



KRUG SECURITY MEET-UP

# AWS Native Service를 이용한 보안 관제 방안 제시

2024.04.25

AWS Professional Services

정하윤

# Incident Manager



# 인시던트란?

---

비즈니스 운영에 중대한 영향을 미칠 수 있는  
예상치 못한 중단이나 서비스 품질 저하의 원인이 되는 것들



AWS 네이티브 서비스인 Security Hub Standards, GuardDuty,  
Inspector등 에서 탐지되는 Findings를 인시던트로 정의

# Incident Manager

---

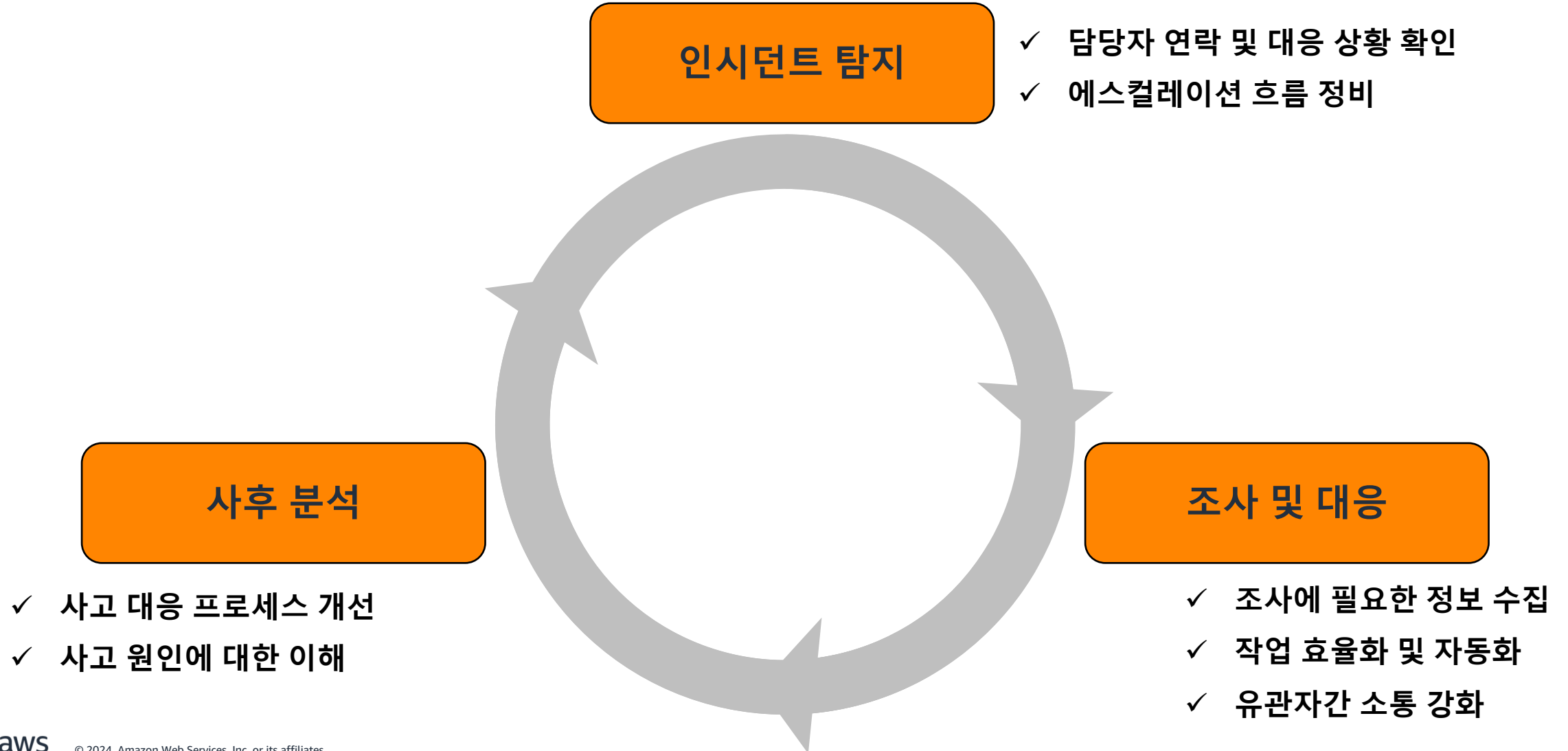


Incident Manager

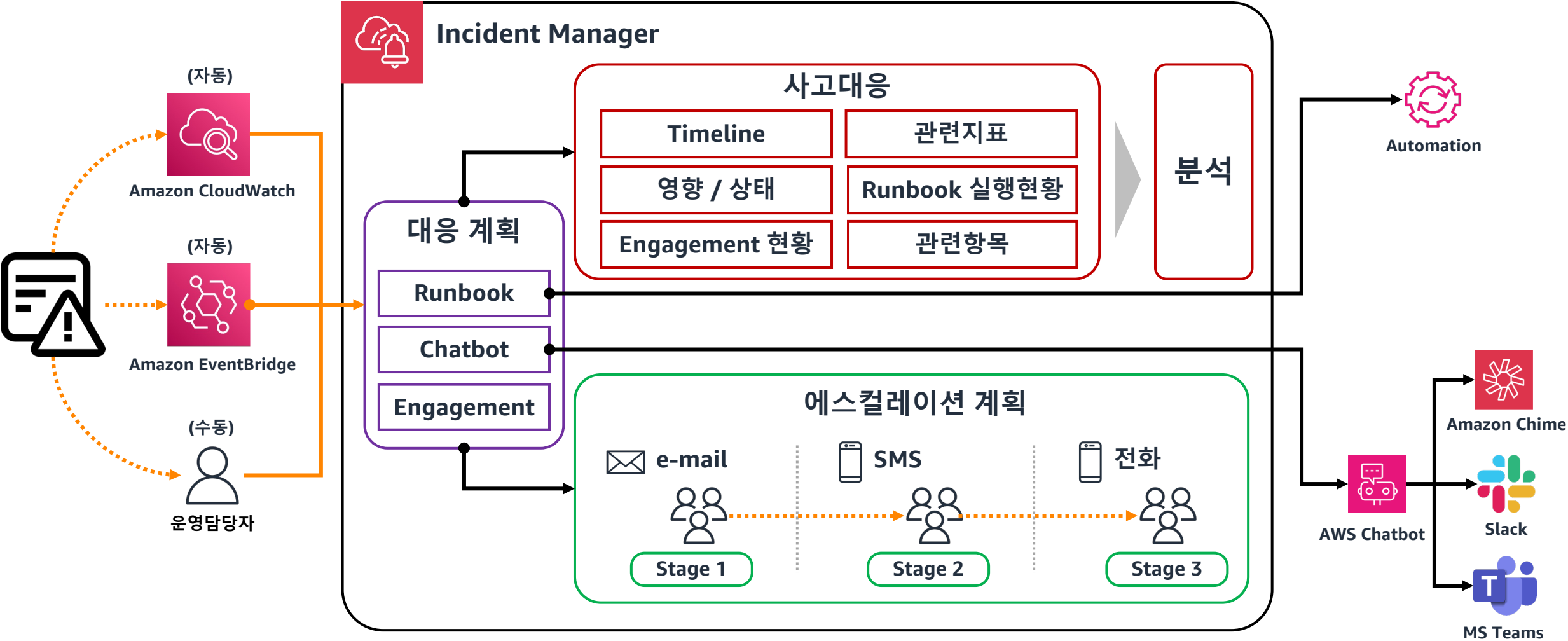
인시던트 해결과 완화에 소요되는 시간을 단축하고  
관련된 **프로세스를 관리** 할 수 있는 기능

인시던트를 **탐지 및 조사**하고, **문제를 해결**하고,  
서비스를 복원하기 위해 취하는 단계를 **문서화**

# 인시던트 관리 프로세스



# Incident Manager Overview



# Incident Manager

## 연락처

- ✓ 인시던트 발생 시 수신 연락처
- ✓ e-mail, SMS, 전화로 수신 가능

## 에스컬레이션 계획

- ✓ 순환 호출처럼 연락처의 응답 여부에 따라 다음 연락처로 자동 에스컬레이션

## 온콜 스케줄

- ✓ 인시던트 발생 시 연락처 로테이션 할 수 있는 스케줄 설정
- ✓ 일, 주, 월 단위로 로테이션 가능

## 채팅 채널

- ✓ 인시던트 업데이트 및 알림을 Chatbot을 통한 채팅 채널로 연동 가능
- ✓ Amazon Chime, Slack, MS Teams 지원

## Runbook

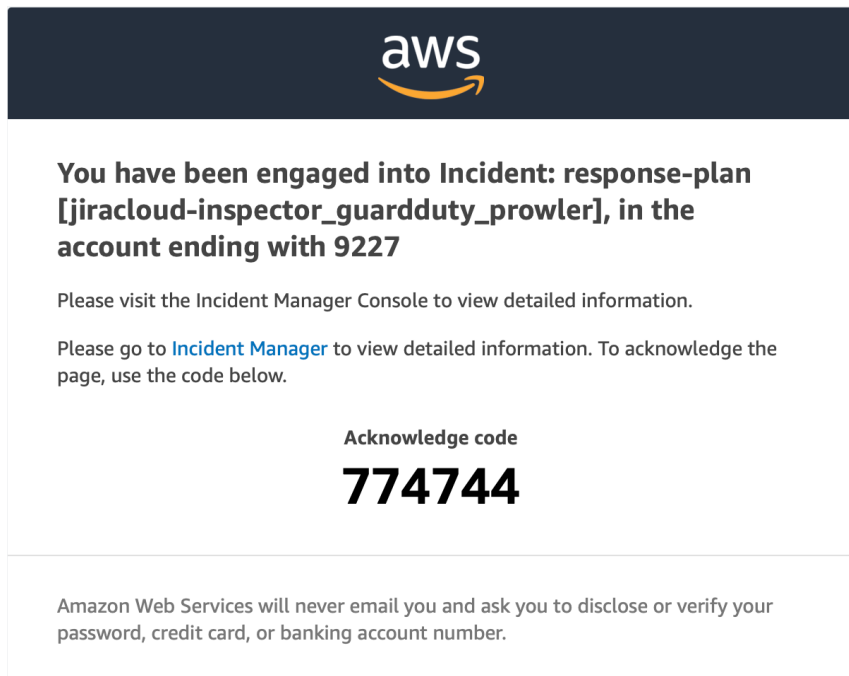
- ✓ 인시던트 대응에 필요한 절차서 연동
- ✓ 애플리케이션 및 인프라 작업 자동화 가능

