할은 CloudTrail에서 CloudWatch로 로깅 또는 RDS Enhanced Monitoring과 같은 활성 문제 해결에서 더 이상 사용되지 않는지 확인한 후 수동으로 제거할 수 있습니다.

관리자 안내서

솔루션의 일부 활성화 및 비활성화

솔루션 관리자는 솔루션의 어떤 기능이 활성화되는지에 대해 다음과 같은 제어 기능을 사용할 수 있습니다.

멤버 및 멤버 역할 스택이 배포되는 위치:

- 관리자 스택은 파라미터 값으로 제공된 관리자 계정 번호로 멤버 및 멤버 역할 스택이 배포된 계정에서만 문제 해결(사용자 지정 작업 또는 완전 자동화된 EventBridge 규칙을 통해)을 시작할 수 있습니다.
- 계정 또는 리전이 솔루션을 완전히 제어할 수 없도록 하려면 해당 계정 또는 리전에 멤버 또는 멤버 역할 스택을 배포하지 마십시오.

Security Hub의 계정 및 리전 결과 집계 구성:

- 관리자 스택은 관리자 계정 및 리전에 도착한 결과에 대해서만 문제 해결(사용자 지정 작업 또는 완전 자동화된 EventBridge 규칙을 통해)을 시작할 수 있습니다.
- 계정 또는 리전이 솔루션을 완전히 제어할 수 없도록 하려면 관리자 스택이 배포된 동일한 관리자 계정 및 리전으로 결과를 전송하기 위해 해당 계정 또는 리전을 포함하지 마십시오.

배포되는 표준 중첩 스택:

- 관리자 스택은 대상 멤버 계정 및 리전에 컨트롤 런북이 배포된 컨트롤에 대한 문제 해결(사용자 지정 작업 또는 완전 자동화된 EventBridge 규칙을 통해)만 시작할 수 있습니다. 각 표준에 대해 멤버 스택에서 배포합니다.
- 관리자 스택은 해당 표준에 대한 관리자 스택에서 배포한 규칙이 있는 제어에 대한 EventBridge 규칙을 사용해야만 완전 자동화된 문제 해결을 시작할 수 있습니다. 이는 관리자 계정에 배포됩니다.
- 간소화를 위해 관리자 및 멤버 계정에 표준을 일관되게 배포하는 것이 좋습니다. AWS FSBP 및 CIS v1.2.0에 관심이 있는 경우이 두 중첩된 관리자 스택을 관리자 계정에 배포하고이 두 중첩된 멤버 스택을 각 멤버 계정 및 리전에 배포합니다.

각 중첩된 멤버 스택에 배포되는 Control 실행서:

- 관리자 스택은 각 표준의 멤버 스택에 의해 대상 멤버 계정 및 리전에 배포된 제어 런북이 있는 제어에 대해서만 (사용자 지정 작업 또는 완전 자동화된 EventBridge 규칙을 통해) 문제 해결을 시작할 수 있습니다.
- 특정 표준에 대해 활성화된 제어에 대해 보다 세분화된 제어를 수행하기 위해 표준의 각 중첩 스택에는 제어 런북이 배포되는 파라미터가 있습니다. 컨트롤의 파라미터를 "사용할 수 없음" 값으로 설정하여 해당 컨트롤 실행서를 배포 취소합니다.

표준을 활성화 및 비활성화하기 위한 SSM 파라미터:

- 관리자 스택은 표준 관리자 스택에 의해 배포된 SSM 파라미터를 통해 활성화된 표준에 대한 문제 해결(사용자 지정 작업 또는 완전 자동화된 EventBridge 규칙을 통해)만 시작할 수 있습니다.
- 표준을 비활성화하려면 경로가 "/Solutions/SO0111/<standard_name>/<standard_version>/status"인 SSM 파라미터의 값을 "No"로 설정합니다.

SNS 알림 예

문제 해결이 시작된 경우


```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```


문제 해결이 성공한 경우

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

문제 해결에 실패하는 경우

```
{
 "severity": "ERROR",
 "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

솔루션 사용

이 자습서는 ASR의 첫 번째 배포를 안내합니다. 솔루션을 배포하기 위한 사전 조건으로 시작하고 멤버 계정의 예제 조사 결과를 수정하는 것으로 끝납니다.

자습서: AWS에서 자동 보안 대응 시작하기

첫 번째 배포를 안내하는 자습서입니다. 솔루션을 배포하기 위한 사전 조건으로 시작하고 멤버 계정의 예제 조사 결과를 수정하는 것으로 끝납니다.

계정 준비

솔루션의 교차 계정 및 교차 리전 문제 해결 기능을 보여주기 위해이 자습서에서는 두 개의 계정을 사용합니다. 솔루션을 단일 계정에 배포할 수도 있습니다.

다음 예제에서는 계정 111111111111 및 222222222222를 사용하여 솔루션을 보여줍니다. 111111111111는 관리자 계정이 되고 222222222222는 멤버 계정이 됩니다. 리전 us-east-1 및의 리소스에 대한 조사 결과를 해결하기 위한 솔루션을 설정합니다us-west-2.

아래 표는 각 계정 및 리전의 각 단계에 대해 수행할 작업을 보여주는 예제입니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	없음	없음
222222222222	Member	없음	없음

관리자 계정은 솔루션의 관리 작업, 즉 수동으로 문제 해결을 시작하거나 EventBridge 규칙을 사용하여 완전 자동화된 문제 해결을 활성화하는 계정입니다. 또한이 계정은 조사 결과를 수정하려는 모든 계정의 Security Hub 위임된 관리자 계정이어야 하지만 계정이 속한 AWS Organizations 관리자 계정일 필요는 없습니다.

AWS Config 활성화

다음 설명서를 검토합니다.

- AWS Config 설명서

- AWS Config 요금
- AWS Config 활성화

두 계정 및 두 리전 모두에서 AWS Config를 활성화합니다. 이로 인해 요금이 발생합니다.

> **Important**
>
> "글로벌 리소스(예: AWS IAM 리소스) 포함" 옵션을 선택해야 합니다. AWS Config를 활성화할 때이 옵션을 선택하지 않으면 글로벌 리소스(예: AWS IAM 리소스)와 관련된 결과가 표시되지 않습니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	AWS Config 활성화	AWS Config 활성화
222222222222	Member	AWS Config 활성화	AWS Config 활성화

AWS 보안 허브 활성화

다음 설명서를 검토합니다.

- AWS Security Hub 설명서
- AWS Security Hub 요금
- AWS Security Hub 활성화

두 계정 및 두 리전 모두에서 AWS Security Hub를 활성화합니다. 이로 인해 요금이 발생합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	AWS Security Hub 활성화	AWS Security Hub 활성화
222222222222	Member	AWS Security Hub 활성화	AWS Security Hub 활성화

통합 제어 조사 결과 활성화

다음 설명서를 검토합니다.

- 제어 조사 결과 생성 및 업데이트

이 자습서에서는 권장 구성인 AWS Security Hub의 통합 제어 조사 결과 기능이 활성화된 솔루션 사용을 보여줍니다. 작성 시점에이 기능을 지원하지 않는 파티션에서는 SC(보안 제어)가 아닌 표준별 플레이북을 배포해야 합니다.

두 계정 및 두 리전 모두에서 통합 제어 조사 결과를 활성화합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	통합 제어 조사 결과 활성화	통합 제어 조사 결과 활성화
222222222222	Member	통합 제어 조사 결과 활성화	통합 제어 조사 결과 활성화

새로운 기능으로 조사 결과를 생성하는 데 다소 시간이 걸릴 수 있습니다. 자습서를 진행할 수 있지만 새 기능 없이는 생성된 결과를 수정할 수 없습니다. 새 기능으로 생성된 결과는 `GeneratorId` 필드 값로 식별할 수 있습니다`security-control/<control_id>`.

교차 리전 조사 결과 집계 구성

다음 설명서를 검토합니다.

- 교차 리전 집계
- 교차 리전 집계 활성화

두 계정 모두에서 us-west-2에서 us-east-1로의 조사 결과 집계를 구성합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	us-west-2에서 집계 구성	없음

Account	용도	us-east-1의 작업	us-west-2의 작업
222222222222	Member	us-west-2에서 집계 구성	없음

조사 결과가 집계 리전으로 전파되는 데 다소 시간이 걸릴 수 있습니다. 자습서를 진행할 수 있지만 집계 리전에 나타나기 시작할 때까지 다른 리전의 결과를 수정할 수 없습니다.

