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

Findings

AWS 네이티브 서비스인 Security Hub Standards, GuardDuty,

Inspector등 에서 탐지되는 Findings를 인시던트로 정의

Incident Manager

Incident Manager

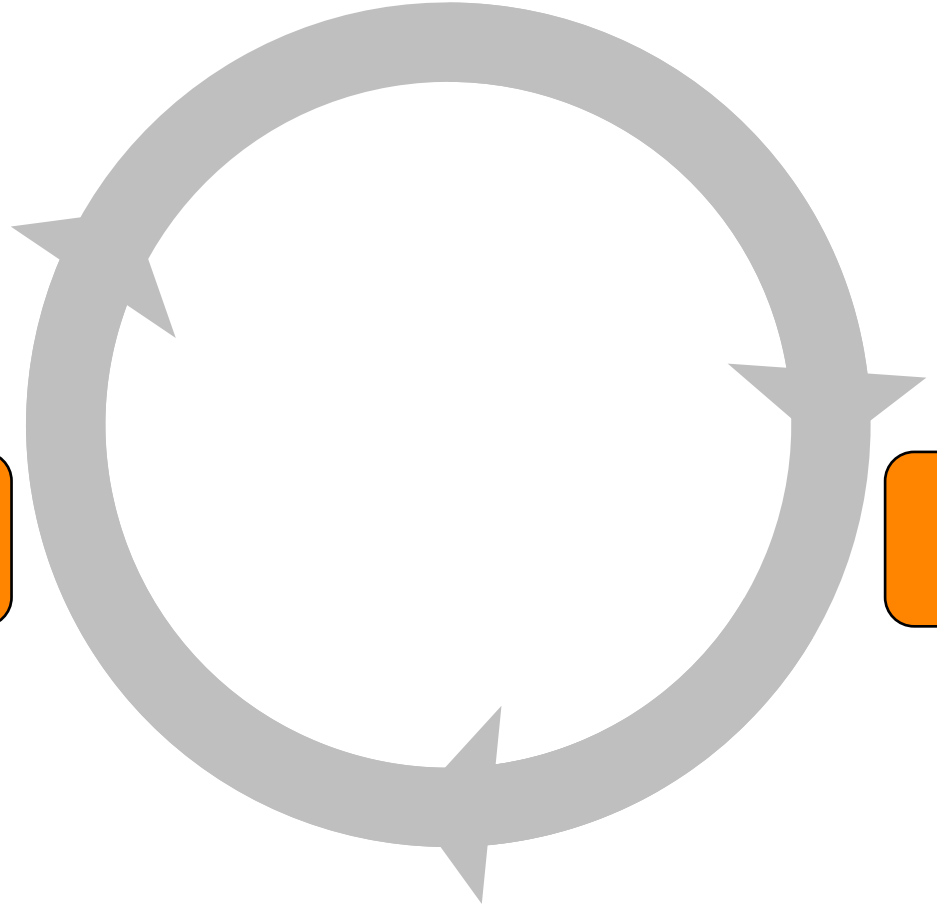
인시던트 해결과 완화에 소요되는 시간을 단축하고
관련된 프로세스를 관리 할 수 있는 기능

인시던트를 탐지 및 조사하고, 문제를 해결하고,
서비스를 복원하기 위해 취하는 단계를 문서화

인시던트 관리 프로세스

인시던트 탐지

- ✓ 담당자 연락 및 대응 상황 확인
- ✓ 에스컬레이션 흐름 정비



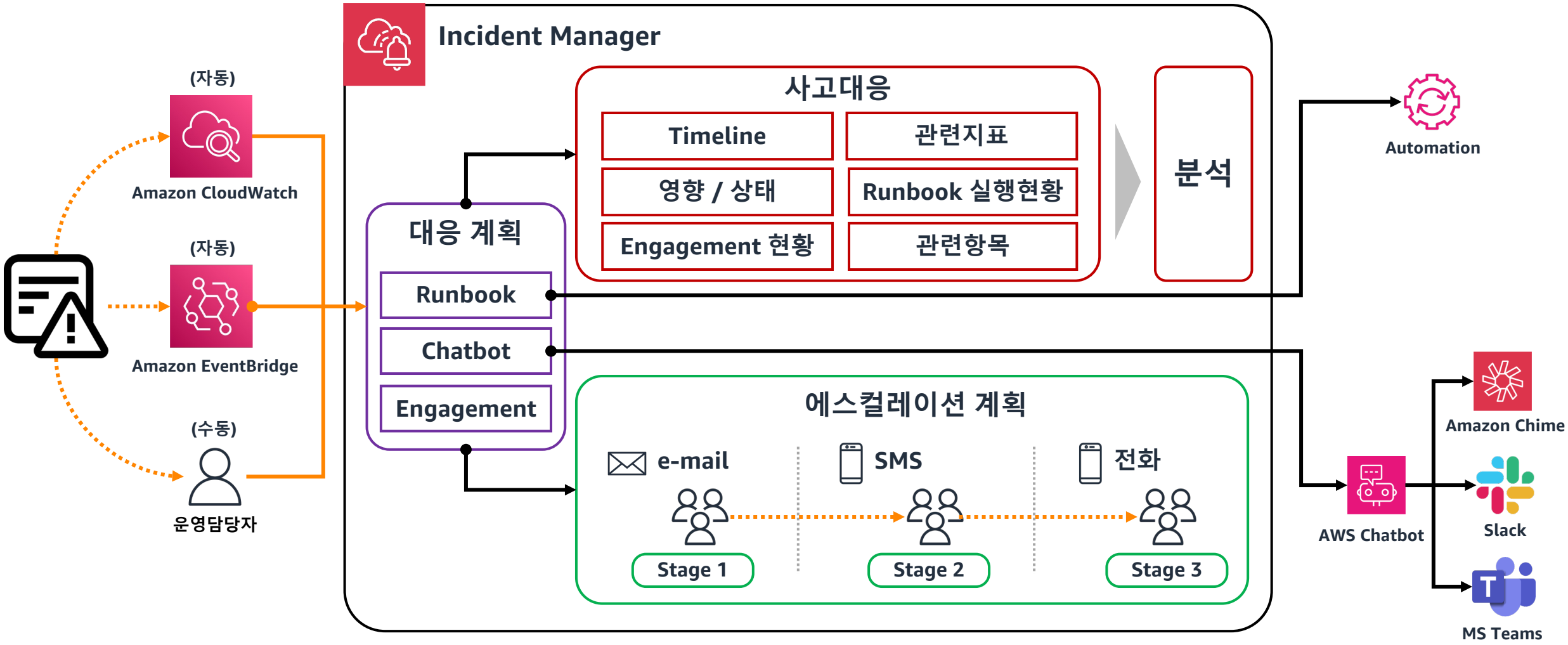
조사 및 대응

- ✓ 조사에 필요한 정보 수집
- ✓ 작업 효율화 및 자동화
- ✓ 유관자간 소통 강화

사후 분석

- ✓ 사고 대응 프로세스 개선
- ✓ 사고 원인에 대한 이해

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 스케쥴

- ✓ 인시던트 발생 시 연락처 로테이션 할 수 있는 스케쥴 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