## 대응 계획

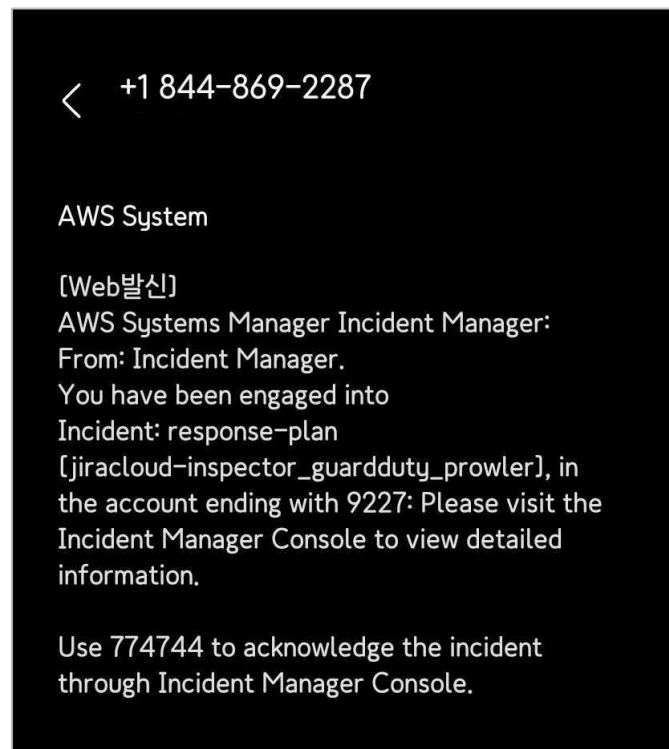
- ✓ 연락처, 에스컬레이션 계획, 온콜 스케줄, 채팅 채널, Runbook을 맵핑
- ✓ 인시던트 발생 시 대응 계획 호출



# 연락처 - 참여 계획



e-mail 알림



SMS 알림



음성 알림

# 온콜 스케줄

- ✓ 온콜 담당자 그룹 내에서 로테이션 설정 가능
- ✓ 로테이션 빈도는 일, 주, 월 단위로 선택
- ✓ 설정한 스케줄에 대한 예외(=일정 기간 동안 근무자 변경) 설정 가능

3/11 ~ 3/15

제 1 연락처



근무자 A

3/18 ~ 3/22



근무자 B

3/25 ~ 3/29



근무자 A

제 2 연락처



근무자 B



근무자 A



근무자 B

# 온콜 스케줄 설정

first

로테이션 이름

first

이름은 1자~255자여야 합니다. 유효한 문자는 a-z, A-Z, 0-9, 공백, \_ - (하이픈)입니다.

시작 날짜

이 로테이션이 시작되는 날짜를 입력합니다.

2024/02/16

시간대

로테이션의 기준이 되는 시간대를 선택합니다.

Asia/Seoul

로테이션 시작 시간

이 로테이션의 시프트 커버리지가 시작되는 시간을 입력합니다.

00:00

로테이션 종료 시간

이 로테이션의 시프트 커버리지가 종료되는 시간을 입력합니다.

12:00

시간은 24시간 형식(hh:mm)으로 입력해야 합니다.

시간은 24시간 형식(hh:mm)으로 입력해야 합니다.

☐ 24시간 커버리지

24시간 커버리지를 켭니다. 24시간 주기가 시작되는 시간을 지정할 수 있습니다.

근무일

이 로테이션을 활성화할 일자를 선택합니다.

☒ 일요일 ☒ 월요일 ☒ 화요일 ☒ 수요일 ☒ 목요일 ☒ 금요일 ☒ 토요일

연락처

순서

연락처

☐ 1 sec-engineer

☐ 2 sec-manager

반복 설정

시프트 반복 빈도

시프트 재발생 빈도를 선택합니다.

매주

시프트 기간

시프트가 지속되는 주 수를 입력합니다.

1

활성화 요일 선택

주 단위 순환

second

로테이션 이름

second

이름은 1자~255자여야 합니다. 유효한 문자는 a-z, A-Z, 0-9, 공백, \_ - (하이픈)입니다.

시작 날짜

이 로테이션이 시작되는 날짜를 입력합니다.

2024/03/07

시간대

로테이션의 기준이 되는 시간대를 선택합니다.

Asia/Seoul

로테이션 시작 시간

이 로테이션의 시프트 커버리지가 시작되는 시간을 입력합니다.

12:00

로테이션 종료 시간

이 로테이션의 시프트 커버리지가 종료되는 시간을 입력합니다.

00:00

시간은 24시간 형식(hh:mm)으로 입력해야 합니다.

시간은 24시간 형식(hh:mm)으로 입력해야 합니다.

☐ 24시간 커버리지

24시간 커버리지를 켭니다. 24시간 주기가 시작되는 시간을 지정할 수 있습니다.

근무일

이 로테이션을 활성화할 일자를 선택합니다.

☒ 일요일 ☒ 월요일 ☒ 화요일 ☒ 수요일 ☒ 목요일 ☒ 금요일 ☒ 토요일

연락처

순서

연락처

☐ 1 sec-manager

반복 설정

시프트 반복 빈도

시프트 재발생 빈도를 선택합니다.

매주

시프트 기간

시프트가 지속되는 주 수를 입력합니다.

1

# 온콜 스케줄 캘린더

3월 2024

Asia/Seoul (local timezone)

🔄

시프트 재정의 생성

◀

오늘

▶

| 월요일                                                                 | 화요일                                                                 | 수요일                                                                 | 목요일                                                                                                 | 금요일                                                                 | 토요일                                                                 | 일요일                                                                 |
|---------------------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------|
| 26<br>00:00 - 23:59<br>sec-manager                                  | 27<br>00:00 - 23:59<br>sec-manager                                  | 28<br>00:00 - 23:59<br>sec-manager                                  | 29<br>00:00 - 23:59<br>sec-manager                                                                  | 01<br>00:00 - 23:59<br>sec-manager                                  | 02<br>00:00 - 00:00<br>sec-manager                                  | 03                                                                  |
| 04<br>00:00 - 23:59<br>sec-manager                                  | 05<br>00:00 - 23:59<br>sec-manager                                  | 06<br>00:00 - 23:59<br>sec-manager                                  | 07<br>00:00 - 00:06<br>sec-manager<br>00:06 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager | 08<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager | 09<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  | 10<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  |
| 11<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  | 12<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  | 13<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  | 14<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager                                  | 15<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager | 16<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager | 17<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager |
| 18<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager | 19<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager | 20<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager | 21<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager                                 | 22<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  | 23<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  | 24<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  |
| 25<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  | 26<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  | 27<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager  | 28<br>00:00 - 12:00<br>sec-manager<br>12:00 - 23:59<br>sec-manager                                  | 29<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager | 30<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager | 31<br>00:00 - 12:00<br>sec-engineer<br>12:00 - 23:59<br>sec-manager |