Security Hub 관리자 계정 지정

다음 설명서를 검토합니다.

- AWS Security Hub에서 계정 관리
- 조직 멤버 계정 관리
- 초대를 통한 멤버 계정 관리

다음 예제에서는 수동 초대 방법을 사용합니다. 프로덕션 계정 세트의 경우 AWS Organizations를 통해 Security Hub 위임된 관리를 관리하는 것이 좋습니다.

관리자 계정(111111111111)의 AWS Security Hub 콘솔에서 멤버 계정(222222222222)을 초대하여 관리자 계정을 Security Hub 위임된 관리자로 수락합니다. 멤버 계정에서 초대를 수락합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	멤버 계정 초대	없음
222222222222	Member	초대 수락	없음

조사 결과가 관리자 계정으로 전파되는 데 다소 시간이 걸릴 수 있습니다. 자습서를 진행할 수 있지만 관리자 계정에 나타나기 시작할 때까지 멤버 계정의 조사 결과를 수정할 수 없습니다.

자체 관리형 StackSets 권한에 대한 역할 생성

다음 설명서를 검토합니다.

- AWS CloudFormation StackSets
- 자체 관리형 권한 부여

CloudFormation 스택을 여러 계정에 배포하므로 StackSets를 사용합니다. 관리자 스택과 멤버 스택에는 서비스에서 지원하지 않는 중첩 스택이 있으므로 서비스 관리형 권한을 사용할 수 없습니다. 따라서 자체 관리형 권한을 사용해야 합니다.

StackSet 작업에 대한 기본 권한을 위해 스택을 배포합니다. 프로덕션 계정의 경우 "고급 권한 옵션" 설명서에 따라 권한을 좁힐 수 있습니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	StackSet 관리자 역할 스택 배포 StackSet 실행 역할 스택 배포	없음
222222222222	Member	StackSet 실행 역할 스택 배포	없음

예제 조사 결과를 생성할 안전하지 않은 리소스 생성

다음 설명서를 검토합니다.

- Security Hub 제어 참조
- AWS Lambda 제어

문제 해결을 보여주기 위해 안전하지 않은 구성이 있는 다음 예제 리소스입니다. 예제 제어는 Lambda.1입니다. Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.

> **Important**
>
> 의도적으로 안전하지 않은 구성으로 리소스를 생성할 예정입니다. 제어의 특성을 검토하고 사용자 환경에서 이러한 리소스를 직접 생성할 때의 위험을 평가하십시오. 이러한 리소스를 감지하고 보고하기 위해 조직에 있을 수 있는 모든 도구에 유의하고 적절한 경우 예외를 요청합니다. 선택한 예제 컨트롤이 부적절한 경우 솔루션이 지원하는 다른 컨트롤을 선택합니다.

멤버 계정의 두 번째 리전에서 AWS Lambda 콘솔로 이동하여 최신 Python 런타임에 함수를 생성합니다. 구성 → 권한에서 인증 없이 URL에서 함수를 호출할 수 있도록 정책 설명을 추가합니다.

콘솔 페이지에서 함수가 퍼블릭 액세스를 허용하는지 확인합니다. 솔루션이이 문제를 해결한 후 권한을 비교하여 퍼블릭 액세스가 취소되었는지 확인합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	없음	없음
222222222222	Member	없음	안전하지 않은 구성으로 Lambda 함수 생성

AWS Config가 안전하지 않은 구성을 감지하는 데 다소 시간이 걸릴 수 있습니다. 자습서를 진행할 수 있지만 Config가 결과를 감지할 때까지 결과를 수정할 수 없습니다.

관련 제어를 위한 CloudWatch 로그 그룹 생성

다음 설명서를 검토합니다.

- Amazon CloudWatch Logs를 사용하여 CloudTrail 로그 파일 모니터링
- CloudTrail 제어

솔루션에서 지원하는 다양한 CloudTrail 제어에는 다중 리전 CloudTrail의 대상인 CloudWatch Log 그룹이 있어야 합니다. CloudTrail 다음 예제에서는 자리 표시자 로그 그룹을 생성합니다. 프로덕션 계정의 경우 CloudTrail과 CloudWatch Logs의 통합을 올바르게 구성해야 합니다.

각 계정 및 리전에서 이름이 같은 로그 그룹을 생성합니다. 예: `asr-log-group`.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	로그 그룹 생성	로그 그룹 생성
222222222222	Member	로그 그룹 생성	로그 그룹 생성

자습서 계정에 솔루션 배포

관리자, 멤버 및 멤버 역할 스택에 대한 세 개의 Amazon S3 URLs을 수집합니다.

관리자 스택 배포

View template

automated-security-response-admin.template

관리자 계정에서 CloudFormation 콘솔로 이동하여 관리자 스택을 Security Hub 조사 결과 집계 리전에 배포합니다.

"SCNo" 또는 "보안 제어" 스택을 제외한 중첩된 관리자 스택을 로드하기 위한 모든 파라미터의 값을 선택합니다. 이 스택에는 계정에서 구성한 통합 제어 조사 결과에 대한 리소스가 포함되어 있습니다.

이전에이 계정 및 리전에이 솔루션을 배포하지 않은 경우 오케스트레이터 로그 그룹 No 재사용을 선택합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	관리자 스택 배포	없음
222222222222	Member	없음	없음

멤버 계정에서 관리자 계정으로 신뢰 관계를 생성할 수 있도록 관리자 스택이 배포를 완료할 때까지 기다렸다가 계속합니다.

멤버 스택 배포

View template

automated-security-response-member.template

관리자 계정에서 CloudFormation StackSets 콘솔로 이동하여 멤버 스택을 각 계정 및 리전에 배포합니다. 이 자습서에서 생성된 StackSets 관리자 및 실행 역할을 사용합니다.

로그 그룹 이름의 파라미터 값으로 생성한 로그 그룹의 이름을 입력합니다.

"SCNo" 또는 "보안 제어" 스택을 제외한 중첩된 멤버 스택을 로드하기 위한 모든 파라미터의 값을 선택합니다. 이 스택에는 계정에서 구성한 통합 제어 조사 결과에 대한 리소스가 포함되어 있습니다.

관리자 계정의 ID를 관리자 계정 번호의 파라미터 값으로 입력합니다. 이 예제에서는 입니다111111111111.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	멤버 StackSet 배포 / 멤버 스택 배포 확인	멤버 스택 배포 확인
222222222222	Member	멤버 스택 배포 확인	멤버 스택 배포 확인

멤버 역할 스택 배포

automated-security-response-member-roles.template 템플릿 버튼 automated-security-response-member-roles.template

관리자 계정에서 CloudFormation StackSets 콘솔로 이동하여 멤버 스택을 각 계정에 배포합니다. 이 자습서에서 생성된 StackSets 관리자 및 실행 역할을 사용합니다. 관리자 계정의 ID를 관리자 계정 번호의 파라미터 값으로 입력합니다. 이 예제에서는 입니다111111111111.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	멤버 StackSet 배포 / 멤버 스택 배포 확인	없음
222222222222	Member	멤버 스택 배포 확인	없음

계속 진행할 수 있지만 CloudFormation StackSets 배포가 완료될 때까지 결과를 수정할 수 없습니다.

SNS 주제 구독

문제 해결 업데이트

주제 -{https---us-east-1-console-aws-amazon-com-sns-v3-home-region-us-east-1—topic-arn-aws-sns-us-east-1-221128147805-SO0111-ASR-Topic}[SO0111-ASR_Topic]

관리자 계정에서 관리자 스택에서 생성한 Amazon SNS 주제를 구독합니다. 그러면 문제 해결이 시작될 때와가 성공 또는 실패할 때 알려줍니다.

경보

주제 -{https---us-east-1-console-aws-amazon-com-sns-v3-home-region-us-east-1—topic-arn-aws-sns-us-east-1-221128147805-SO0111-ASR-Alarm-Topic}[SO0111-ASR_Alarm_Topic]

관리자 계정에서 관리자 스택에서 생성한 Amazon SNS 주제를 구독합니다. 그러면 지표 경보가 시작될 때 알려줍니다.