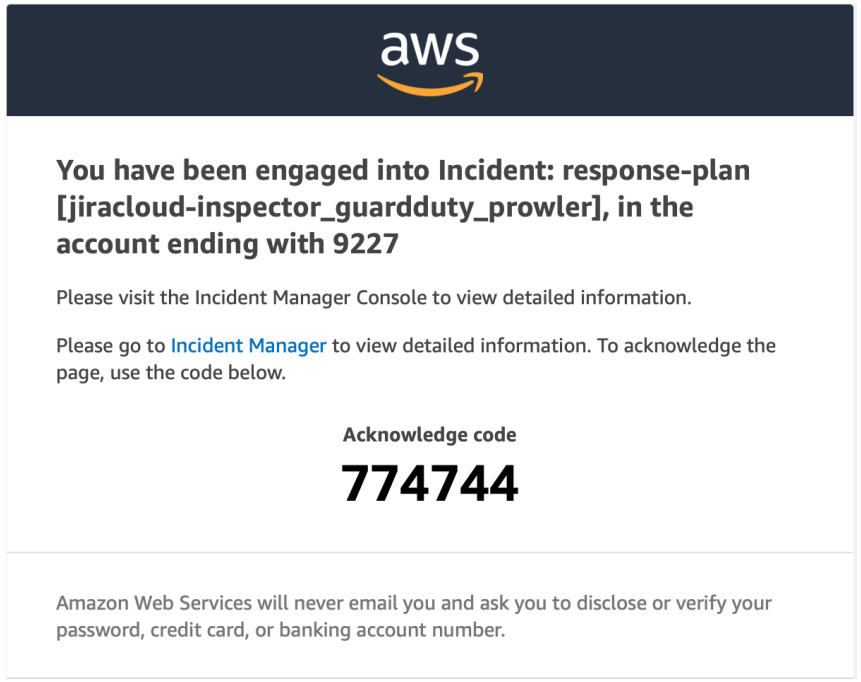
Runbook

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

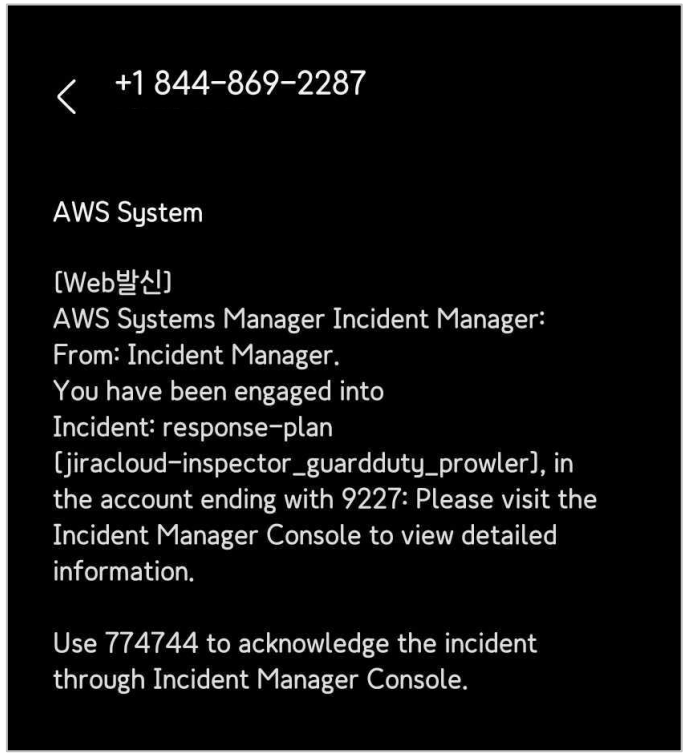
대응 계획

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

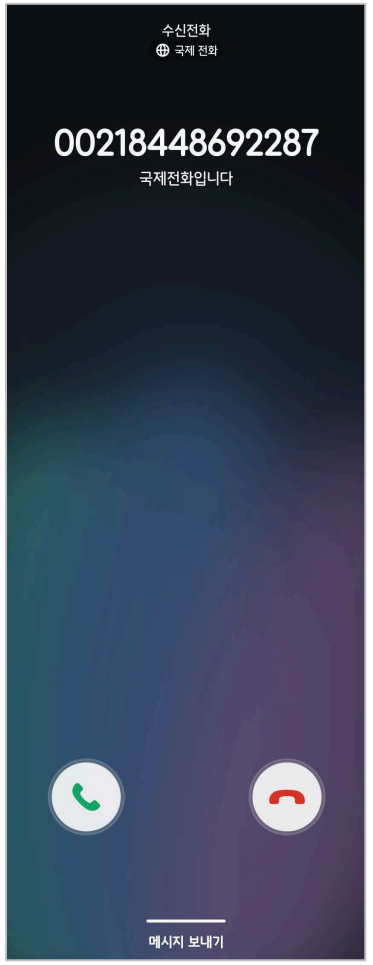
연락처 – 참여 계획



e-mail 알림



SMS 알림



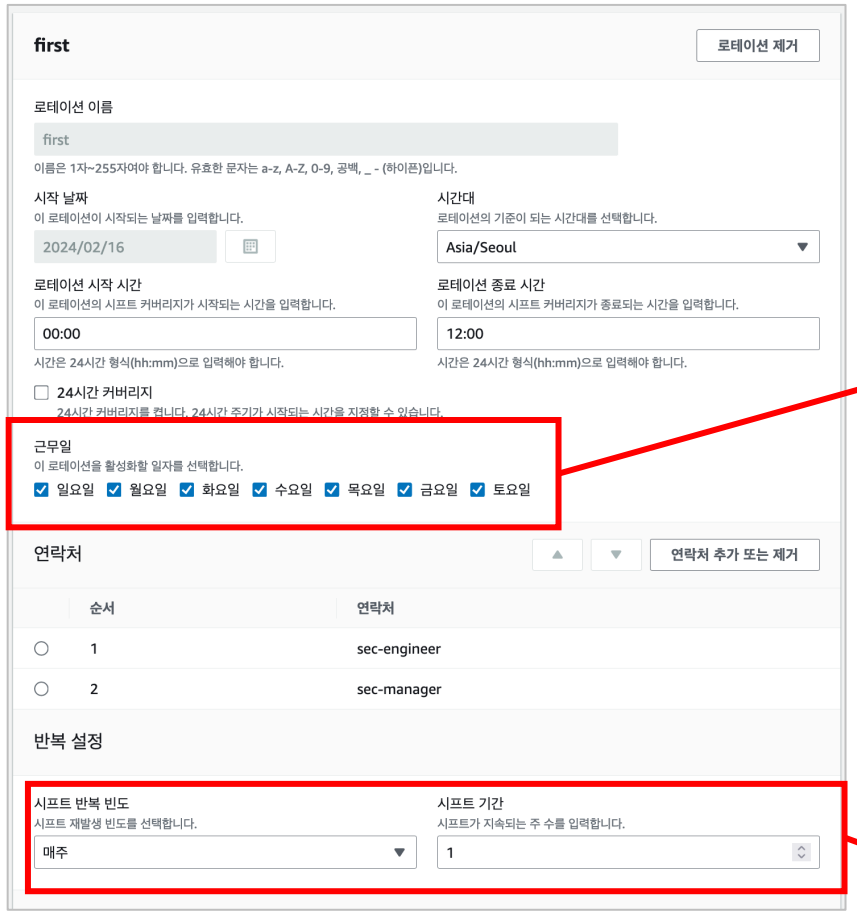
음성 알림

온콜 스케쥴

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

	3/11 ~ 3/15	3/18 ~ 3/22	3/25 ~ 3/29
제 1 연락처	 근무자 A	 근무자 B	 근무자 A
제 2 연락처	 근무자 B	 근무자 A	 근무자 B