☒ first

sec-engineer

sec-manager

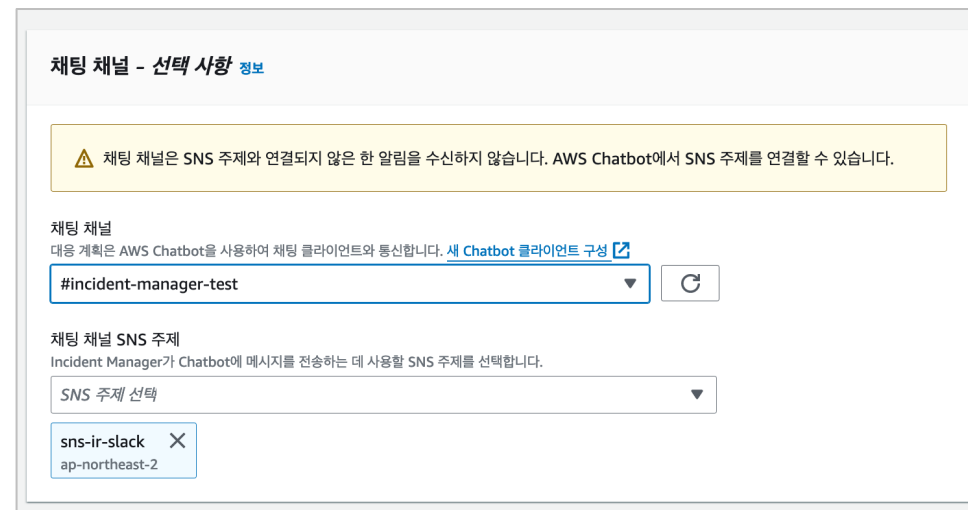
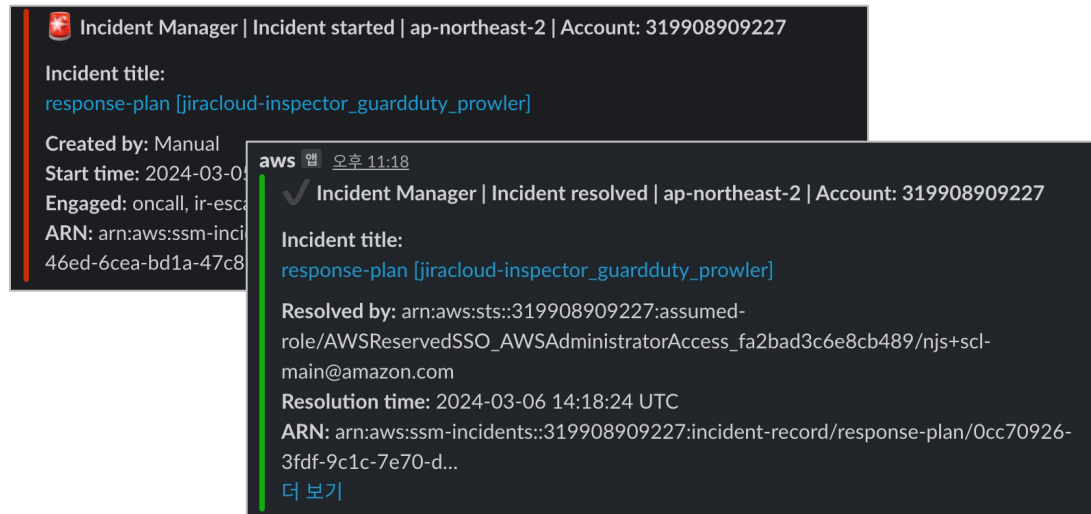
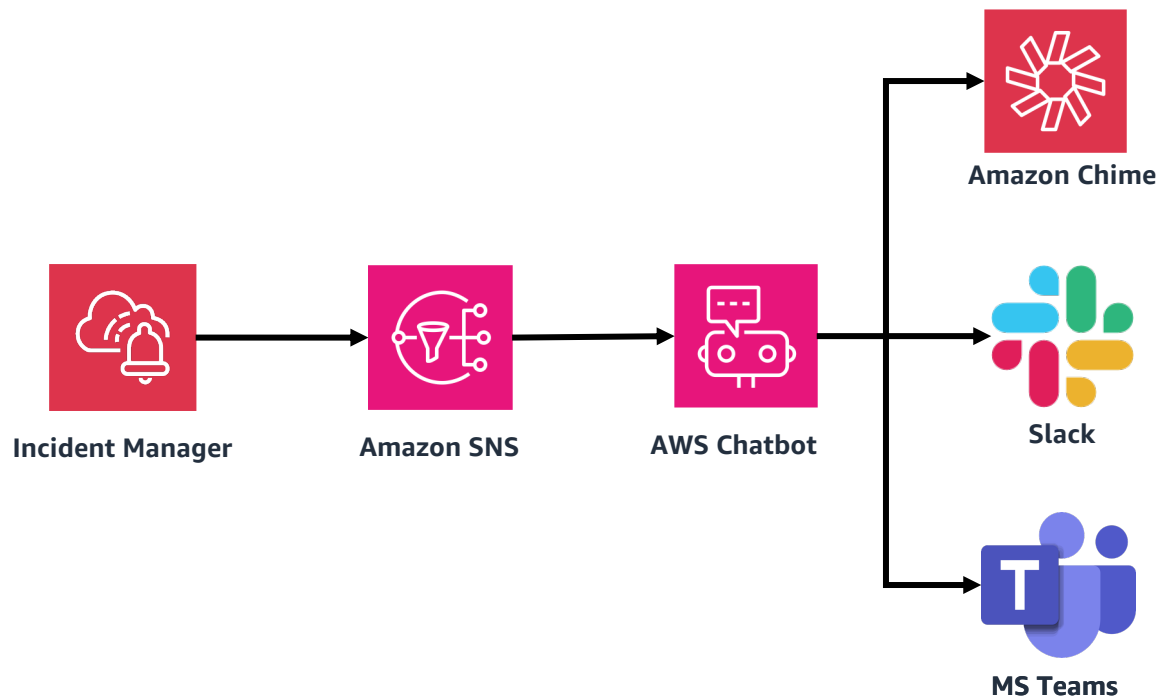
☒ second