예제 조사 결과 수정

관리자 계정에서 Security Hub 콘솔로 이동하여이 자습서의 일부로 생성한 안전하지 않은 구성으로 리소스에 대한 결과를 찾습니다.

여러 방법으로 수행할 수 있습니다.

1. 통합 제어 조사 결과 기능을 지원하는 파티션에서 "Controls"라는 페이지가 있으면 통합 제어 ID로 조사 결과를 찾을 수 있습니다.
2. "보안 표준" 페이지에서 어떤 표준에 속하는지에 따라 컨트롤을 찾을 수 있습니다.
3. "조사 결과" 페이지에서 모든 조사 결과를 보고 속성별로 검색할 수 있습니다.

생성한 퍼블릭 Lambda 함수의 통합 제어 ID는 Lambda.1입니다.

문제 해결 시작

생성한 리소스와 관련된 결과의 왼쪽에 있는 확인란을 선택합니다. "작업" 드롭다운 메뉴에서 "ASR로 수정"을 선택합니다. 조사 결과가 Amazon EventBridge로 전송되었다는 알림이 표시됩니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	문제 해결 시작	없음
222222222222	Member	없음	없음

문제 해결로 조사 결과가 해결되었는지 확인

두 개의 SNS 알림을 받게 됩니다. 첫 번째는 문제 해결이 시작되었음을 나타내고 두 번째는 문제 해결이 성공했음을 나타냅니다. 두 번째 알림을 받은 후 멤버 계정의 Lambda 콘솔로 이동하여 퍼블릭 액세스가 취소되었는지 확인합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	없음	없음
222222222222	Member	없음	문제 해결이 성공했는지 확인

문제 해결 실행 추적

솔루션의 작동 방식을 더 잘 이해하기 위해 문제 해결 실행을 추적할 수 있습니다.

EventBridge 규칙

관리자 계정에서 Remediate_with_ASR_CustomAction이라는 EventBridge 규칙을 찾습니다. 이 규칙은 Security Hub에서 전송한 결과와 일치하며 Orchestrator Step Functions로 전송합니다.

Step Functions 실행

관리자 계정에서 "SO0111-ASR-Orchestrator"라는 AWS Step Functions를 찾습니다. 이 단계 함수는 대상 계정 및 리전에서 SSM 자동화 문서를 호출합니다. 이 AWS Step Functions.

SSM 자동화

멤버 계정에서 SSM Automation 콘솔로 이동합니다. "ASR-SC_2.0.0_Lambda.1"이라는 문서의 두 실행과 "ASR-RemoveLambdaPublicAccess"라는 문서의 한 실행을 확인할 수 있습니다.

첫 번째 실행은 대상 계정의 오케스트레이터 단계 함수에서 수행됩니다. 두 번째 실행은 조사 결과가 시작된 리전이 아닐 수 있는 대상 리전에서 수행됩니다. 최종 실행은 Lambda 함수에서 퍼블릭 액세스 정책을 취소하는 문제 해결입니다.

CloudWatch 로그 그룹

관리자 계정에서 CloudWatch Logs 콘솔로 이동하여 "SO0111-ASR"이라는 로그 그룹을 찾습니다. 이 로그 그룹은 Orchestrator Step Functions의 상위 수준 로그의 대상입니다.

완전 자동화 문제 해결 활성화

솔루션의 다른 작업 모드는 조사 결과가 Security Hub에 도착하면 자동으로 해결하는 것입니다.

이 결과가 실수로 적용될 수 있는 리소스가 없는지 확인합니다.

자동 수정을 활성화하면 활성화한 제어(Lambda.1)와 일치하는 모든 리소스에 대한 수정이 시작됩니다.

> **Important**
>
> 솔루션 범위 내의 모든 퍼블릭 Lambda 함수가이 권한을 취소하도록 할지 확인합니다. 완전 자동화 문제 해결은 생성한 함수로 범위가 제한되지 않습니다. 솔루션은 설치된 계정 및 리전에서 감지되면이 제어를 해결합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	원하는 퍼블릭 함수 없음 확인	원하는 퍼블릭 함수 없음 확인
222222222222	Member	원하는 퍼블릭 함수 없음 확인	원하는 퍼블릭 함수 없음 확인

규칙 활성화

관리자 계정에서 SC_2.0.0_Lambda.1_AutoTrigger라는 EventBridge 규칙을 찾아 활성화합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	자동 문제 해결 규칙 활성화	없음
222222222222	Member	없음	없음

리소스 구성

멤버 계정에서 퍼블릭 액세스를 허용하도록 Lambda 함수를 다시 구성합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	없음	없음
222222222222	Member	없음	퍼블릭 액세스를 허용하도록 Lambda 함수 구성

문제 해결로 조사 결과가 해결되었는지 확인

Config가 안전하지 않은 구성을 다시 감지하는 데 시간이 걸릴 수 있습니다. 두 개의 SNS 알림을 받게 됩니다. 첫 번째는 수정이 시작되었음을 나타냅니다. 두 번째는 문제 해결이 성공했음을 나타냅니다. 두 번째 알림을 받은 후 멤버 계정의 Lambda 콘솔로 이동하여 퍼블릭 액세스가 취소되었는지 확인합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	자동 문제 해결 규칙 활성화	없음
222222222222	Member	없음	문제 해결이 성공했는지 확인

정리

예제 리소스 삭제

멤버 계정에서 생성한 Lambda 함수 예제를 삭제합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	없음	없음
222222222222	Member	없음	예제 Lambda 함수 삭제

관리자 스택 삭제

관리자 계정에서 관리자 스택을 삭제합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	관리자 스택 삭제	없음
222222222222	Member	없음	없음

멤버 스택 삭제

관리자 계정에서 멤버 StackSet를 삭제합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	멤버 StackSet 삭제 멤버 스택 삭제 확인	멤버 스택 삭제 확인
222222222222	Member	멤버 스택 삭제 확인	멤버 스택 삭제 확인

멤버 역할 스택 삭제

관리자 계정에서 멤버 역할 StackSet를 삭제합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	멤버 역할 StackSet 삭제 멤버 역할 스택 삭제 확인	없음
222222222222	Member	멤버 역할 스택 삭제 확인	없음

보관된 역할 삭제

각 계정에서 보관된 IAM 역할을 삭제합니다.

중요: 이러한 역할은 수정이 계속 작동하기 위해 역할이 필요한 수정을 위해 유지됩니다(예: VPC 흐름 로깅). 역할을 삭제하기 전에 이러한 역할의 지속적인 기능이 필요하지 않은지 확인합니다.

SO0111- 접두사가 붙은 모든 역할을 삭제합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	보관된 역할 삭제	없음
222222222222	Member	보관된 역할 삭제	없음

보존된 KMS 키 삭제 예약

관리자 스택과 멤버 스택 모두 KMS 키를 생성하고 유지합니다. 이러한 키를 유지하면 요금이 발생합니다.

이러한 키는 솔루션으로 암호화된 모든 리소스에 액세스할 수 있도록 보존됩니다. 삭제를 예약하기 전에 필요하지 않은지 확인합니다.

솔루션 또는 CloudFormation 기록에서 생성된 별칭을 사용하여 솔루션에서 배포한 키를 식별합니다. 삭제를 예약합니다.

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	삭제를 위한 관리자 키 식별 및 예약 삭제를 위한 멤버 키 식별 및 예약	삭제를 위한 멤버 키 식별 및 예약
222222222222	Member	삭제를 위한 멤버 키 식별 및 예약	삭제를 위한 멤버 키 식별 및 예약

자체 관리형 StackSets 권한에 대한 스택 삭제

자체 관리형 StackSets 권한을 허용하도록 생성된 스택 삭제

Account	용도	us-east-1의 작업	us-west-2의 작업
111111111111	관리자	StackSet 관리자 역할 스택 삭제	없음
222222222222	Member	StackSet 실행 역할 스택 삭제	없음

개발자 안내서

이 섹션에서는 솔루션의 소스 코드와 추가 사용자 지정을 제공합니다.