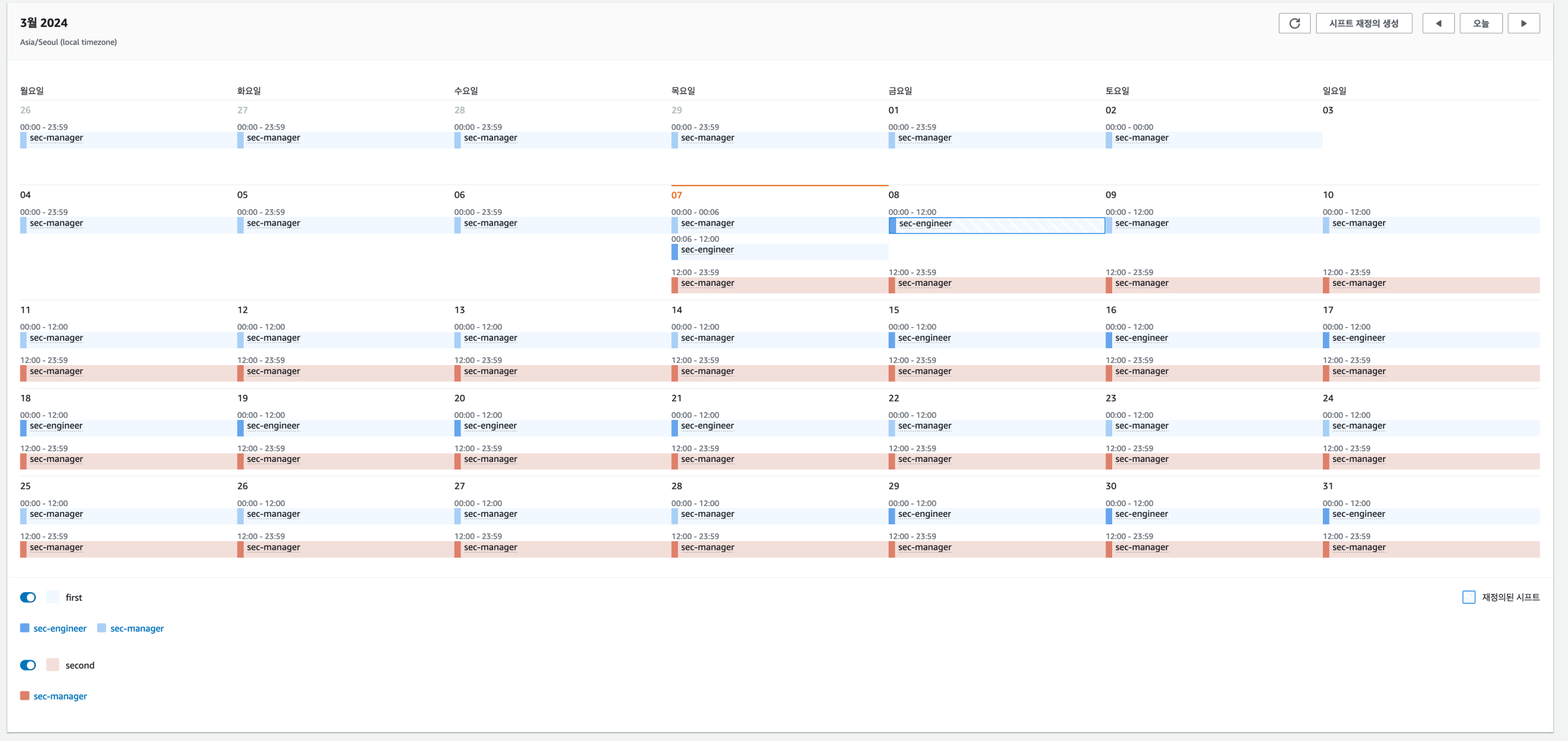
온콜 스케쥴 설정



활성화 요일 선택

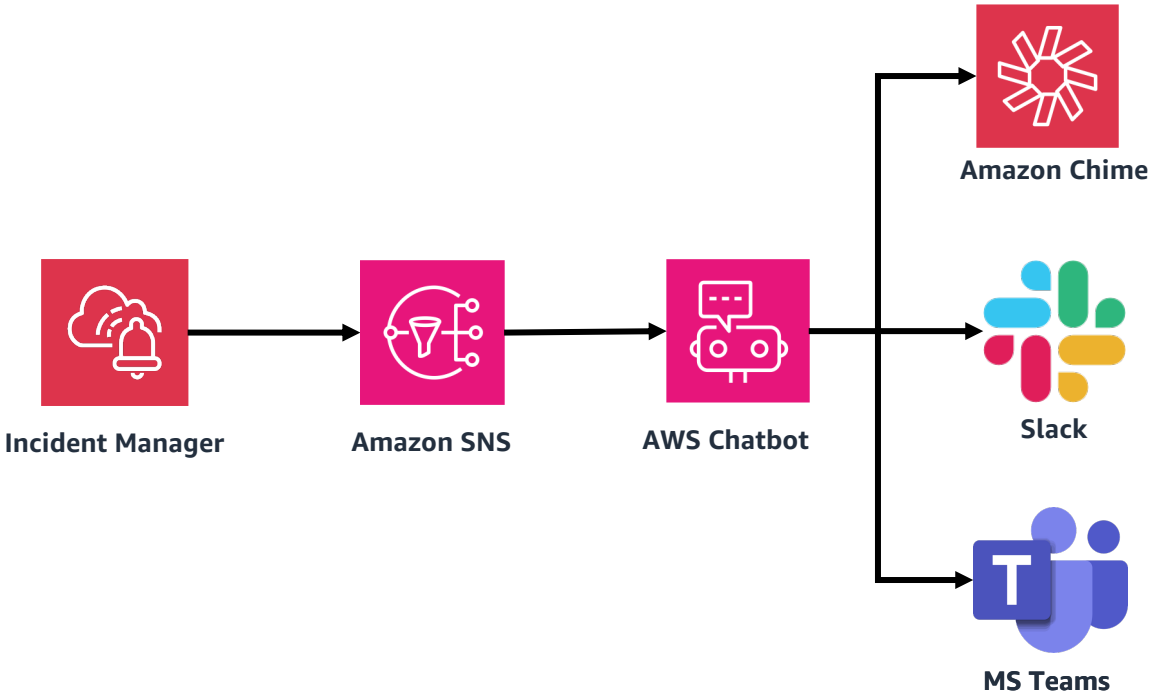
주 단위 순환

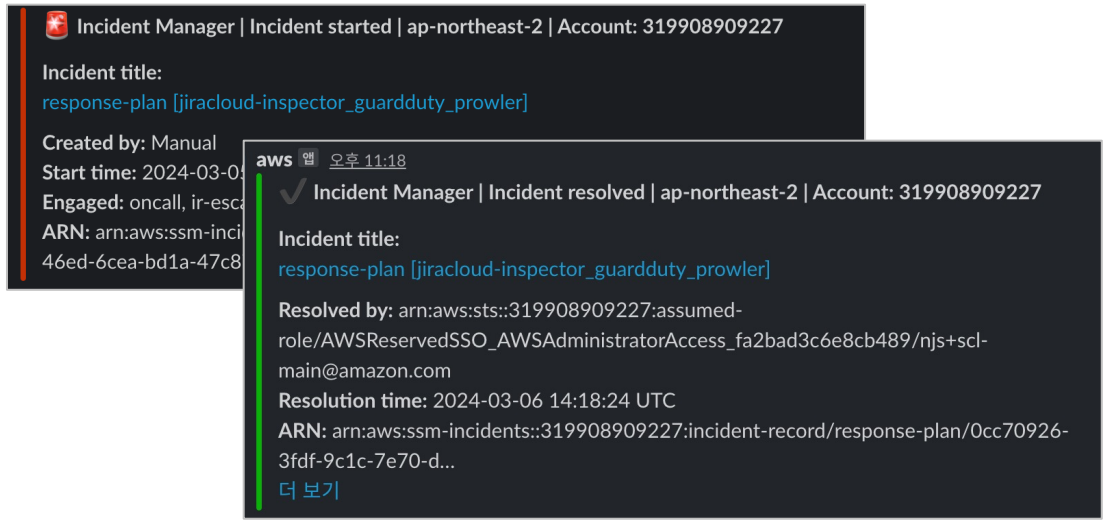
온콜 스케쥴 캘린더

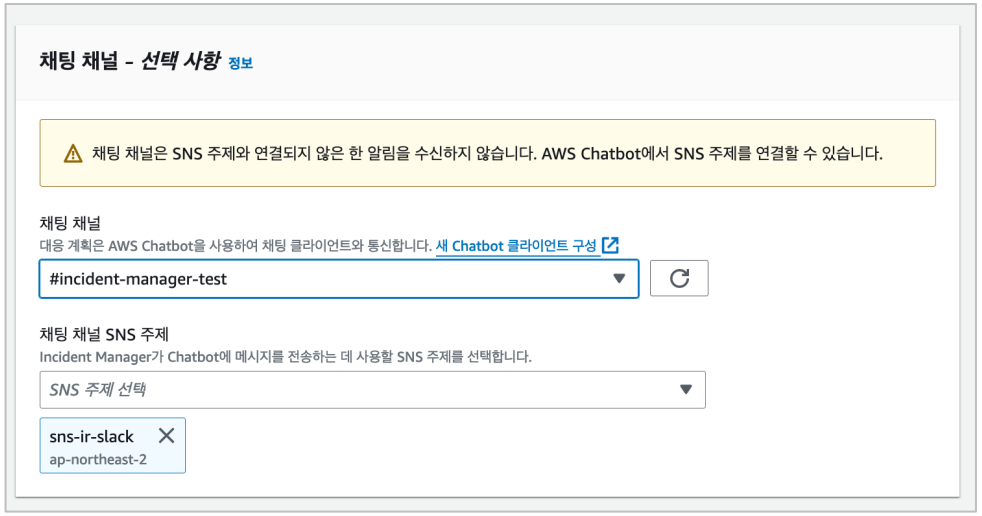


채팅 채널

✓ 인시던트 업데이트 및 알림을 채팅 채널로 푸시

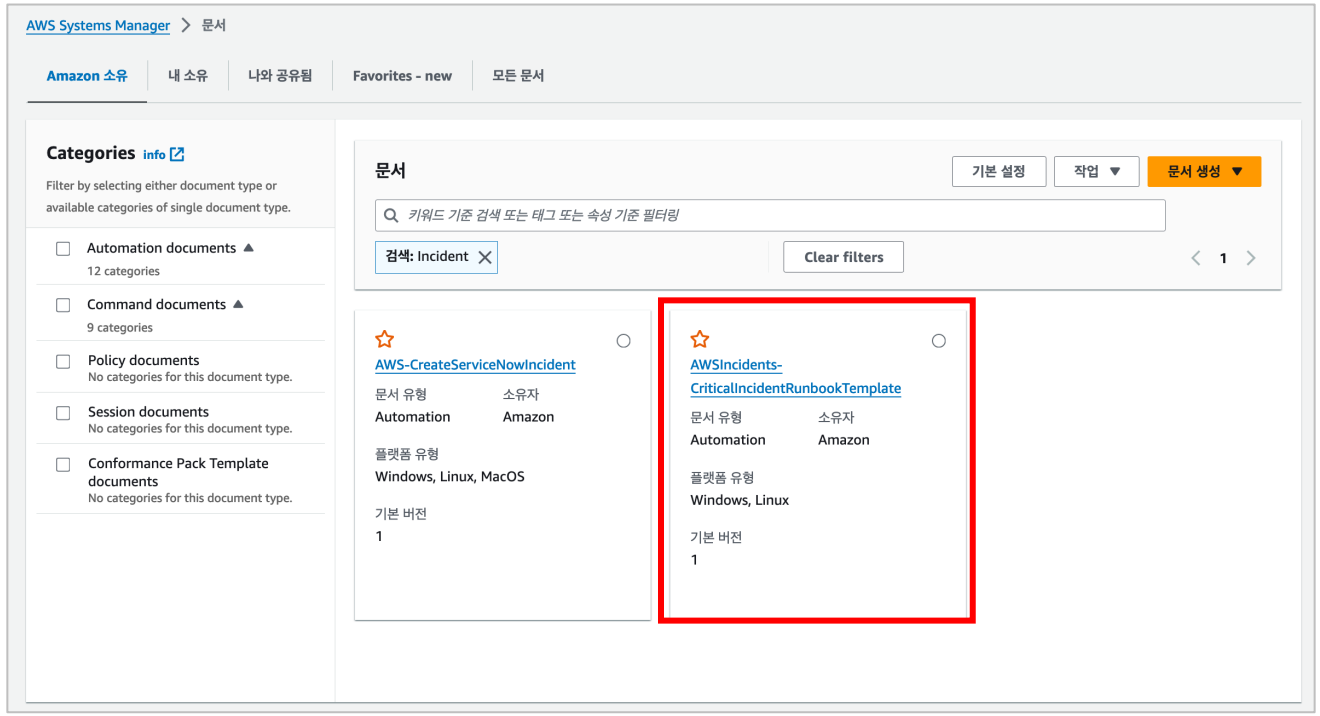






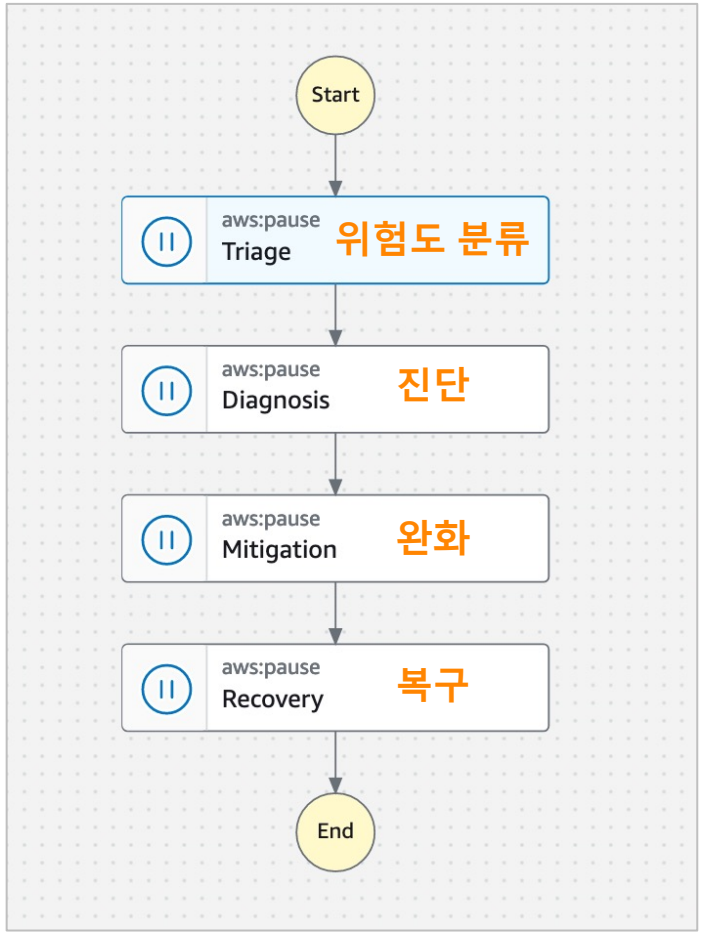
Runbook

- ✓ 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



단계 이름
Triage
작업
aws:pause

설명

Determine customer impact

- View the **Metrics** tab of t
find key performance ind
- Use CloudWatch Syntheti
customer workflows.

Communicate customer impac

Update the following fields to a

- **Title** - The title should be
particular incident.
- **Summary** - The summary
information to quickly on
- **Impact** - Select one of th
  - 1 – Critical impact,
  - 2 – High impact, pa
  - 3 – Medium impact
  customers.
  - 4 – Low impact, the
  - 5 – No impact, cust
  needed to avoid im

단계 이름
Diagnosis
작업
aws:pause

설명

Rollback

- Look for recent c
incident. Engage
- Rollback these cl

Locate failures

- Review metrics a
alarms to the Me
- Use CloudWatch
- Investigate the p
known incidents
links to the Relat
- Avoid going too
customer impact
is identified.

단계 이름
Mitigation
작업
aws:pause

설명

Collaborate

- Communicate
members of th
ways to mitiga
- Engage additio
tab.
- If necessary, pr

Implement mitigatio

- Consider re-rou
customer impa
- Look for comm
- Update the Tim
needed, review
proceeding.