sec-manager

☐ 재정의된 시프트

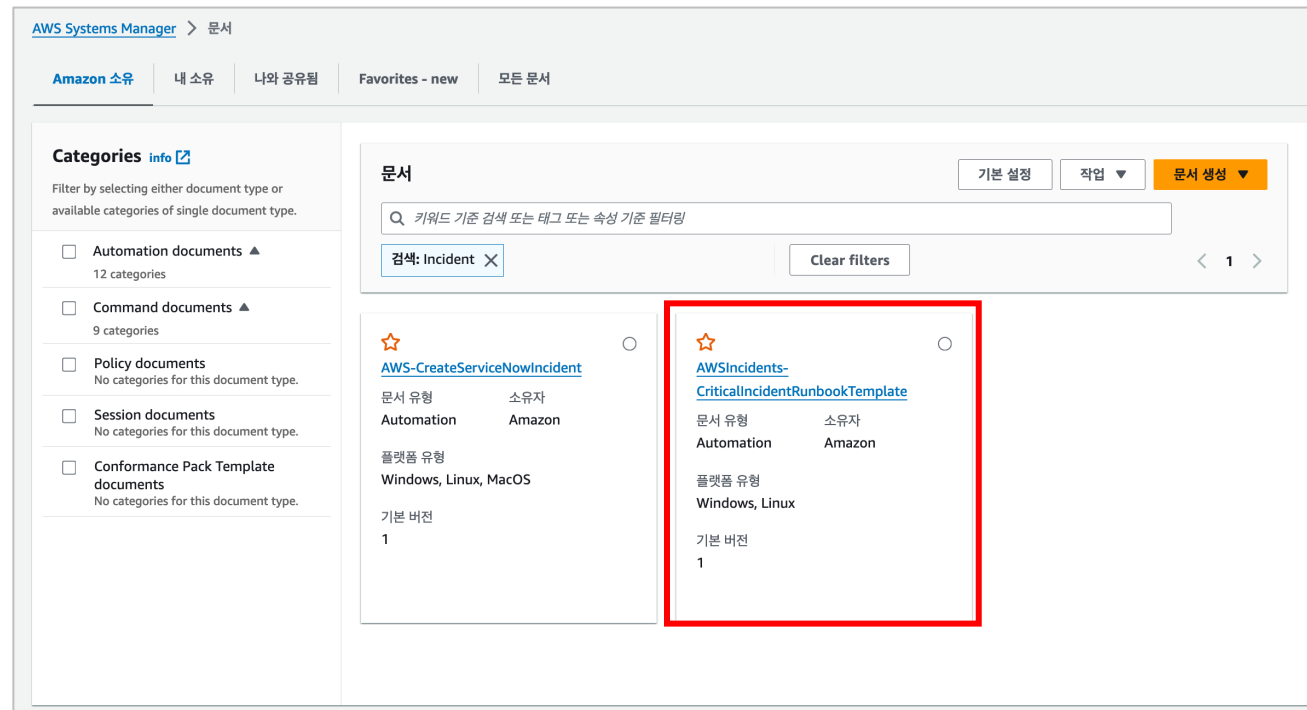
# 채팅 채널

## ✓ 인시던트 업데이트 및 알림을 채팅 채널로 푸시



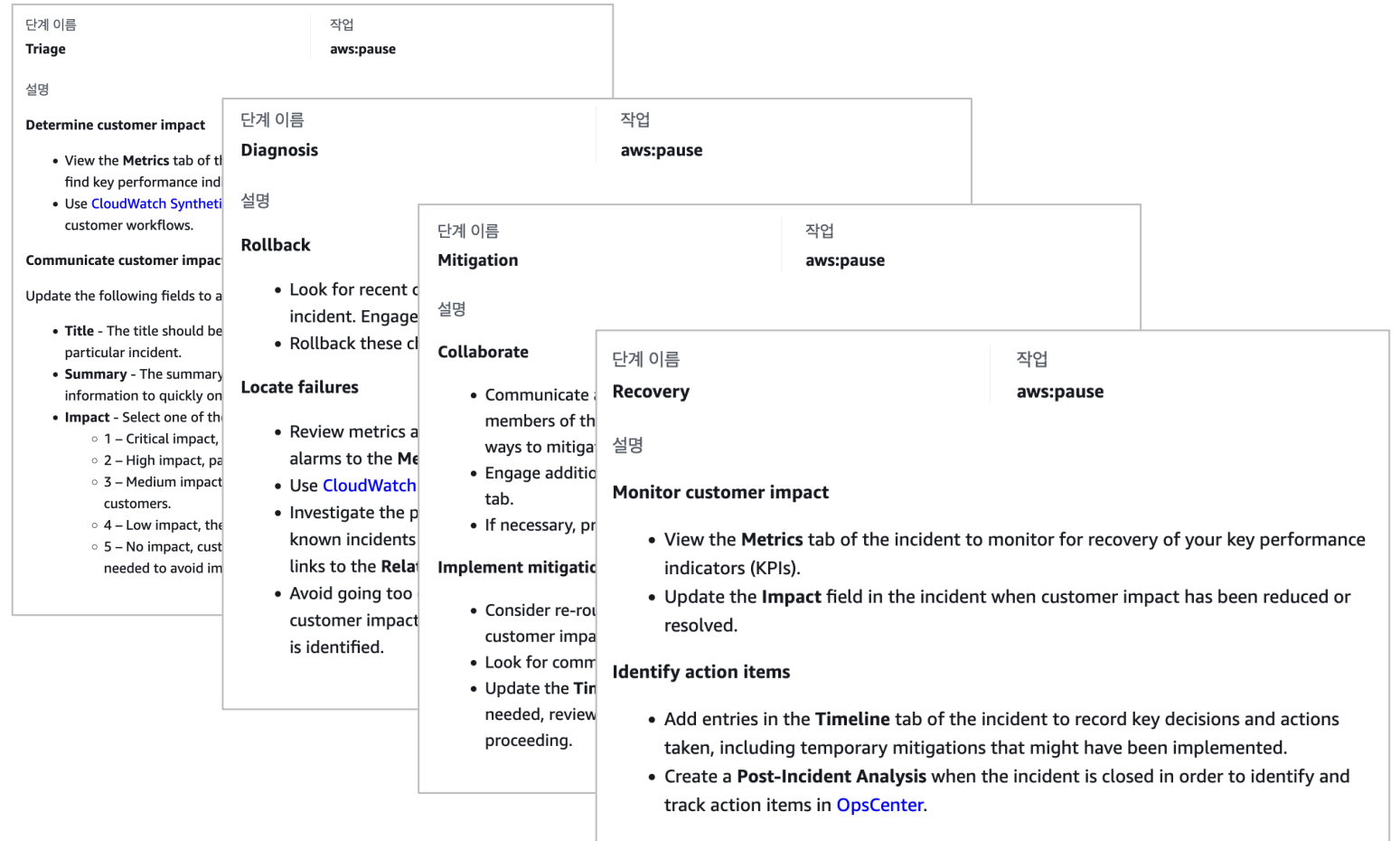
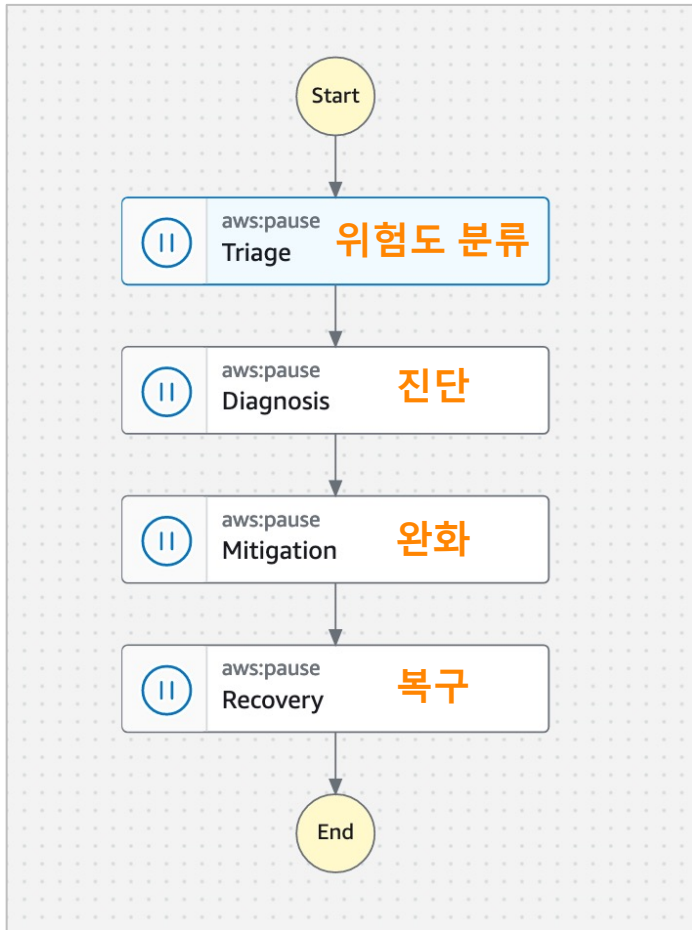
# Runbook

- ✓ 인시던트 발생 시 AWS Systems Manager Automation의 Runbook 호출 가능
- ✓ 인시던트 대응에 필요한 절차 및 처리 단계의 순차적 정의를 통한 대응 시간 단축 가능
- ✓ 인시던트 대응을 위한 Runbook 템플릿 제공



# Runbook Template - AWSIncidents-CriticalIncidentRunbookTemplate

✓ 사고 대응의 일반적인 단계가 정의되어 있으며, 각 단계별 수행 조치 명시



# 대응 계획

인시던트 기본값

제목

인시던트 제목은 고유하고 식별 가능하며 인시던트와 관련이 있어야 합니다. 인시던트 제목은 인시던트 목록에 표시되고 그 뒤에 인시던트 ARN이 표시됩니다.

response-plan

영향

영향은 고객에게 미치는 영향과 인시던트의 범위를 정의합니다.

중요

요약 - 선택 사항

요약은 인시던트의 개요를 제공하는 데 사용되는 간단한 설명입니다. Markdown을 사용할 수 있습니다.

security check

Markdown 미리 보기 표시

중복 제거 문자열 - 선택 사항

중복 제거 문자열은 인시던트 관리자가 동일한 근본 원인으로 여러 인시던트를 식별할 수 있도록 합니다.

중복 제거 문자열 입력

인시던트 태그 - 선택 사항

이 응답 계획을 사용하여 시작된 모든 인시던트에 이러한 태그가 있음

새 태그 추가

태그를 최대 50개 더 추가할 수 있습니다.

런북 구성 - 선택 사항 정보

런북을 생성할 때 필요한 권한이 있는 IAM 역할을 지정해야 합니다. 이러한 권한을 부여하지 않으면 런북을 실행할 수 없습니다.

런북

런북은 수동 지침과 자동화된 완화를 결합한 Systems Manager 자동화 문서입니다. [새 런북 구성](#)

☒ 템플릿에서 런북 복제

기본 인시던트 관리자 런북을 복제합니다. [템플릿 보기](#)

☐ 기존 런북 선택

기존 자동화 런북을 선택합니다.

런북 이름

런북 이름은 런북의 목적을 설명합니다.

이름 입력

이름은 3~128자여야 합니다. 유효한 문자는 a~z, A~Z, 0~9, \_ 및 - 입니다.

런북 서비스 역할

인스턴트 관리자가 이 런북 워크플로를 시작하는 데 필요한 권한이 있는 IAM 역할을 선택합니다. 필요한 경우 이러한 권한을 사용하여 새 IAM 역할을 생성할 수 있습니다. [새 역할 생성에 대해 자세히 알아보세요](#)

☒ 새 서비스 역할 생성

필요한 최소 권한을 제공하는 새 서비스 역할을 생성합니다.

☐ 기존 서비스 역할 사용

기존 서비스 역할을 사용하여 런북 워크플로를 시작합니다.

역할 이름

역할 이름 입력

이름은 최대 64자일 수 있습니다. 유효한 문자: a~z, A~Z, 0~9 및 +, -, @, \_

권한 세부 정보 보기

## 채팅 채널 - 선택 사항 정보

채팅 채널은 SNS 주제와 연결되지 않은 한 알림을 수신하지 않습니다. AWS Chatbot에서 SNS 주제를 연결할 수 있습니다.

채팅 채널

대응 계획은 AWS Chatbot을 사용하여 채팅 클라이언트와 통신합니다. [새 Chatbot 클라이언트 구성](#)

#incident-manager-test

채팅 채널 SNS 주제

Incident Manager가 Chatbot에 메시지를 전송하는 데 사용할 SNS 주제를 선택합니다.

SNS 주제 선택

sns-ir-slack  
ap-northeast-2

## 참여 - 선택 사항 정보

활성화되지 않은 연락처 채널은 참여할 수 없습니다.

참여

연락처, 에스컬레이션 계획 및 참여하려는 대기 일정을 선택하세요. [새 연락처 생성](#) [새 에스컬레이션 계획 생성](#) [새로운 대기 일정 생성](#)

참여 채널 찾기

ir-escalation  
에스컬레이션 계획

oncall  
대기 일정

 © 2024, Amazon Web Services, Inc. or its affiliates.

# 인시던트 확인

✓ 지표, 타임라인, Runbook, 참여 계획 등을 각 탭에서 확인 가능

AWS Systems Manager > 인시던트 관리자 > response-plan [jiracloud-inspector\_guarddduty\_pr...

response-plan [jiracloud-inspector\_guarddduty\_prowler]

↺

새로 고침 간격: 꺼짐 ▼

속성 편집

인시던트 해결

상태  
열림

영향  
중요

채팅 채널 #incident-manager-test

기간  
3시간 11분

런북  
-

진단  
-

참여  
2개 참여됨

개요

진단

타임라인

런북

참여

관련 항목

속성

요약

편집

security check

Event rule ARN: arn:aws:events:ap-northeast-2:319908909227:rule/jiracloud-inspector\_guarddduty\_prowler

Description: Security Hub Findings - Imported

Event source: aws.securityhub

Resources: arn:aws:securityhub:ap-northeast-2::product/aws/config/arn:aws:config:ap-northeast-2:319908909227:config-rule/config-rule-8kdfb4/finding/da88e8511dca0ba0103d3d16cc5045c56d0cabf5

Timestamp: 2024-03-06 14:19:04 UTC

Detail:

findings:

- ProductArn: arn:aws:securityhub:ap-northeast-2::product/aws/config
  - Types:
    - Software and Configuration Checks
  - Description: "This finding is created for a resource compliance change for config\ \ rule: elb-deletion-protection-enabled"
  - ProductName: Config
  - Compliance:
    - Status: FAILED
  - CreatedAt: 2024-03-05T07:13:15.937Z

# 인시던트 확인 - 타임라인

개요

진단

타임라인

런북

참여

관련 항목

속성

타임라인 정보

삭제

편집

추가

최신 항목 먼저 표시

☐ 사용자 지정 이벤트만 표시

날짜

2024년 3월 6일

UTC 오프셋

UTC+9:00

오전 01:05:12

- https://njs1120.atlassian.net/jira/servicedesk/projects/10001/queues/issue/MS-2397이(가) 관련 항목에 추가되었습니다.