소스 코드

GitHub 리포지토리를 방문하여이 솔루션의 템플릿과 스크립트를 다운로드하고 사용자 지정을 다른 사용자와 공유합니다.

플레이북

이 솔루션에는 Center for Internet Security(CIS) AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0https://docs.aws.amazon.com/securityhub/latest/userguide/cis-aws-foundations-benchmark.html#cis3v0-standard, AWS Foundational Security Best Practices(FSBP) v.1.0.0, Payment Card Industry Data Security Standard(PCI-DSS) v3.2.1 및 National Institute of Standards and Technology(NIST)의 일부로 정의된 보안 표준에 대한 플레이북 수정 사항이 포함되어 있습니다.

통합 제어 조사 결과를 활성화한 경우 이러한 제어는 모든 표준에서 지원됩니다. 이 기능이 활성화된 경우 SC 플레이북만 배포하면 됩니다. 그렇지 않은 경우 플레이북은 이전에 나열된 표준에 대해 지원됩니다.

> **Important**
>
> 서비스 할당량에 도달하지 않도록 활성화된 표준에 대한 플레이북만 배포합니다.

특정 문제 해결에 대한 자세한 내용은 계정의 솔루션에서 배포한 이름이 포함된 Systems Manager 자동화 문서를 참조하세요. AWS Systems Manager 콘솔로 이동한 다음 탐색 창에서 문서를 선택합니다.

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
총 문제 해결	63	34	29	33	65	19	90

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableAutoScalingGroupELBHealthCheck 로드 밸런서와 연결된 Auto Scaling 그룹은 로드 밸런서 상태 확인을 사용해야 합니다.	Autoscaling.1		Autoscaling.1		Autoscaling.1		Autoscaling.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-ConfigureAutoScalingLaunchConfigToRequireIMDSv2 Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.					Autoscaling.3		Autoscaling.3

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateCloudTrailMultiRegionTrail CloudTrail을 활성화하고 하나 이상의 다중 리전 추적으로 구성해야 합니다.	CloudTrail.1	2.1	CloudTrail.2	3.1	CloudTrail.1	3.1	CloudTrail.1
ASR-EnableEncryption CloudTrail에는 저장 데이터 암호화가 활성화되어 있어야 합니다.	CloudTrail.2	2.7	CloudTrail.1	3.7	CloudTrail.2	3.5	CloudTrail.2

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableLogFileValidation CloudTrail 로그 파일 검증이 활성화되었는지 확인	CloudTrail.4	2.2	CloudTrail.3	3.2	CloudTrail.4		CloudTrail.4
ASR-EnableCloudTrailToCloudWatchLogging CloudTrail 추적이 Amazon CloudWatch Logs와 통합되었는지 확인	CloudTrail.5	2.4	CloudTrail.4	3.4	CloudTrail.5		CloudTrail.5

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-ConfigureS3BucketLogging CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인		2.6		3.6		3.4	CloudTrail.7
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.	Codebuild.2		Codebuild.2		Codebuild.2		CodeBuild.2

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableAWSConfig AWS Config가 활성화되었는지 확인	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1
ASR-MakeEBSSnapshotsPrivate Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다.	EC2.1		EC2.1		EC2.1		EC2.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-RemoveVPCDefaultSecurityGroupRules VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 금지해야 합니다.	EC2.2	4.3	EC2.2	5.3	EC2.2	5.4	EC2.2
ASR-EnableVPCFlowLogs VPC 흐름 로깅은 모든 VPC에서 활성화되어야 합니다.	EC2.6	2.9	EC2.6	3.9	EC2.6	3.7	EC2.6

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableEbsEncryptionByDefault EBS 기본 암호화를 활성화해야 합니다.	EC2.7	2.2.1			EC2.7	2.2.1	EC2.7
ASR-RevokeUnrotatedKeys 사용자의 액세스 키는 90일 이하마다 교체해야 합니다.	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
ASR-SetIAMPasswordPolicy IAM 기본 암호 정책	IAM.7	1.5-1.11	IAM.8	1.8	IAM.7	1.8	IAM.7

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-RevokeUnusedIAMUserCredentials 90일 이내에 사용하지 않으면 사용자 자격 증명을 꺼야 합니다.	IAM.8	1.3	IAM.7		IAM.8		IAM.8
ASR-RevokeUnusedIAMUserCredentials 45일 이내에 사용하지 않으면 사용자 자격 증명을 꺼야 합니다.				1.12		1.12	IAM.22

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-RemoveLambdaPublicAccess Lambda 함수는 퍼블릭 액세스를 금지해야 합니다.	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR-MakeRDSSnapshotPrivate RDS 스냅샷은 퍼블릭 액세스를 금지해야 합니다.	RDS.1		RDS.1		RDS.1		RDS.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-DisablePublicAccessToRDSInstance RDS DB 인스턴스는 퍼블릭 액세스를 금지해야 합니다.	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2
ASR-EncryptRDSSnapshot RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화해야 합니다.	RDS.4				RDS.4		RDS.4

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableMultiAZOnRDSInstance RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.	RDS.5				RDS.5		RDS.5
ASR-EnableEnhancedMonitoringOnRDSInstance RDS DB 인스턴스 및 클러스터에 대해 향상된 모니터링을 구성해야 합니다.	RDS.6				RDS.6		RDS.6

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableRDSClusterDeletionProtection RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.	RDS.7				RDS.7		RDS.7
ASR-EnableRDSInstanceDeletionProtection RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.	RDS.8				RDS.8		RDS.8

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableMinorVersionUpgradeOnRDSDBInstance RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.	RDS.13				RDS.13	2.3.2	RDS.13
ASR-EnableCopyTagsToSnapshotOnRDSCluster 태그를 스냅샷에 복사하도록 RDS DB 클러스터를 구성해야 합니다.	RDS.16				RDS.16		RDS.16

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-DisablePublicAccessToRedshiftCluster Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.	Redshift.1		Redshift.1		Redshift.1		Redshift.1
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.	Redshift.3				Redshift.3		Redshift.3

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableRedshiftClusterAuditLogging Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.	Redshift.4				Redshift.4		Redshift.4
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift는 메이저 버전으로 자동 업그레이드가 활성화되어 있어야 합니다.	Redshift.6				Redshift.6		Redshift.6

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-ConfigureS3PublicAccessBlock S3 퍼블릭 액세스 차단 설정을 활성화해야 합니다.	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
ASR-ConfigureS3BucketPublicAccessBlock S3 버킷은 퍼블릭 읽기 액세스를 금지해야 합니다.	S3.2		S3.2	2.1.5.2	S3.2		S3.2

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-ConfigureS3BucketPublicAccessBlock S3 버킷은 퍼블릭 쓰기 액세스를 금지해야 합니다.		S3.3					S3.3
ASR-EnableDefaultEncryptionS3 S3 버킷에는 서버 측 암호화가 활성화되어 있어야 합니다.	S3.4		S3.4	2.1.1	S3.4		S3.4

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-SetSSLBucketPolicy S3 버킷에는 SSL 사용 요청이 필요합니다.	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5
ASR-S3BlockDenylist 버킷 정책의 다른 AWS 계정에 부여된 Amazon S3 권한은 제한되어야 합니다.	S3.6				S3.6		S3.6

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
S3 퍼블릭 액세스 차단 설정은 버킷 수준에서 활성화해야 합니다.	S3.8				S3.8		S3.8
ASR-ConfigureS3BucketPublicAccessBlock 에 대한 S3 버킷 CloudTrail 로그에 공개적으로 액세스할 수 없는지 확인합니다.		2.3					CloudTrail.6

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateAccessLoggingBucket CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.		2.6					CloudTrail.7
ASR-EnableKeyRotation 고객 생성 CMKs에 대한 교체가 활성화되었는지 확인		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateLogMetricFilterAndAlarm 무단 API 호출에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.1		4.1			Cloudwatch.1
ASR-CreateLogMetricFilterAndAlarm MFA 없이 AWS Management Console 로그인에 대한 로그 지표 필터 및 경보가 존재하는지 확인		3.2		4.2			Cloudwatch.2

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateLogMetricFilterAndAlarm "루트" 사용자 사용에 대한 로그 지표 필터 및 경보가 존재하는지 확인합니다.		3.3	CW.1	4.3			Cloudwatch.3
ASR-CreateLogMetricFilterAndAlarm IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.4		4.4			Cloudwatch.4