단계 이름
Recovery
작업
aws:pause

설명

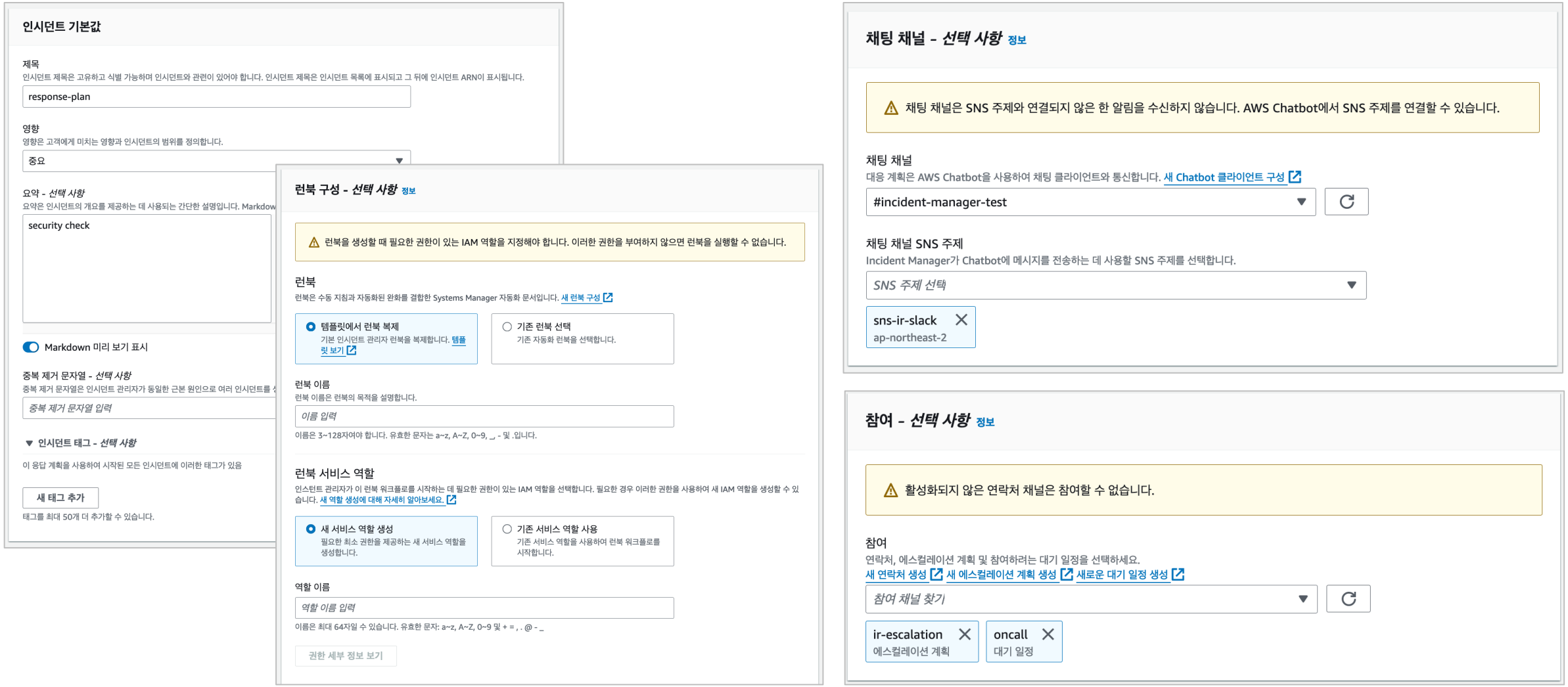
Monitor customer impact

- View the **Metrics** tab of the incident to monitor for recovery of your key performance indicators (KPIs).
- Update the **Impact** field in the incident when customer impact has been reduced or resolved.

Identify action items

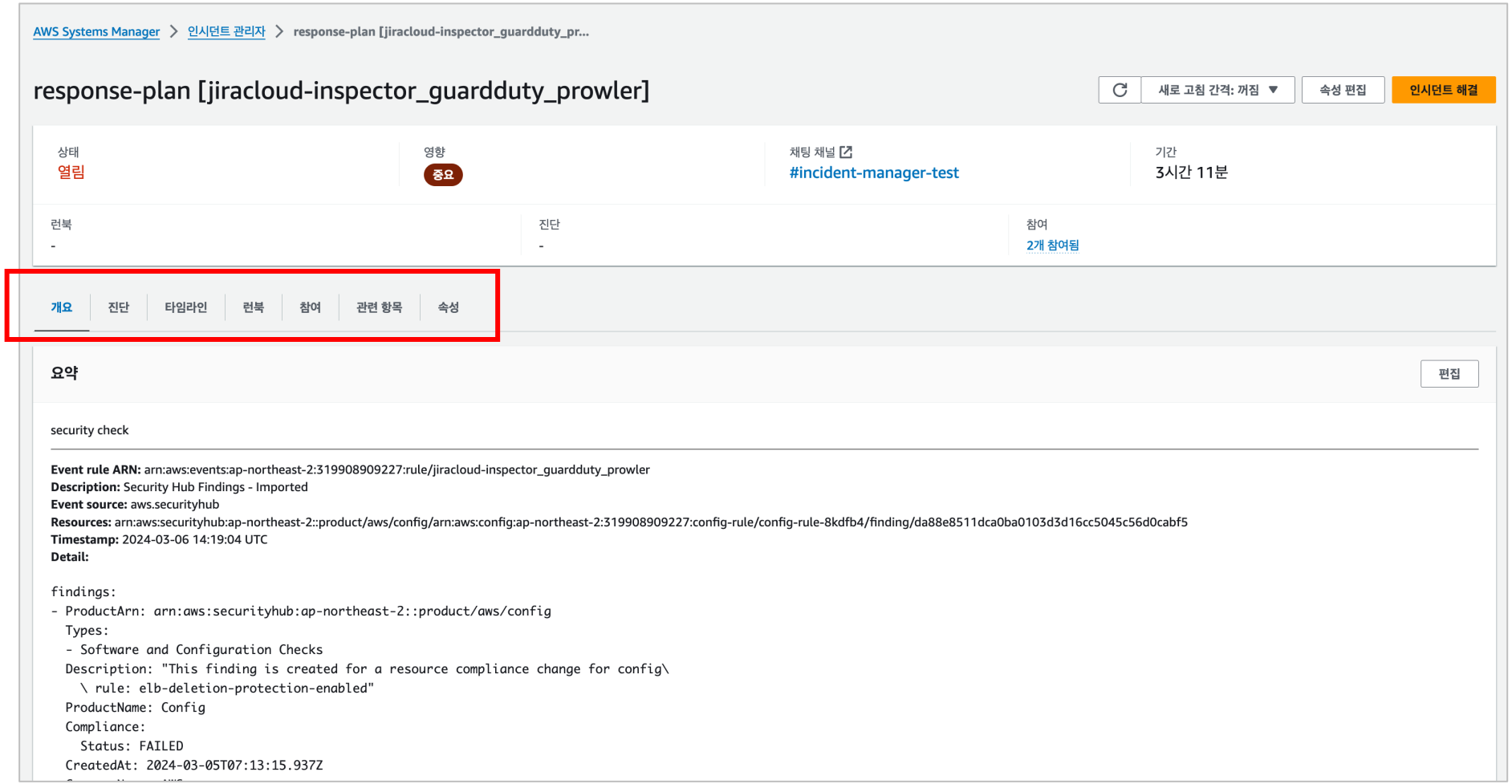
- Add entries in the **Timeline** tab of the incident to record key decisions and actions taken, including temporary mitigations that might have been implemented.
- Create a **Post-Incident Analysis** when the incident is closed in order to identify and track action items in OpsCenter.