항목 추가됨

오전 01:05:03

- 상위 OpsItem arn:aws:ssm:ap-northeast-2:319908909227:opsitem/oi-33fb7b56a065이(가) 관련 항목에 추가되었습니다.

항목 추가됨

오전 01:05:03

- ir-escalation 에스컬레이션 계획에서 sec-manager을(를) 참여시킴

참여 중인 연락처

오전 01:05:03

- oncall 대기 일정에서 sec-manager을(를) 참여시킴

참여 중인 연락처

오전 01:05:00

- 인시던트 response-plan [gd-event-capture]이(가) 생성되었습니다.

인시던트 레코드 생성됨

오전 01:05:00

- EventBridge 규칙 gd-event-capture이(가) 소스 aws.guardduty에서 일치했습니다.

EventBridge 규칙

추가 로드

# 인시던트 대응 – Runbook 실행

- ✓ 인시던트 대응을 위한 Runbook을 Incident Manager 콘솔에서 실행 가능

런북 시작

☐ 내 소유

☒ Amazon 소유

☐ 나와 공유됨

런북

Q 런북 찾기

< 1 2 3 4 5 6 7 8 ... >

| 이름                                                                               | 기본 버전 |
|----------------------------------------------------------------------------------|-------|
| <input type="radio"/> <a href="#">AWS-ASGEnterStandby</a>                        | 1     |
| <input type="radio"/> <a href="#">AWS-ASGExitStandby</a>                         | 1     |
| <input type="radio"/> <a href="#">AWS-AddOpsitemDedupStringToEventBridgeRule</a> | 1     |
| <input type="radio"/> <a href="#">AWS-ArchiveEBSVolumeSnapshots</a>              | 1     |
| <input type="radio"/> <a href="#">AWS-ArchiveS3BucketToIntelligentTiering</a>    | 1     |

버전

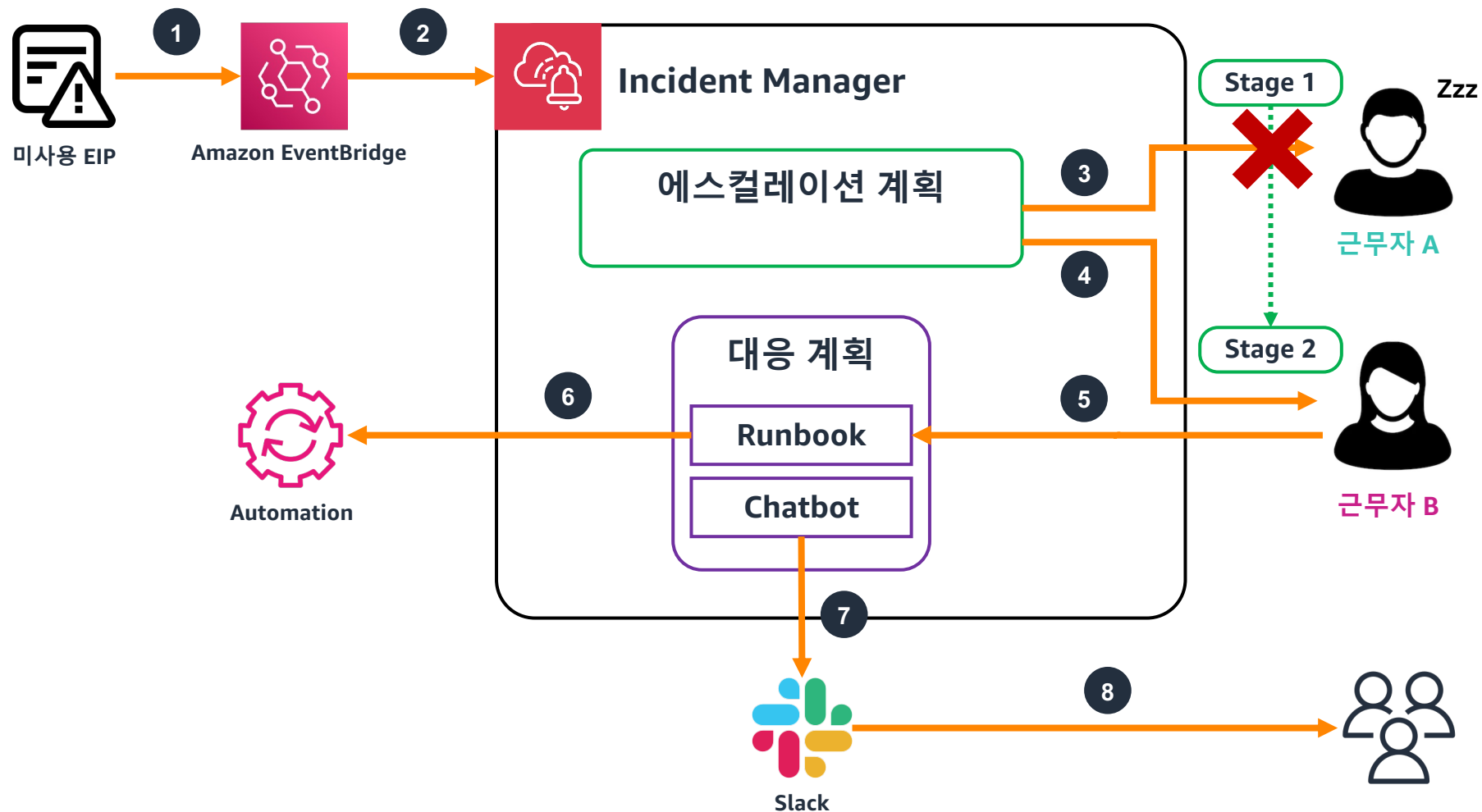
버전 선택

취소

시작



# Flow

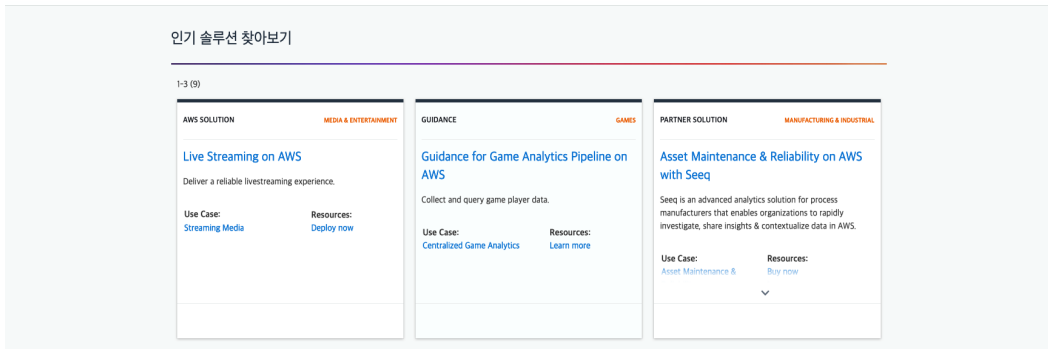
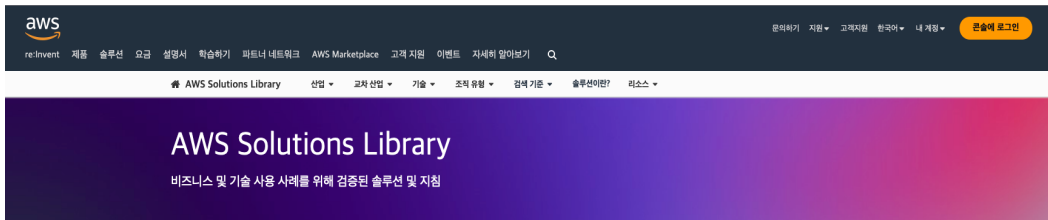


- 1 Config <-> Security Hub 연계를 통한 Findings 감지
- 2 EventBridge를 통해 Incident Manager로 인시던트 생성
- 3 사전 정의된 에스컬레이션 계획에 따라 근무자 A에게 알림
- 4 근무자 A 미응답, 근무자 B 알림
- 5 근무자 B가 Runbook으로 대응 시작
- 6 Automation을 통한 자동 조치
- 7 채팅 채널로 진행 상황 자동 전달
- 8 업무 유관자들은 Slack에서 인시던트 상태 및 처리 현황 확인