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateLogMetricFilterAndAlarm CloudTrail 구성 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.5		4.5			Cloudwatch.5
ASR-CreateLogMetricFilterAndAlarm AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인		3.6		4.6			Cloudwatch.6

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateLogMetricFilterAndAlarm 고객 생성 CMK 활성화 또는 예약된 삭제에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.7		4.7			Cloudwatch.7

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateLogMetricFilterAndAlarm S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.8		4.8			Cloudwatch.8
ASR-CreateLogMetricFilterAndAlarm AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인		3.9		4.9			Cloudwatch.9

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateLogMetricFilterAndAlarm 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.10		4.10			Cloudwatch.10

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateLogMetricFilterAndAlarm 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.11		4.11			Cloudwatch.11

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateLogMetricFilterAndAlarm 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.12		4.12			Cloudwatch.12
ASR-CreateLogMetricFilterAndAlarm 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.13		4.13			Cloudwatch.13

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-CreateLogMetricFilterAndAlarm VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.		3.14		4.14			Cloudwatch.14
AWS-DisablePublicAccessForSecurityGroup 어떤 보안 그룹에서도 0.0.0.0/0에서 포트 22로의 수신을 허용하지 않는지 여부를 확인합니다.		4.1	EC2.5		EC2.13		EC2.13

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
AWS-DisablePublicAccessForSecurityGroup 어떤 보안 그룹에서도 0.0.0.0/0에서 포트 3389로의 수신을 허용하지 않는지 여부를 확인합니다.		4.2			EC2.14		EC2.14
ASR-ConfigureSNSTopicForStack	CloudFormation.1				CloudFormation.1		CloudFormation.1
ASR-CreateIAMSupportRole		1.20		1.17		1.17	IAM.18

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-DisablePublicIPAutoAssign Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.	EC2.15				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail.4	2.2	CloudTrail.3	3.2			CloudTrail.4
ASR-EnableEncryptionForSNSTopic	SNS.1				SNS.1		SNS.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableDeliveryStatusLoggingForSNSTopic 주제에 전송된 알림 메시지에 대해 전송 상태 로깅을 활성화해야 합니다.	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionForSQSQueue	SQS.1				SQS.1		SQS.1
ASR-MakeRDSSnapshotPrivate RDS 스냅샷은 프라이빗이어야 합니다.	RDS.1		RDS.1				RDS.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-BlockSSMDocumentPublicAccess SSM 문서는 공개되어서는 안 됩니다.	SSM.4				SSM.4		SSM.4
ASR-EnableCloudFrontDefaultRootObject CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.	CloudFront.1				CloudFront.1		CloudFront.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-SetCloudFrontOriginDomain CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.	CloudFront.12				CloudFront.12		CloudFront.12
ASR-RemoveCodeBuildPrivilegedMode CodeBuild 프로젝트 환경에는 로깅 AWS 구성이 있어야 합니다.	Codebuild.5				Codebuild.5		Codebuild.5

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-TerminateEC2Instance 중지된 EC2 인스턴스는 지정된 기간 후에 제거해야 합니다.	EC2.4				EC2.4		EC2.4
ASR-EnableIMDSV2OInstance EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.	EC2.8				EC2.8	5.6	EC2.8

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-RevokeUnauthorizedInboundRules 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.	EC2.18				EC2.18		EC2.18
여기에 제목 삽입 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.	EC2.19				EC2.19		EC2.19

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-DisableTGWAutcAcceptSharedAttachments Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락해서는 안 됩니다.	EC2.23				EC2.23		EC2.23
ASR-EnablePrivateRepositoryScanning ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.	ECR.1				ECR.1		ECR.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableGuardDuty GuardDuty를 활성화해야 합니다.	GuardDuty.1		GuardDuty.1		GuardDuty.1		GuardDuty.1
ASR-ConfigureS3BucketLogging S3 버킷 서버 액세스 로깅을 활성화해야 합니다.	S3.9				S3.9		S3.9
ASR-EnableBucketEventNotifications S3 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.	S3.11				S3.11		S3.11

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-SetS3LifecyclePolicy S3 버킷에는 수명 주기 정책이 구성되어 있어야 합니다.	S3.13				S3.13		S3.13
ASR EnableAutoSecretRotation Secrets Manager 비밀번호에는 자동 로테이션이 활성화되어 있어야 합니다.	SecretsManager.1				SecretsManager.1		SecretsManager.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-RemoveUnusedSecret 사용하지 않는 Secrets Manager 암호를 제거합니다.	SecretsManager.3				SecretsManager.3		SecretsManager.3
ASR-UpdateSecretRotationPeriod Secrets Manager 암호는 지정된 일수 내에 교체되어야 합니다.	SecretsManager.4				SecretsManager.4		SecretsManager.4

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableAPIGatewayCacheDataEncryption API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.					APIGateway.5		APIGateway.5
ASR-SetLogGroupRetentionDays CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.					CloudWatch.16		CloudWatch.16

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-AttachServiceVPCEndpoint Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.	EC2.10				EC2.10		EC2.10
ASR-TagGuardDutyResource GuardDuty 필터에 태그를 지정해야 합니다.							GuardDuty.2

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-TagGuardDutyResource GuardDuty 탐지기에 태그를 지정해야 합니다.							GuardDuty.4
ASR-AttachSSMPermissionsToEC2 Amazon EC2 인스턴스는 Systems Manager에서 관리해야 합니다.	SSM.1		SSM.3				SSM.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-ConfigureLaunchConfigNoPublicIPDocument Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.					AutoScaling.5		Autoscaling.5
ASR-EnableAPIGatewayExecutionLogs	APIGateway.1						APIGateway.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnablEMacie Amazon Macie가 활성화되어야 합니다.	Macie.1				Macie.1		Macie.1
ASR-EnablEAthenaWorkGroupLogging Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.	Athena.4						Athena.4

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnforceHTTPSForALB Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.	ELB.1		ELB.1		ELB.1		ELB.1
ASR-LimitECSRootFilesystemAccess ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다.	ECS.5				ECS.5		ECS.5

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableElastiCacheBackups ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.	ElastiCache.1				ElastiCache.1		ElastiCache.1
ASR-EnableElastiCacheVersionUpgrades ElastiCache 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.	ElastiCache.2				ElastiCache.2		ElastiCache.2

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-EnableElastiCacheReplicationGroupFailover ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.	ElastiCache.3				ElastiCache.3		ElastiCache.3
ASR-ConfigureDynamoDBAutoScaling DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.	DynamoDB.1				DynamoDB.1		DynamoDB.1

설명	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	보안 제어 ID
ASR-TagDynamoDBTableResource DynamoDB 테이블에 태그를 지정해야 합니다.							DynamoDB.5
ASR-EnableDynamoDDeletionProtection DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.					DynamoDB.6		DynamoDB.6

새 문제 해결 추가

해결 방법은 원하는 워크플로에 따라 적절한 플레이북 파일을 업데이트하여 수동으로 추가하거나 CDK 구문을 통해 솔루션을 프로그래밍 방식으로 확장하여 추가할 수 있습니다.

> **Note**
>
> 다음 지침은 솔루션에서 설치한 리소스를 시작점으로 활용합니다. 대부분의 솔루션 리소스 이름에는 ASR 및/또는 SO0111이 포함되어 있어 쉽게 찾고 식별할 수 있습니다.

수동 워크플로 개요

AWS 실행서의 자동 보안 응답은 다음 표준 이름을 따라야 합니다.

ASR-*<standard>*-*<version>*-*<control>*

표준: 보안 표준의 약어입니다. 이는 ASR에서 지원하는 표준과 일치해야 합니다. "CIS", "AFSBP", "PCI", "NIST" 또는 "SC" 중 하나여야 합니다.

버전: 표준의 버전입니다. 다시 말하지만, ASR에서 지원하는 버전과 결과 데이터의 버전과 일치해야 합니다.

제어: 수정할 제어의 제어 ID입니다. 이는 결과 데이터와 일치해야 합니다.