대응 계획

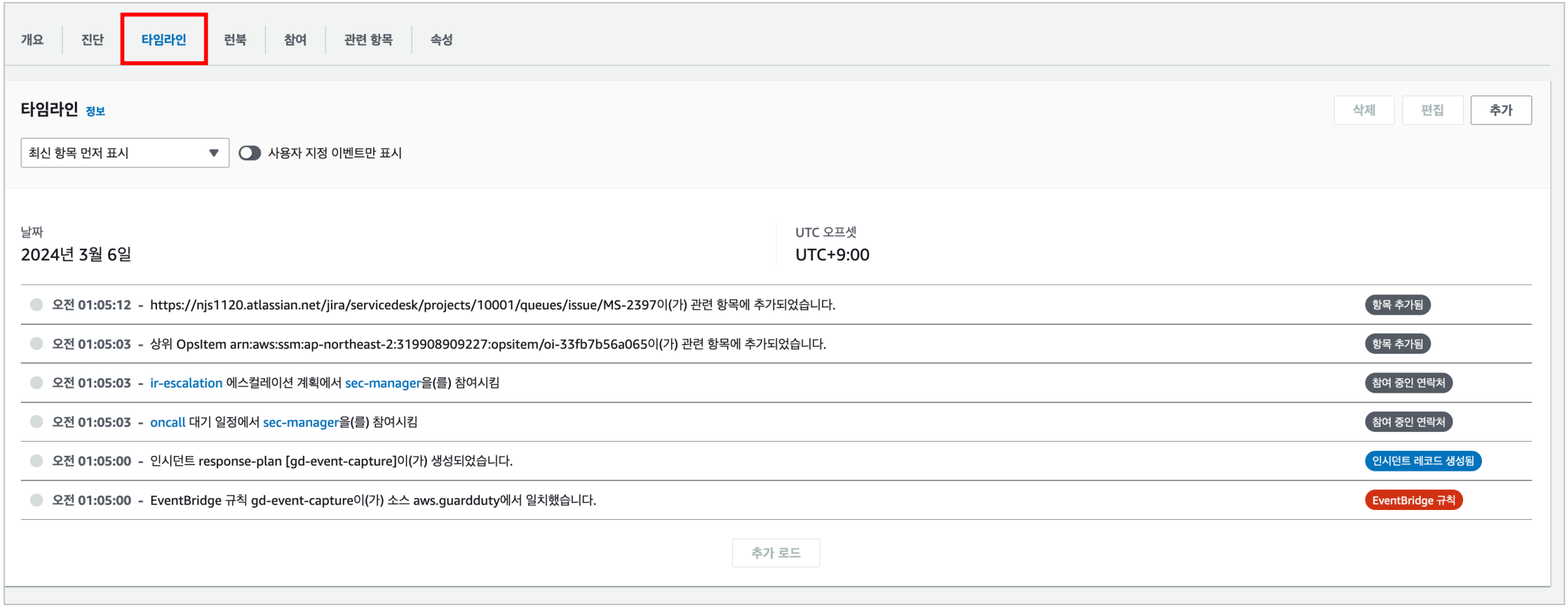


인시던트 확인

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

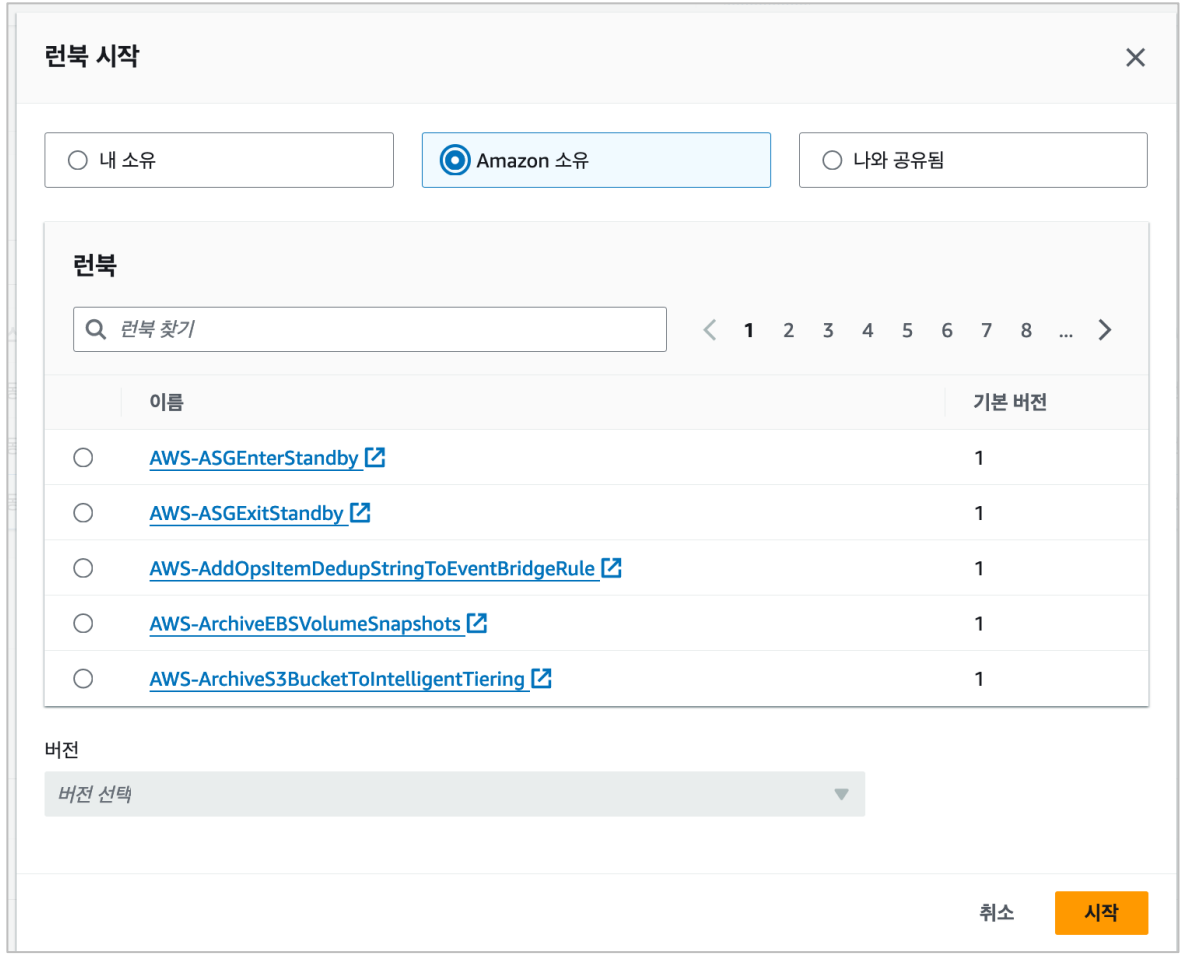


인시던트 확인 - 타임라인

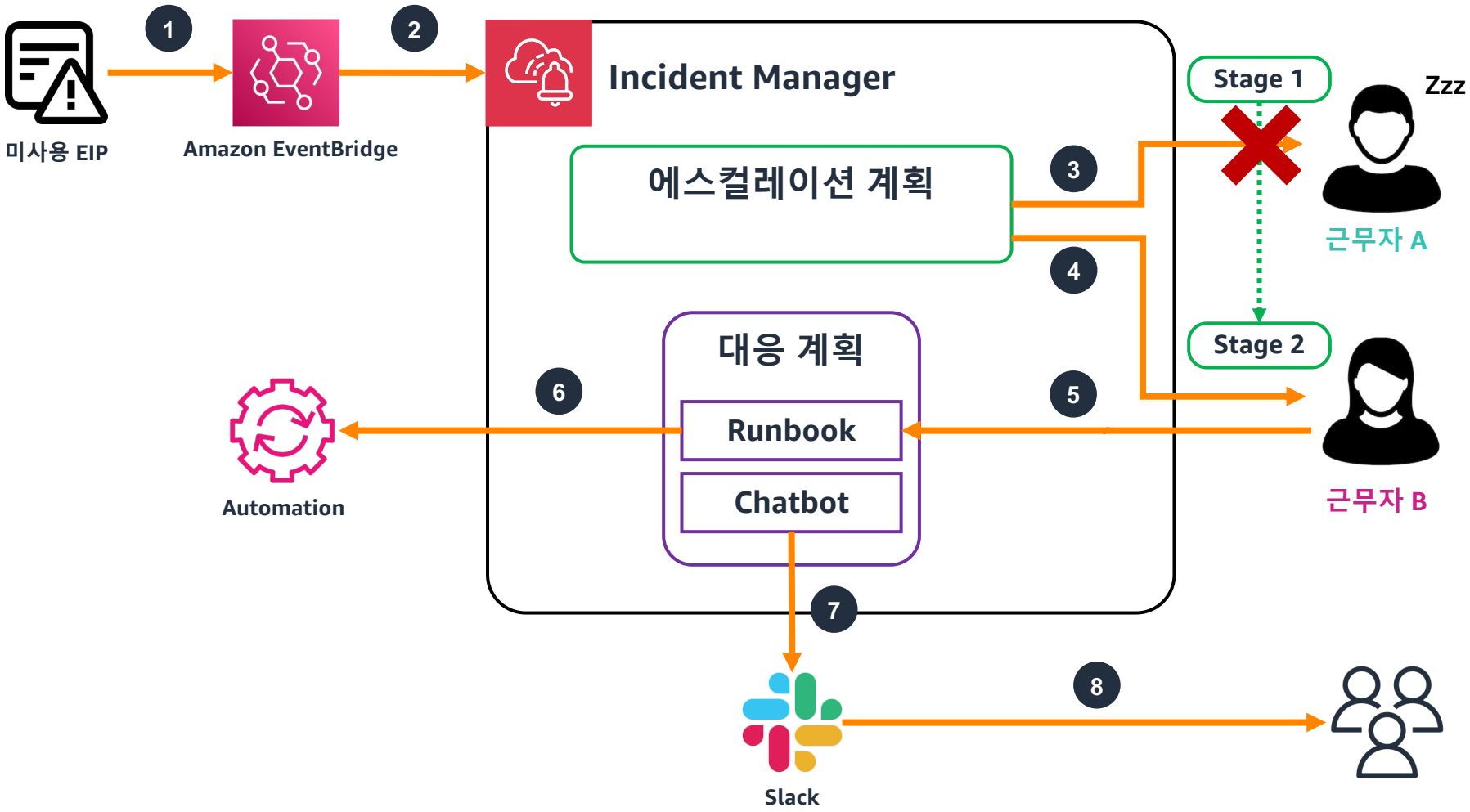


인시던트 대응 – Runbook 실행

✓ 인시던트 대응을 위한 Runbook을 Incident Manager 콘솔에서 실행 가능



Flow

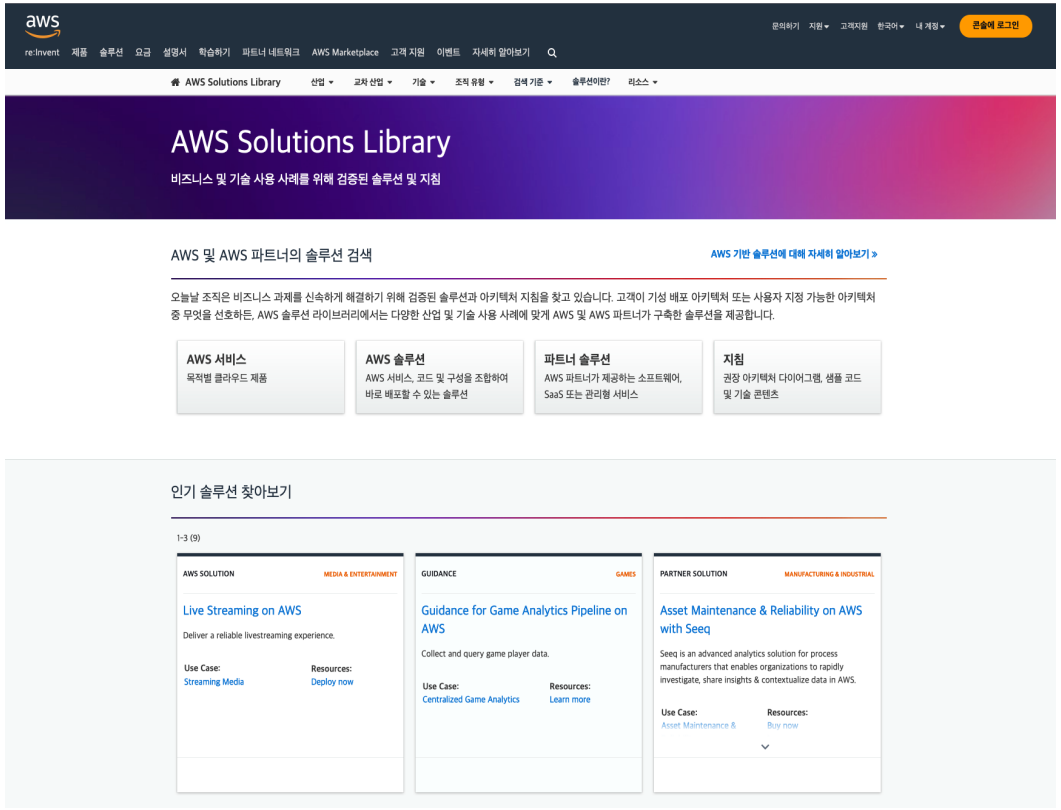


1. Config <-> Security Hub 연계를 통한 Findings 감지