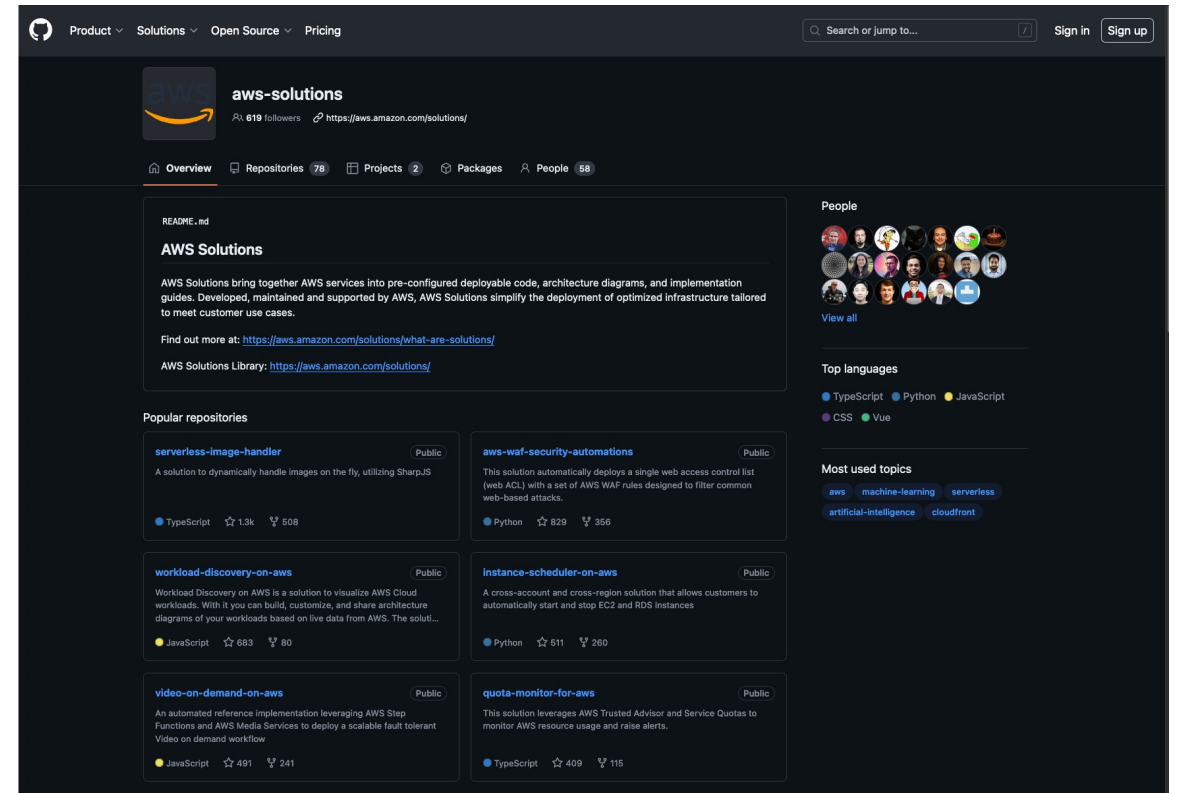
# Automated Security Response (ASR) on AWS

# AWS Solutions

솔루션이란 : Amazon Web Services는 비즈니스 과제를 신속하게 해결하기 위한 교육 정보가 포함된 맞춤형 서비스, 즉시 배포 가능한 소프트웨어 패키지, 사용자 정의 가능한 아키텍처를 제공합니다.

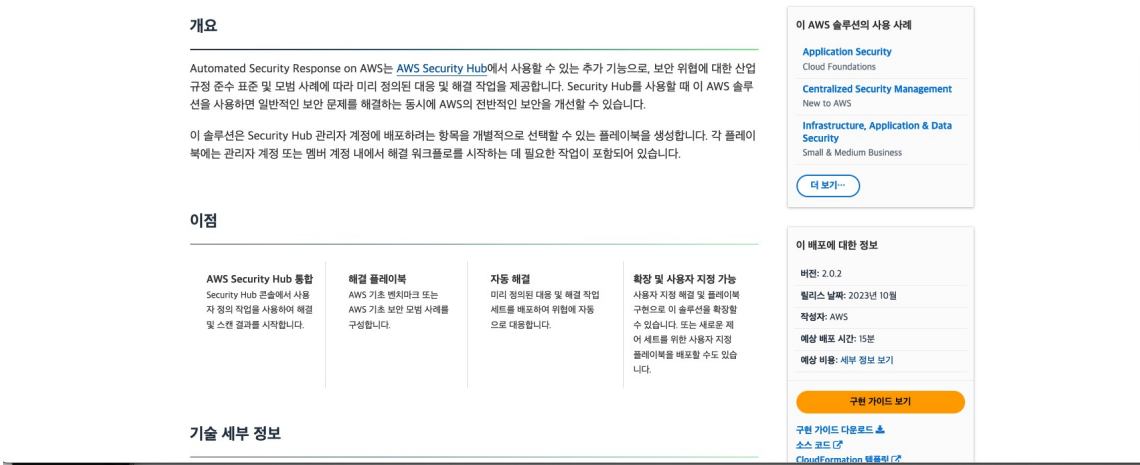


## AWS Solutions Library Page



## aws-solutions(github)





## aws-solutions(github)



# Automated Security Response on AWS

| Benefit             | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| AWS Security Hub 통합 | Control에 대한 Amazon EventBridge 규칙을 활성화하여 해당 제어에 대한 결과가 AWS Security Hub에 나타나는 즉시 자동으로 문제를 해결                              |
| 플레이북                | 5가지 업계 표준에 매핑되는 70개 이상의 보안 제어에 대한 수정:<br>- AWS 기초 보안 모범 사례, NIST SP 800-53 Rev. 5, CIS AWS 기초 벤치마크 v1.2.0/v1.4.0, PCI DSS |
| 자동 교정               | 위협에 자동으로 대응하기 위해 사전 정의된 대응 및 교정 조치 세트를 배포                                                                                 |
| 확장 가능하고 사용자 정의 가능   | 지정된 AWS Systems Manager 자동화 문서와 AWS IAM 역할을 배포 필요<br>솔루션에서 구현되지 않은 새로운 컨트롤 세트를 지원 시 사용자 지정 플레이북을 배포                       |
| 표준화된 교정             | 일관된 구현 및 감사를 쉽게 하기 위해 AWS 조직 전체의 보안 취약성 해결을 표준화                                                                           |



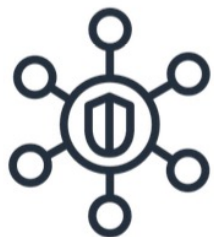
# Solution Deploy

| Account        | Deploy                                                       | 배포 리소스                                                                          |
|----------------|--------------------------------------------------------------|---------------------------------------------------------------------------------|
| Admin Account  | aws-sharr-deploy.template                                    | AWS Security Hub, Lambda, Event Bridge, DynamoDB, SNS, SQS 등                    |
| Member Account | aws-sharr-member.template<br>aws-sharr-member-roles.template | Systems Manager Document<br>Systems Manager Automation Document 실행을 위한 IAM Role |

| AWS 서비스                                            | 내용                                                      |
|----------------------------------------------------|---------------------------------------------------------|
| <a href="#">Amazon EventBridge</a>                 | 핵심. 결과가 수정될 때 오케스트레이터 단계 기능을 시작하는 이벤트를 배포               |
| <a href="#">AWS IAM</a>                            | 핵심. 다양한 리소스에 대한 수정을 허용하기 위해 많은 역할을 배포                   |
| <a href="#">AWS Lambda</a>                         | 핵심. 문제를 해결하기 위해 step function 오케스트레이터가 사용할 여러 람다 함수를 배포 |
| <a href="#">AWS Security Hub</a>                   | 핵심. 고객에게 AWS 보안 상태에 대한 포괄적인 보기를 제공                      |
| <a href="#">AWS Step Functions</a>                 | 핵심. AWS 시스템 관리자 API 호출을 통해 문제 해결 문서를 호출하는 오케스트레이터를 배포   |
| <a href="#">AWS Systems Manager</a>                | 핵심 . 실행될 교정 로직이 포함된 System Manager Document(문서 링크)를 배포  |
| <a href="#">Amazon CloudWatch</a>                  | 지원. 결과를 기록하는 데 사용할 로그 그룹을 배포. 경보와 함께 대시보드에 표시할 지표를 수집   |
| <a href="#">AWS DynamoDB</a>                       | 지원. 마지막 실행 수정을 저장하여 수정 예약을 최적화                          |
| <a href="#">Service Catalog AppRegistry</a>        | 지원. 비용 및 사용량을 추적하기 위해 배포된 스택에 대한 애플리케이션을 배포             |
| <a href="#">Amazon Simple Notification Service</a> | 지원. 수정이 완료되면 알림을 받는 SNS 주제를 배포                          |
| <a href="#">AWS SQS</a>                            | 솔루션이 많은 수정을 동시에 실행할 수 있도록 수정 예약을 지원                     |

# Security Hub

## What is AWS Security Hub?



AWS Security Hub는 보안 모범 사례 점검을 **지속적**으로 수행하고 AWS 및 타사 서비스의 보안 결과를 **원활하게** 집계하여 자동화된 대응을 가능하게 하는 클라우드 보안 태세 관리 서비스(CSPM)