1. 멤버 계정(들)에서 실행서를 생성합니다.
2. 멤버 계정(들)에서 IAM 역할을 생성합니다.
3. (선택 사항) 관리자 계정에서 자동 문제 해결 규칙을 생성합니다.

1단계. 멤버 계정(들)에서 실행서 생성

1. AWS Systems Manager 콘솔에 로그인하고 조사 결과 JSON의 예를 가져옵니다.
2. 결과를 수정하는 자동화 실행서를 생성합니다. 내 소유 탭에서 `ASR-` 문서 탭 아래의 문서를 시작점으로 사용합니다.
3. 관리자 계정의 AWS Step Functions가 실행서를 실행합니다. 실행서를 호출할 때 전달하려면 실행서에서 문제 해결 역할을 지정해야 합니다.

2단계. 멤버 계정(들)에서 IAM 역할 생성

1. AWS Identity and Access Management 콘솔에 로그인합니다.
2. IAM SO0111 역할에서 예를 얻고 새 역할을 생성합니다. 역할 이름은 SO0111-Remediate-*<standard>*-*<version>*-*<control>*로 시작해야 합니다. 예를 들어 CIS v1.2.0 컨트롤 5.6을 추가하는 경우 역할은 여야 합니다`SO0111-Remediate-CIS-1.2.0-5.6`.

3. 이 예제를 사용하여 수정을 수행하는 데 필요한 API 호출만 허용하는 적절한 범위의 역할을 생성합니다.

이 시점에서 수정은 활성 상태이며 AWS Security Hub의 ASR 사용자 지정 작업에서 자동 수정에 사용할 수 있습니다.

3단계: (선택 사항) 관리자 계정에서 자동 문제 해결 규칙 생성

자동('자동'이 아님) 수정은 AWS Security Hub에서 결과를 받는 즉시 수정을 즉시 실행하는 것입니다. 이 옵션을 사용하기 전에 위험을 신중하게 고려하세요.

1. CloudWatch Events에서 동일한 보안 표준에 대한 예제 규칙을 봅니다. 규칙의 이름 지정 표준은 입니다`standard_control_*AutoTrigger*`.
2. 사용할 예제에서 이벤트 패턴을 복사합니다.
3. 조사 결과 JSON의 `GeneratorId`와 일치하도록 `GeneratorId` 값을 변경합니다.
4. 규칙을 저장하고 활성화합니다.

CDK 워크플로 개요

요약하면 ASR 리포지토리의 다음 파일이 수정되거나 추가됩니다. 이 예제에서는 ElastiCache.2에 대한 새로운 수정 사항이 SC 및 AFSBP 플레이북에 추가되었습니다.

> **Note**
>
> 모든 새로운 수정 사항은 ASR에서 사용 가능한 모든 수정 사항을 통합하므로 SC 플레이북에 추가해야 합니다. 특정 플레이북 세트(예: AFSBP)만 배포하려는 경우 (1) 의도한 플레이북에만 문제 해결을 추가하거나 (2) SC 플레이북 외에도 해당 Security Hub Standard에 있는 모든 플레이북에 문제 해결을 추가할 수 있습니다. 두 번째 옵션은 유연성을 위해 권장됩니다.

이 예제에서는 ElastiCache.2가 다음 Security Hub 표준에 포함되어 있습니다.

- AFSBP
- 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)

- PCI DSS v4.0.1/6.3.3

기본적으로 ASR은 AFSBP 및 NIST.800-53용 플레이북만 구현하므로 SC 외에도 이러한 플레이북에 이 새로운 수정 사항을 추가할 것입니다.

Modify

- source/lib/remediation-runbook-stack.ts
- source/playbooks/AFSBP/lib/[standard name]_remediations.ts
- source/playbooks/NIST80053/lib/control_runbooks-construct.ts
- source/playbooks/NIST80053/lib/[standard name]_remediations.ts
- source/playbooks/SC/lib/control_runbooks-construct.ts
- source/playbooks/SC/lib/sc_remediations.ts
- source/test/regex_registry.ts

Add

- source/playbooks/SC/ssmdocs/SC_ElastiCache.2.ts
- source/playbooks/SC/ssmdocs/descriptions/ElastiCache.2.md
- source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml

> **Note**
>
> 실행서에 대해 선택한 이름은 나머지 변경 사항과 일치하는 한 모든 문자열이 될 수 있습니다.

- source/playbooks/NIST80053/ssmdocs/NIST80053_ElastiCache.2.ts
- source/playbooks/AFSBP/ssmdocs/AFSBP_ElastiCache.2.yaml

개발 단계

1. 문제 해결 런북을 생성합니다.
2. 컨트롤 런북을 생성합니다.
3. 각 컨트롤 런북을 플레이북과 통합합니다.

4. 수정 IAM 역할 생성 및 수정 런북 통합
5. 단위 테스트 업데이트

1단계: 문제 해결 런북 생성

이 문서는 리소스를 수정하는 데 사용되는 SSM 문서입니다. 여기에는 수정을 실행할 권한이 있는 IAM 역할인 `AutomationAssumeRole` 파라미터가 포함되어야 합니다. 새 문제 해결 실행서를 생성할 때 기존 파일을 참조`source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml`로 봅니다.

모든 새 실행서를 `source/remediation_runbooks/` 디렉터리에 추가해야 합니다.

2단계: 컨트롤 런북 생성

컨트롤 런북은 지정된 표준의 결과 데이터를 구문 분석하고 적절한 문제 해결 런북을 실행하는 플레이북별 런북입니다. SC, AFSBP 및 NIST80053 플레이북에 ElastiCache.2 문제 해결을 추가하므로 각각에 대해 새 컨트롤 런북을 생성해야 합니다. 다음 파일이 생성됩니다.

- source/playbooks/SC/ssmdocs/SC_ElastiCache.2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ElastiCache.2.ts
- source/playbooks/AFSBP/ssmdocs/AFSBP_ElastiCache.2.yaml

Example

이러한 파일의 이름은 중요하며 <PLAYBOOK_NAME>_<CONTROL.ID>.ts/yaml 형식을 따라야 합니다.

ASR의 일부 플레이북은 TypeScript의 IaC 제어 런북을 지원하는 반면 원시 YAML로 작성해야 하는 플레이북도 있습니다. 각 플레이북의 기존 수정 사항을 예제로 참조하세요. 이 예제에서는 IaC를 사용하는 SC 플레이북을 다룹니다.

SC 플레이북에서 새 컨트롤 런북은 ControlRunbookDocument를 확장하고 문제 해결 런북의 이름과 일치하는 클래스를 내보내야 합니다. 아래 예제를 살펴보십시오.

```
export class EnableElastiCacheVersionUpgrades extends ControlRunbookDocument {
  constructor(scope: Construct, id: string, props: ControlRunbookProps) {
    super(scope, id, {
      ...props,
      securityControlId: 'ElastiCache.2',
      remediationName: 'EnableElastiCacheVersionUpgrades',
```

```
      scope: RemediationScope.REGIONAL,
      resourceIdRegex: <Regex>,
      resourceIdName: 'ClusterId',
      updateDescription: new StringFormat('Automatic minor version upgrades enabled for
 cluster %s.', [
        StringVariable.of(`ParseInput.ClusterId`),
      ]),
    });
  }
}
```

- `securityControlId`는 Security Hub의 통합 제어 보기에 정의된 대로 추가하려는 수정에 대한 제어 ID입니다.
- `remediationName`는 문제 해결 런북에 대해 선택한 이름입니다.
- `scope`는 수정하려는 리소스의 범위로, 전역적으로 존재하는지 또는 특정 리전에 존재하는지를 나타냅니다.
- `resourceIdRegex`는 파라미터로 문제 해결 실행서에 전달하려는 리소스 ID를 캡처하는 데 사용되는 정규식입니다. 하나의 그룹만 캡처해야 하며 다른 모든 그룹은 캡처되지 않아야 합니다. 전체 ARN을 전달하려면이 필드를 생략합니다.
- `resourceIdName`는를 사용하여 캡처된 리소스 ID에 대해 설정하려는 이름이며`resourceIdRegex`, 이는 문제 해결 실행서의 리소스 ID 파라미터 이름과 일치해야 합니다.
- `updateDescription`는 문제 해결이 성공하면 Security Hub에서 조사 결과의 "참고" 섹션에 할당하려는 문자열입니다.