2. EventBridge를 통해 Incident Manager로 인시던트 생성
3. 사전 정의된 에스컬레이션 계획에 따라 근무자 A에게 알림
4. 근무자 A 미응답, 근무자 B 알림
5. 근무자 B가 Runbook으로 대응 시작
6. Automation을 통한 자동 조치
7. 채팅 채널로 진행 상황 자동 전달
8. 업무 유관자들은 Slack에서 인시던트 상태 및 처리 현황 확인

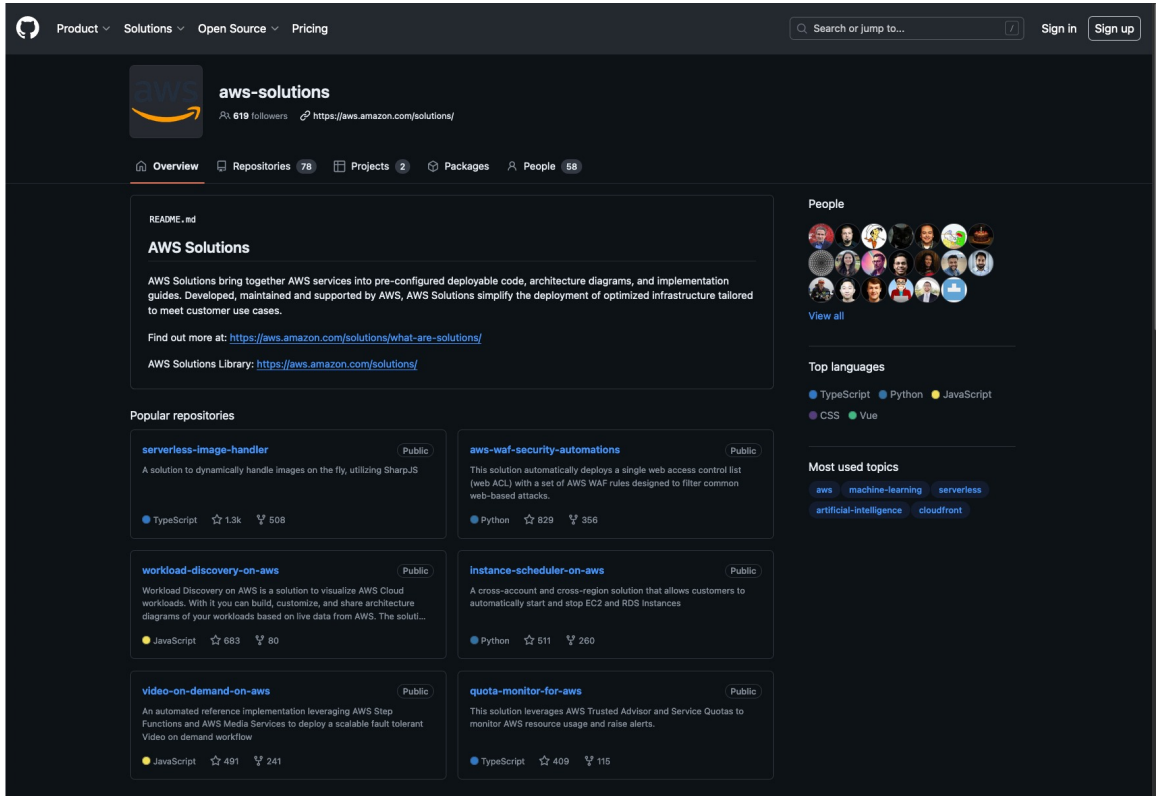
Automated Security Response (ASR) on AWS

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.