자동화된  
지속적인 모범  
사례 점검



AWS 서비스 및  
파트너 서비스  
검사 결과와 통합



표준화된 결과  
형식 및 교차 리전  
간 집계



규제 및 특정  
프레임워크에  
부합하는 보안  
표준 제공



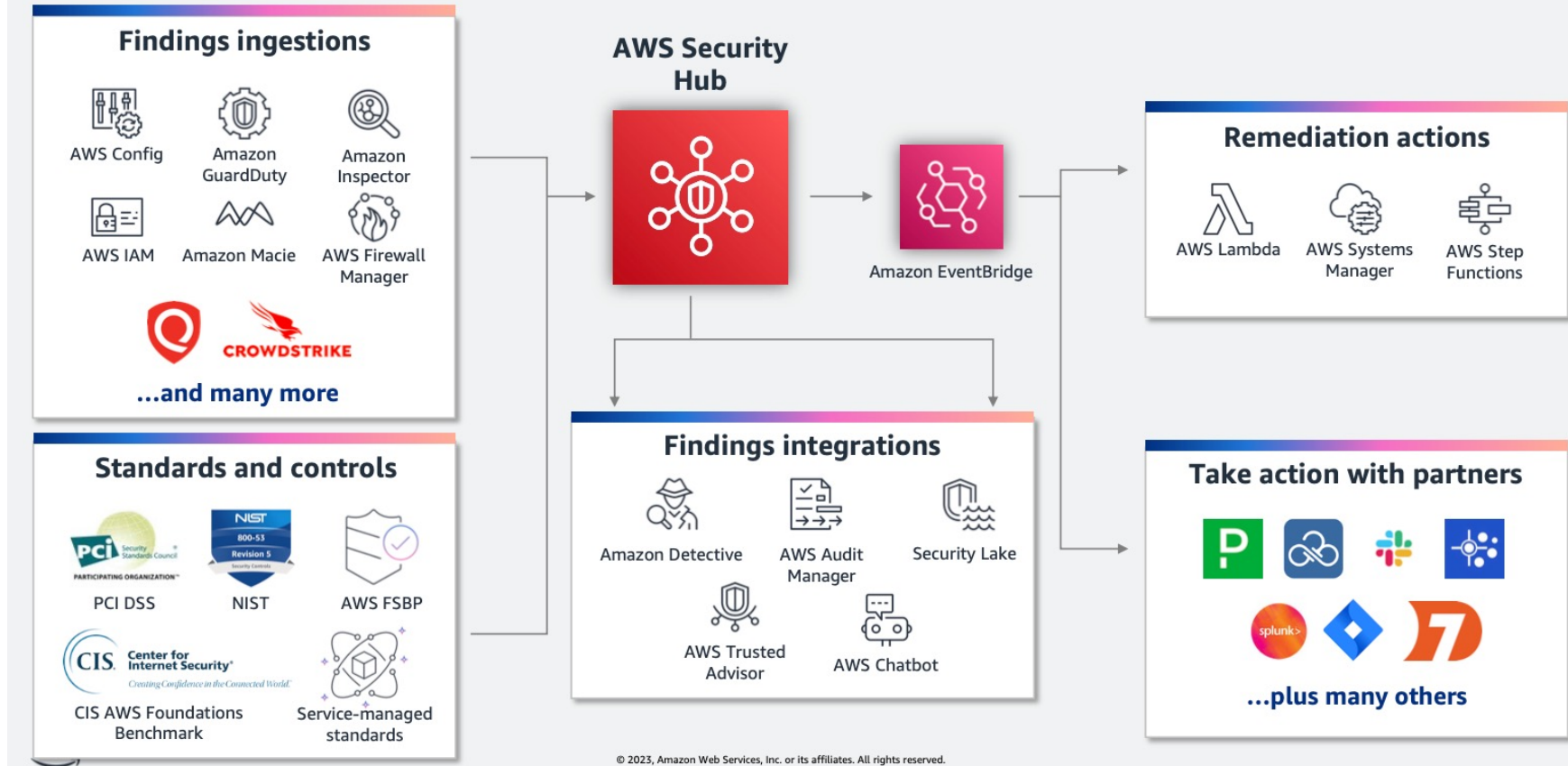
자동화된 대응,  
수정 및 강화 조치

2023년 아홉번째 - 참가자 사례발표 - Security Hub 9월 21일  
Security Hub 어디까지 써봤니?- 김대곤(AWS)



# Security Hub

## Security Hub information flows



2023년 아홉번째 - 참가자 사례발표 - Security Hub 9월 21일  
Security Hub 어디까지 써봤니?- 김대곤(AWS)

# Security Hub

Security Hub > Settings

- Accounts
- Custom actions
- Usage
- General

Custom actions

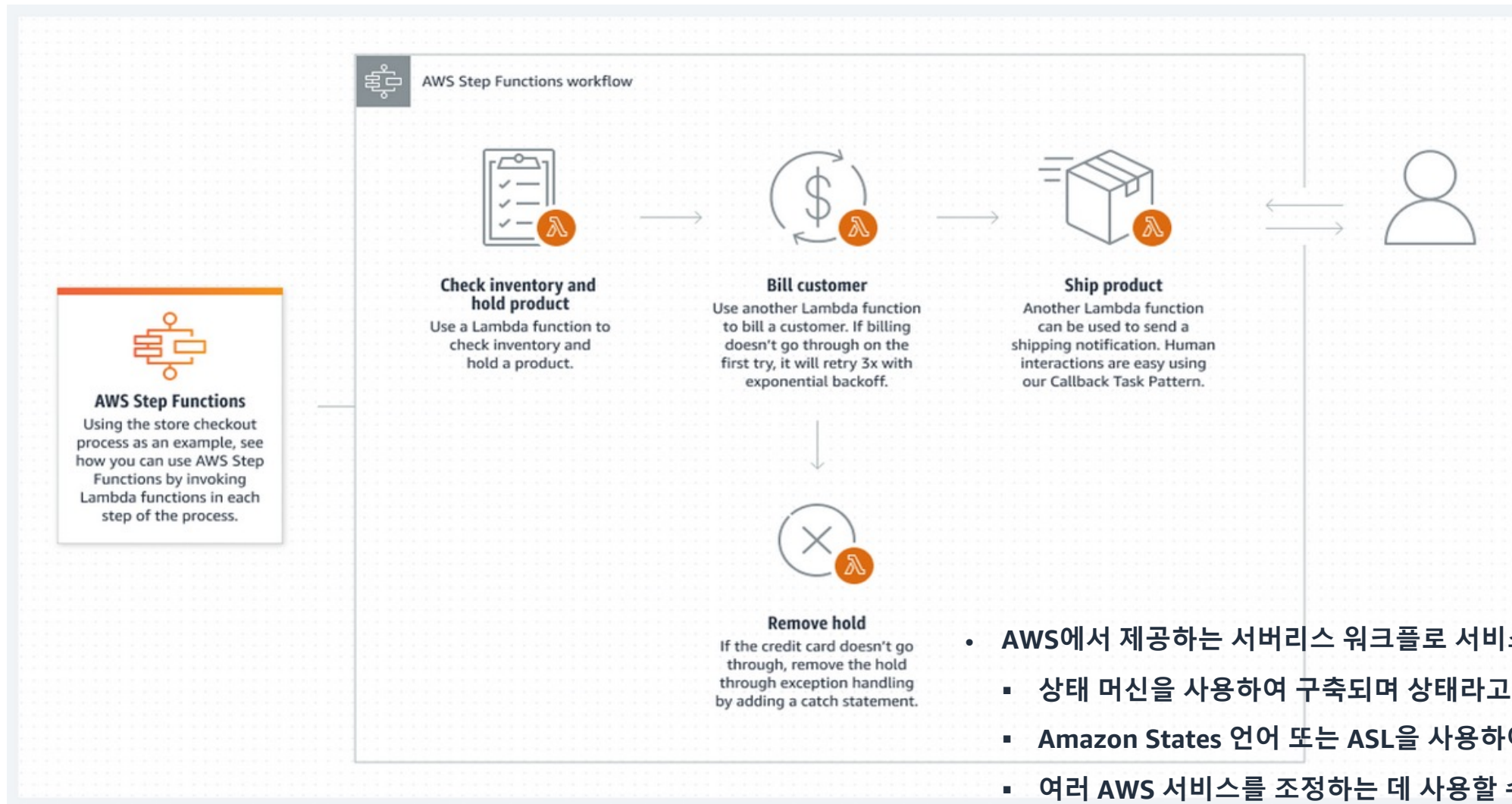
Configure AWS Security Hub to send selected insights and findings to CloudWatch Events by creating a custom action.

Delete

Create custom action

|                       | Name                | Description                                                                  | Custom action ARN                                                            |
|-----------------------|---------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <input type="radio"/> | Send to Email       | Send this finding to email                                                   | arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_email       |
| <input type="radio"/> | Isolate Instance    | Custom Action that will isolate the EC2 instance associated with the finding | arn:aws:securityhub:us-east-1:526039161745:action/custom/isolate_instance    |
| <input type="radio"/> | Terminate Instance  | Terminate the EC2 instance associated with this finding                      | arn:aws:securityhub:us-east-1:526039161745:action/custom/terminate_instance  |
| <input type="radio"/> | Send to Slack       | Send the details of this finding to Slack                                    | arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_slack       |
| <input type="radio"/> | Send to Security    | Send this to the security team so they can workflow it further               | arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_sec_wf      |
| <input type="radio"/> | Disable Access Keys | Disable the access keys associated with an IAM finding                       | arn:aws:securityhub:us-east-1:526039161745:action/custom/disable_access_keys |

# AWS Step Functions



# AWS Step Functions

## ✓ Workflow Studio: Low-code visual designer

The screenshot shows the AWS Step Functions Workflow Studio interface. On the left, there is a sidebar with a search bar and a list of actions under the 'Actions' tab. The actions listed are: AWS Lambda Invoke, Amazon SNS Publish, Amazon ECS RunTask, AWS Step Functions StartExecution, AWS Glue StartJobRun, AWS Glue DataBrew StartJobRun, Amazon EventBridge PutEvents, and AWS Batch SubmitJob. The central canvas displays a workflow diagram with a 'Start' node, a state machine box labeled 'Drag first state here', and an 'End' node. The right sidebar shows the configuration for the selected state machine, including a 'Comment' field (optional) and a 'TimeoutSeconds' field (optional) set to 600.

Workflow Studio는 드래그 앤 드롭 방식의 시각적 빌더입니다.