클래스의 새 인스턴스를 반환`createControlRunbook`하는 라는 함수도 내보내야 합니다. ElastiCache.2,의 경우 다음과 같습니다.

```
export function createControlRunbook(scope: Construct, id: string, props:
 PlaybookProps): ControlRunbookDocument {
  return new EnableElastiCacheVersionUpgrades(scope, id, { ...props, controlId:
 'ElastiCache.2' });
}
```

여기서 `controlId`는 작동 중인 플레이북과 연결된 보안 표준에 정의된 제어 ID입니다.

Security Hub 컨트롤에 문제 해결 런북에 전달하려는 파라미터가 있는 경우 다음 메서드에 재정의를 추가하여 전달할 수 있습니다. - `getExtraSteps`: Security Hub에서 컨트롤에 대해 구현된 각 파라미터의 기본값을 정의합니다.

> **Note**
>
> Security Hub의 각 파라미터에는 기본값이 부여되어야 합니다.

- `getInputParamsStepOutput`: 제어 실행서의 GetInputParams 단계에 대한 출력을 정의합니다.
- 각 출력에는 name, `outputType`및가 있습니다`selector`. 는 `getExtraSteps` 메서드 재정의에 사용된 것과 동일한 선택기여야 `selector` 합니다.
- `getRemediationParams`: GetInputParams 단계 출력에서 가져온 문제 해결 실행서에 전달된 파라미터를 정의합니다.

예를 보려면 `source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts` 파일로 이동합니다.

3단계: 각 컨트롤 런북을 플레이북과 통합

이전 단계에서 생성된 각 컨트롤 런북에 대해 이제 연결된 플레이북의 인프라 정의와 통합해야 합니다. 각 컨트롤 런북에 대해 아래 단계를 따릅니다.

> **Important**
>
> 형식 스크립트 IaC 대신 원시 YAML을 사용하여 컨트롤 런북을 생성한 경우 다음 섹션으로 건너뜁니다.

새로 생성된 컨트롤 런북 파일 */<playbook_name>*`/control_runbooks-construct.ts` 가져오기에서 다음과 같이 다음을 수행합니다.

```
import * as elasticache_2 from '../ssmdocs/SC_ElastiCache.2';
```

다음으로의 배열로 이동합니다.

```
const controlRunbooksRecord: Record<string, any>
```

그리고 컨트롤 ID(플레이북별)를 생성한 `createControlRunbook` 메서드에 매핑하는 새 항목을 추가합니다.

```
'ElastiCache.2': elasticache_2.createControlRunbook,
```

다음과 *<playbook_name>*_remediations.ts 같이의 문제 해결 목록에 플레이북별 제어 ID를 추가합니다.

```
{ control: 'ElastiCache.2', versionAdded: '2.3.0' },
```

versionAdded 필드는 솔루션의 최신 버전이어야 합니다. 수정을 추가하면 템플릿 크기 제한을 위반하는 경우를 늘립니다versionAdded. 의 각 플레이북 멤버 스택에 포함된 문제 해결 수를 조정할 수 있습니다solution_env.sh.

4단계: 수정 IAM 역할 생성 및 수정 런북 통합

각 수정에는 수정 실행서를 실행하는 데 필요한 사용자 지정 권한이 있는 자체 IAM 역할이 있습니다. 또한 1단계에서 생성한 문제 해결 런북을 솔루션의 CloudFormation 템플릿에 추가하려면 RunbookFactory.createRemediationRunbook 메서드를 호출해야 합니다.

에서 remediation-runook-stack.ts각 수정은 RemediationRunbookStack 클래스에 자체 코드 블록이 있습니다. 다음 코드 블록은 ElastiCache.2 문제 해결을 위한 새 IAM 역할 생성 및 문제 해결 런북 통합을 보여줍니다.

```
    //-----------------------
    // EnableElastiCacheVersionUpgrades
    //
    {
      const remediationName = 'EnableElastiCacheVersionUpgrades'; // should match the
 name of your remediation runbook
      const inlinePolicy = new Policy(props.roleStack, `ASR-Remediation-Policy-
${remediationName}`);

      const remediationPolicy = new PolicyStatement();
      remediationPolicy.addActions('elasticache:ModifyCacheCluster');
      remediationPolicy.effect = Effect.ALLOW;
      remediationPolicy.addResources(`arn:${this.partition}:elasticache:*:
${this.account}:cluster:*`);
      inlinePolicy.addStatements(remediationPolicy);

      new SsmRole(props.roleStack, 'RemediationRole ' + remediationName, { // creates
 the remediation IAM role
        solutionId: props.solutionId,
        ssmDocName: remediationName,
        remediationPolicy: inlinePolicy,
        remediationRoleName: `${remediationRoleNameBase}${remediationName}`,
```

```
      });

      RunbookFactory.createRemediationRunbook(this, 'ASR ' + remediationName, { // adds
the remediation runbook to the solution's cloudformation templates
        ssmDocName: remediationName,
        ssmDocPath: ssmdocs,
        ssmDocFileName: `${remediationName}.yaml`,
        scriptPath: `${ssmdocs}/scripts`,
        solutionVersion: props.solutionVersion,
        solutionDistBucket: props.solutionDistBucket,
        solutionId: props.solutionId,
        namespace: namespace,
      });
    }
```

5단계: 단위 테스트 업데이트

새 문제 해결을 추가한 후 단위 테스트를 업데이트하고 실행하는 것이 좋습니다.

먼저 `source/test/regex_registry.ts` 파일에 새 정규식(아직 추가되지 않음)을 추가해야 합니다. 이 파일은 솔루션의 실행서에 포함된 각 새 정규식에 대한 테스트를 적용합니다. ElastiCache 문제 해결에 사용되는 정규식을 테스트하는 데 사용되는 `addElastiCacheClusterTestCases` 함수를 예로 들어 보겠습니다.

마지막으로 각 스택의 스냅샷을 업데이트해야 합니다. 스냅샷은 ASR 인프라의 변경 사항을 추적하는 데 사용되는 버전 관리형 CloudFormation 템플릿 정의입니다. `deployment` 디렉터리에서 다음 명령을 실행하여 이러한 스냅샷 파일을 업데이트할 수 있습니다.

```
./run-unit-tests.sh update
```

이제 새 수정 사항을 배포할 준비가 되었습니다! 새 변경 사항을 사용하여 솔루션을 빌드하고 배포하는 방법에 대한 지침은 아래 빌드 및 배포 섹션으로 이동합니다.

새 플레이북 추가

GitHub 리포지토리에서 AWS 솔루션 플레이북 및 배포 소스 코드의 자동 보안 대응을 다운로드합니다.

AWS CloudFormation 리소스는 AWS CDK 구성 요소에서 생성되며, 리소스에는 새 플레이북을 생성하고 구성하는 데 사용할 수 있는 플레이북 템플릿 코드가 포함되어 있습니다. 프로젝트 설정 및 플레이북 사용자 지정에 대한 자세한 내용은 GitHub의 README.md 파일을 참조하세요.

AWS Systems Manager Parameter Store

AWS의 자동 보안 응답은 운영 데이터 저장을 위해 AWS Systems Manager Parameter Store를 사용합니다. 다음 파라미터는 Parameter Store에 저장됩니다.

이름	값	사용
/Solutions/SO0111/CMK_REMEDIATION_ARN	FSBP 문제 해결을 위해 데이터를 암호화하는 AWS KMS 키	문제 해결의 일환으로 CloudTrail 로그와 같은 고객 데이터 암호화
/Solutions/SO0111/CMK_ARN	ASR이 데이터를 암호화하는 데 사용할 AWS KMS 키	솔루션 데이터 암호화
/Solutions/SO0111/SNS_Topic_ARN	솔루션에 대한 Amazon SNS 주제의 ARN	문제 해결 이벤트 알림
/Solutions/SO0111/SNS_Topic_Config.1	AWS Config 업데이트에 대한 SNS 주제	Config.1 문제 해결
/Solutions/SO0111/sendAnonymousMetrics	Yes	익명화된 지표 수집
/Solutions/SO0111/version	솔루션 버전	
/Solutions/SO0111 /<### # ##>/<##>/상태	enabled	솔루션에서 표준이 활성 상태인지 여부를 나타냅니다. 이를로 변경하여 자동 문제 해결을 위해 표준을 비활성화할 수 있습니다. disabled
/Solutions/SO0111 /<### # ##>/짧은 이름	String	보안 표준의 짧은 이름입니다. 예: CIS, AFSBP, PCI
/Solutions/SO0111 /<### # ##>/<##>/<###>/재매핑	String	한 컨트롤이 다른 컨트롤과 동일한 문제 해결을 사용하는 경

이름	값	사용
		우 이러한 파라미터는 다시 매핑을 수행합니다.