새로운 개발자를 위한 첫 번째 워크플로를 구축하는 시간이 단축됩니다.

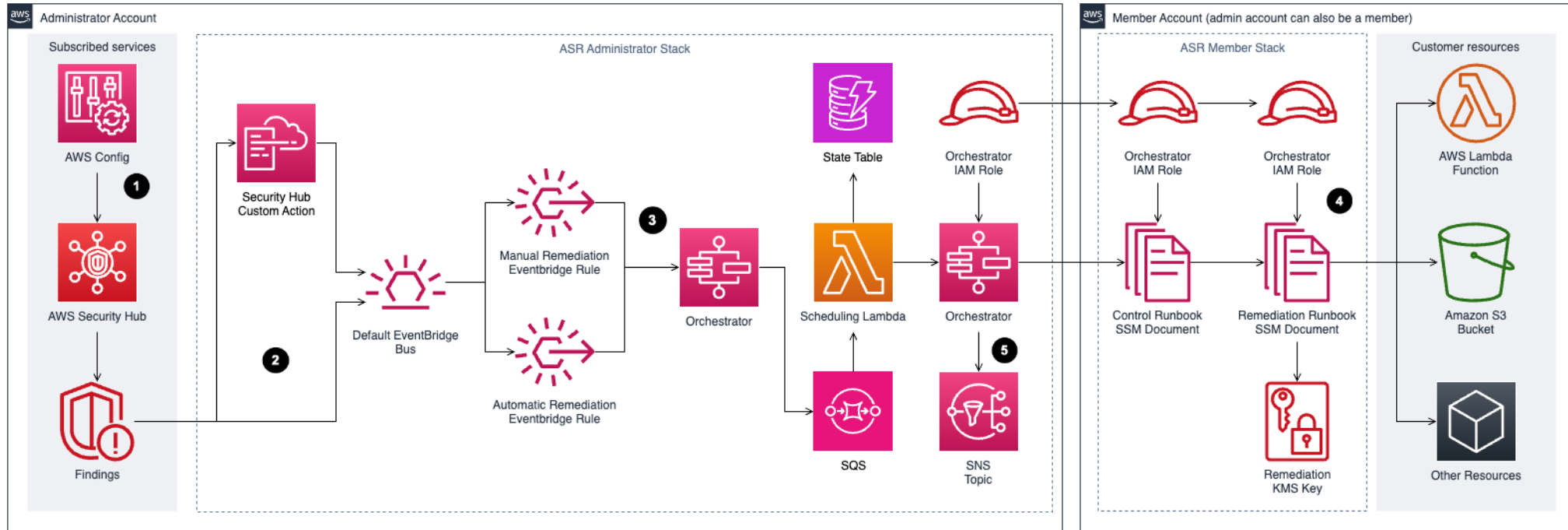
숙련된 개발자는 이를 사용하여 프로토타입을 구축하고 stackholders와 더 빠르게 공유할 수 있습니다.

AWS 서비스 아이콘, 자동 워크플로 레이아웃, 워크플로 정의의 시각적 신호를 사용하여 워크플로 시각화가 개선되었습니다.



# Automated Security Response on AWS

- ✓ AWS Security Hub와 함께 작동하고 보안 위협에 대한 업계 규정 준수 표준 및 모범 사례를 기반으로 사전 정의된 대응 및 해결 조치를 제공하는 추가 기능입니다.

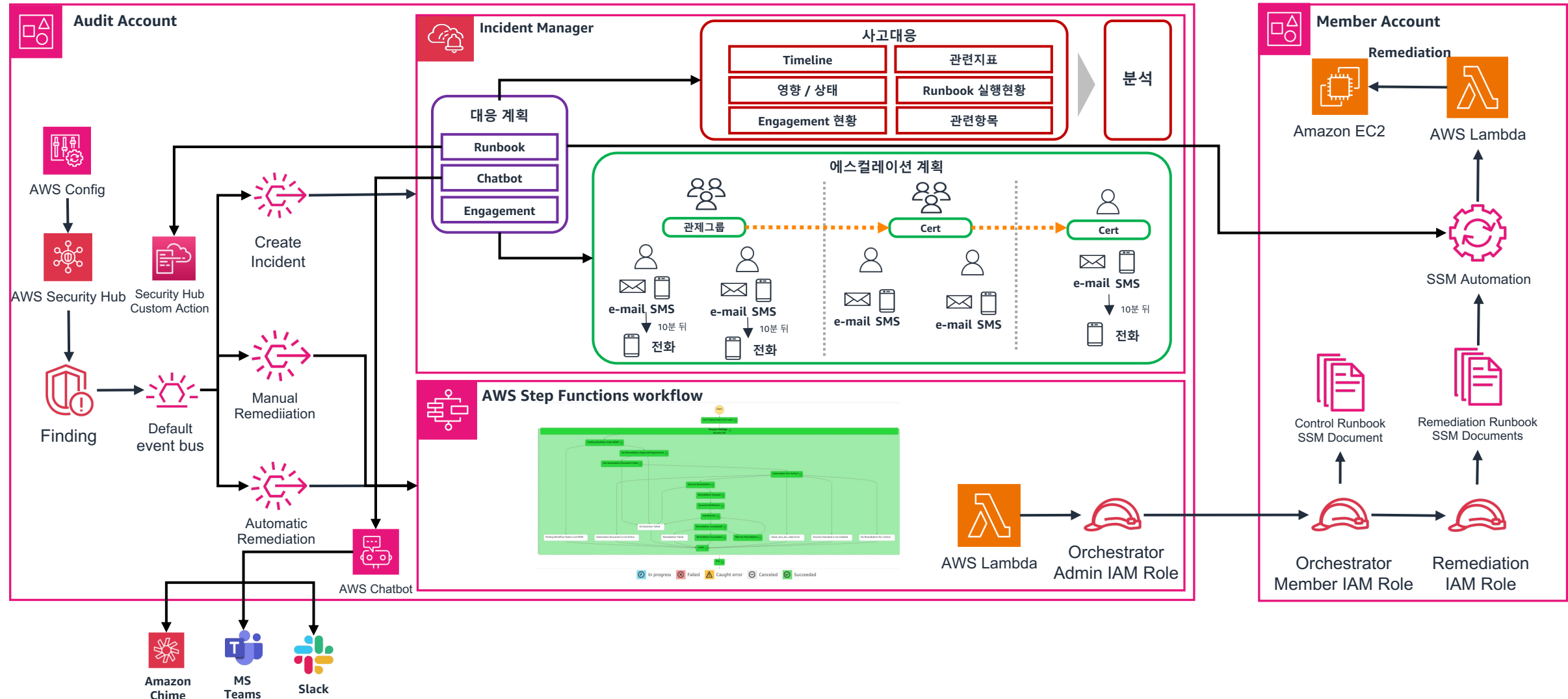


1. 탐지: SecuriHub Control, AWS Config, Amazon Guard Duty 및 AWS Firewall Manager 등에서 이벤트와 데이터를 수집하여 작동
2. 시작: Amazon EventBridge 이벤트 발생 후 해결하기 위해 AWS 플레이북에서 자동화된 보안 대응을 시작(Manual or Automation)
3. 오케스트레이션: 관리자 계정의 Step Functions는 보안 결과를 생성한 리소스가 포함된 멤버 계정의 수정을 호출
4. 해결: 멤버 계정의 AWS Systems Manager Automation Document는 리소스에 대한 결과를 해결하는 데 필요한 작업을 수행
5. 로그: Playbook 결과를 Amazon CloudWatch Logs 그룹에 기록, Amazon SNS에 알림을 보내고 Security Hub 결과를 업데이트

# 최종 아키텍처



# ASR with Incident Manager



# Demo



# 마무리

## • Useful

- Native Service 를 이용해 티켓 관리 시스템 및 자동화시스템을 만들 수 있음
- JIRA와도 연동 가능하며 부분 별로 분리도 가능
- 이메일, 문자, 전화가 정말 좋습니다 (단점은 ...영어로...)
- 스택을 사용해 복잡한 자동화 구성이 간단하게 배포
- 사용자 입장에서는 대응을 하는 방법이 매우 간단함
- 생각보다는 많은 Playbook과 저렴한 비용
- 지속적인 업데이트(기능도 추가 됨)

## • Challenge

- 경계보안, 다른 AWS Native Service에 대한 자동화는 포함 되어 있지 않음
- 모든 Control에 대한 Playbook이 존재하지는 않음
- Custom이 필요할 경우 SSM Document를 해석하고 작성 할 수 있어야 함



# Reference

- Automated Security Response on AWS
  - [https://aws.amazon.com/ko/solutions/implementations/automated-security-response-on-aws/?did=sl\\_card&trk=sl\\_card](https://aws.amazon.com/ko/solutions/implementations/automated-security-response-on-aws/?did=sl_card&trk=sl_card)
  - [automated-security-response-on-aws](#)
- AWS Security Hub
  - <https://aws.amazon.com/ko/security-hub/>
  - [https://github.com/awskrug/security-group/blob/main/files/AWSKRUG\\_2023\\_09\\_SecurityHub.pdf](https://github.com/awskrug/security-group/blob/main/files/AWSKRUG_2023_09_SecurityHub.pdf)
- AWS Step Functions
  - <https://aws.amazon.com/ko/step-functions/>
- Incident Manager
  - [https://docs.aws.amazon.com/ko\\_kr/incident-manager/latest/userguide/what-is-incident-manager.html](https://docs.aws.amazon.com/ko_kr/incident-manager/latest/userguide/what-is-incident-manager.html)





# Thank you!