Amazon SNS 주제 - 문제 해결 진행 상황

AWS의 자동 보안 응답은 Amazon SNS 주제 SO0111-ASR_Topic을 생성합니다. 이 주제는 문제 해결 진행 상황에 대한 업데이트를 게시하는 데 사용됩니다. 다음은이 주제로 보낼 수 있는 세 가지 알림입니다.

```
Remediation queued for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
Remediation failed for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
[.replaceable]`<control_ID>` remediation was successfully invoke via AWS Systems
 Manager in account [.replaceable]`<account_ID>`
```

완료 메시지입니다. 오류 없이 문제 해결이 완료되었음을 나타냅니다. 그러나 성공적인 문제 해결을 위한 최종 테스트는 AWS Config 검사 및/또는 수동 검증입니다.

SNS 주제 구독 필터링

Amazon SNS 구독 필터 정책:

1. SNS 주제 구독으로 이동합니다.
2. 구독 필터 정책에서 “편집”을 선택합니다.
3. "구독 필터 정책"을 확장하고 "구독 필터 정책" 옵션을 전환하여 필터를 활성화합니다.
4. "메시지 본문" 범위를 선택합니다.
5. JSON 편집기에 정책을 추가합니다.
6. 변경 내용을 저장합니다.

정책 예제:

계정별 필터링

```
{
"finding": {
"account": [
"111111111111",
"222222222222"
]
}
```

오류 필터링

```
{
"severity": ["ERROR"]
}
```

제어를 기준으로 필터링

```
{
"finding": {
"standard_control": ["S3.9","S3.6"]
}
}
```

Amazon SNS 주제 - CloudWatch 경보

이 솔루션은 Amazon SNS 주제를 생성합니다`SO0111-ASR_Alarm_Topic`. 이 주제는 경보 알림을 게시하는 데 사용됩니다.

ALARM 상태로 전환되는 모든 경보에 대한 세부 정보가이 주제로 전송됩니다.

Config 조사 결과에 대한 런북 시작

이 솔루션은 사용자 지정 AWS Config 조사 결과를 기반으로 런북을 시작할 수 있습니다. 이렇게 하려면 다음을 수행해야 합니다.

1. 수정하려는 AWS Config 규칙 이름을 찾습니다. 이는 AWS Config 또는 Security Hub가이 규칙에 대해 생성하는 조사 결과에서 찾을 수 있습니다.
2. AWS Systems Manager 파라미터 스토어로 이동하여 파라미터 생성을 선택합니다.

3. 규칙의 이름은 /Solutions/SO0111/[.replaceable]이어야 합니다.Rule name from Step 1
4. 값은 다음과 같이 형식이 지정되어야 합니다.

```
{

"RunbookName":"Name of SSM runbook",

"RunbookRole": "Role that Orchestrator will assume"

}
```

1. RunbookName은 필수 필드이며이 Config 규칙을 수정할 때 실행되는 실행서입니다. RunbookRole은 오케스트레이터가이 역할을 실행할 때 수임할 역할입니다. 필수 필드가 아니며, 비워 두면 오케스트레이터는 기본적으로 계정의 멤버 역할을 사용합니다.
2. 이 작업이 적용되면 Security Hub에 있는 "ASR로 수정" 사용자 지정 작업을 사용하여 Config 규칙을 수정할 수 있습니다.

레퍼런스

이 섹션에는이 솔루션의 고유한 지표를 수집하기 위한 선택적 기능, 관련 리소스에 대한 포인터,이 솔루션에 기여한 빌더 목록에 대한 정보가 포함되어 있습니다.

익명화된 데이터 수집

이 솔루션에는 익명화된 운영 지표를 AWS로 전송하는 옵션이 포함되어 있습니다. 당사는 이 데이터를 사용하여 고객이 이 솔루션과 관련 서비스 및 제품을 어떻게 사용하는지 더 잘 이해합니다. 활성화되면 다음 정보가 수집되어 AWS로 전송됩니다.

- 솔루션 ID - AWS 솔루션 식별자
- 고유 ID(UUID) - 각 AWS Security Hub 응답 및 수정 배포에 대해 무작위로 생성된 고유 식별자
- 타임스탬프 - 데이터 수집 타임스탬프
- 인스턴스 데이터 -이 스택 배포에 대한 정보
- 솔루션 구성 - 초기 시작 시 설정된 기능 및 파라미터
- 상태 - 배포 상태(합격 또는 실패 솔루션) 또는 (합격 또는 실패 문제 해결)
- 오류 메시지 - 상태 필드의 일반 오류 메시지
- Generator_id - Security Hub 규칙 정보
- 유형 - 문제 해결 유형 및 이름
- productArn - Security Hub가 배포된 리전
- finding_triggered_by - 수행된 문제 해결 유형(사용자 지정 작업 또는 자동 트리거)

AWS는이 설문 조사를 통해 수집된 데이터를 소유합니다. 데이터 수집에는 AWS 개인 정보 보호 고지가 적용됩니다. 이 기능을 옵트아웃하려면 AWS CloudFormation 템플릿을 시작하기 전에 다음 단계를 완료하세요.

1. AWS CloudFormation 템플릿을 로컬 하드 드라이브에 다운로드합니다.
2. 텍스트 편집기를 사용하여 AWS CloudFormation 템플릿을 엽니다.
3. AWS CloudFormation 템플릿 매핑 섹션을 다음에서 수정합니다.

```
Mappings:
Solution:
Data:
```

```
SendAnonymizedUsageData: 'Yes'
```

변경 후:

```
Mappings:
Solution:
Data:
SendAnonymizedUsageData: 'No'
```

4. AWS CloudFormation 콘솔에 로그인합니다.
5. 스택 생성을 선택합니다.
6. 스택 생성 페이지, 템플릿 지정 섹션에서 템플릿 파일 업로드를 선택합니다.
7. 템플릿 파일 업로드에서 파일 선택을 선택하고 로컬 드라이브에서 편집한 템플릿을 선택합니다.
8. 다음을 선택하고 이 안내서의 자동 배포 섹션에 있는 스택 시작의 단계를 따르세요.

관련 리소스

- AWS Security Hub를 사용한 자동 응답 및 해결
- CIS Amazon Web Services Foundations 벤치마크, 버전 1.2.0
- 기반 보안 모범 사례 표준
- PCI DSS(지불 카드 산업 데이터 보안 표준)
- NIST(National Institute of Standards and Technology) SP 800-53 개정 5

기여자

다음 개인이 이 문서에 기여했습니다.

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- 최대 Granat
- 팀 메카리
- Aaron Schuetter

- Andrew Yankowsky
- Josh Moss
- Ryan Garay
- Thiemo Belmega
- Mykhailo Markhain

개정

게시 날짜: 2020년 8월(마지막 업데이트: 2025년 1월)

GitHub 리포지토리의 CHANGELOG.md://를 방문하여 버전별 개선 사항 및 수정 사항을 추적하세요.

고지 사항

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서: (a) 정보 제공 목적으로만 사용되며, (b) 예고 없이 변경될 수 있는 AWS의 현재 제품 제공 및 관행을 나타내며, (c) AWS 및 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정이나 보장도 생성하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 표현 또는 조건 없이 "있는 그대로" 제공됩니다. 고객에 대한 AWS의 책임과 책임은 AWS 계약의 적용을 받으며,이 문서는 AWS와 고객 간의 계약의 일부이거나 수정하지 않습니다.

AWS의 자동 보안 응답은 Apache Software Foundation에서 제공되는 Apache 라이선스 버전 2.0의 약관에 따라 라이선스가 부여됩니다.

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