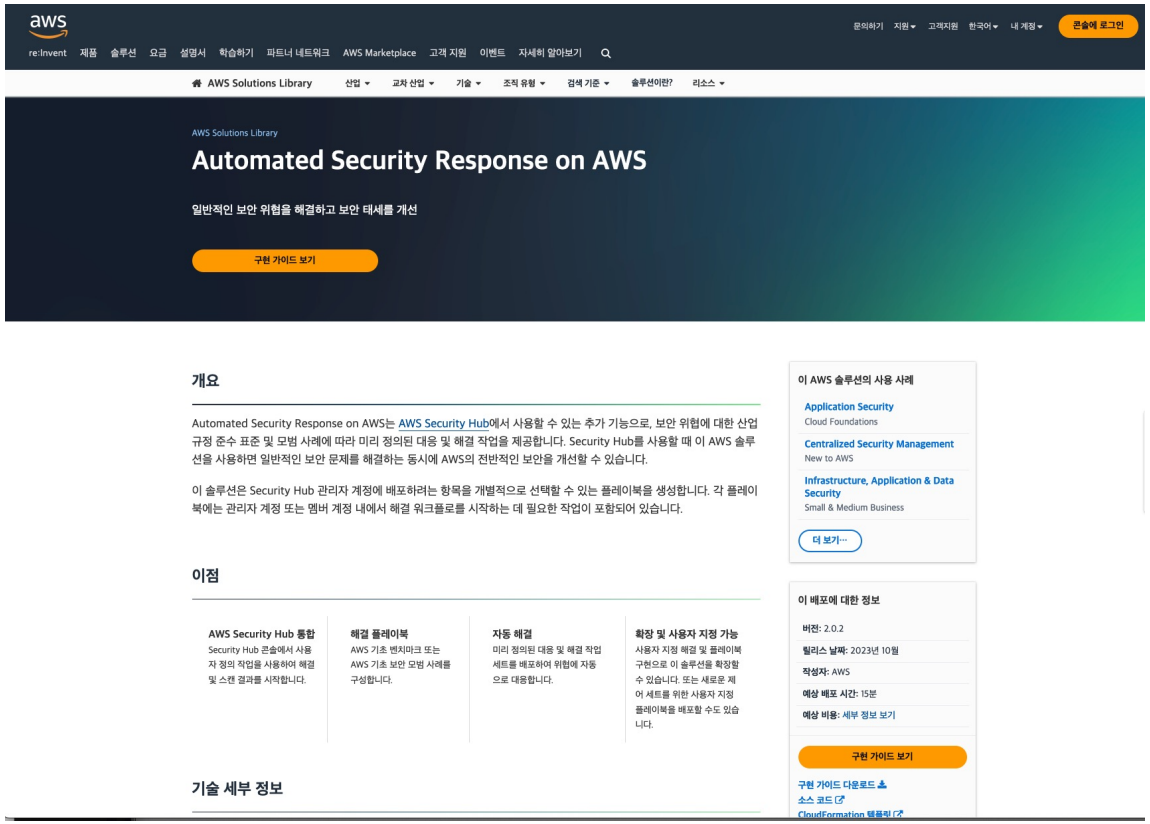


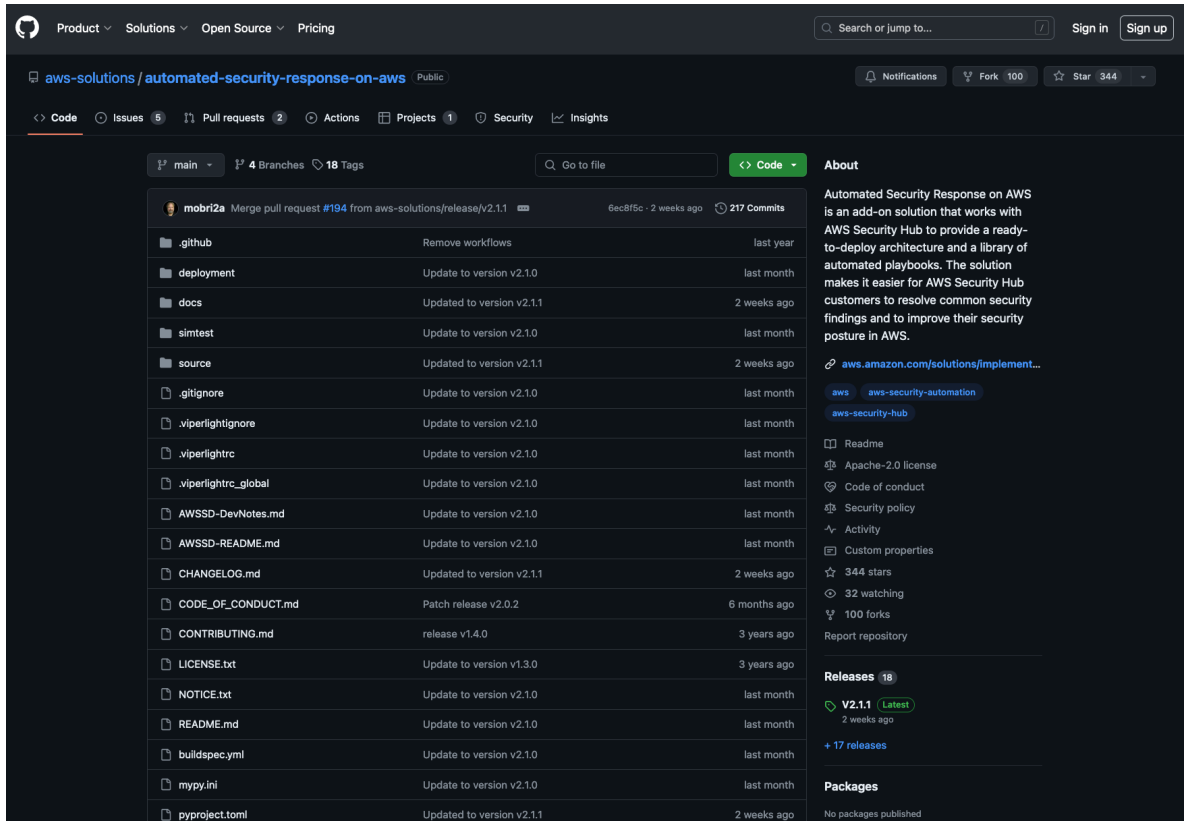
[AWS Solutions Library Page]



[aws-solutions(github)]

솔루션 - Automated Security Response on AWS





[AWS Solutions Library Page]

[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: - 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 배포필요 솔루션에서 구현되지 않은 새로운 컨트롤 세트를 지원 시사용자 지정 플레이북을 배포
표준화된 교정	일관된 구현 및 감사를 쉽게 하기 위해 AWS 조직 전체의 보안 취약성 해결을 표준화

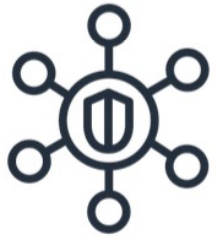
Solution Deploy

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 aws-sharr-member-roles.template	Systems Manager Document Systems Manager Automation Document 실행을 위한 IAM Role

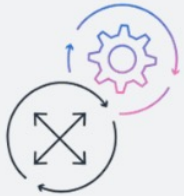
AWS 서비스	내용
Amazon EventBridge	핵심. 결과가 수정될 때 오케스트레이터 단계 기능을 시작하는 이벤트를 배포
AWS IAM	핵심. 다양한 리소스에 대한 수정을 허용하기 위해 많은 역할을 배포
AWS Lambda	핵심. 문제를 해결하기 위해 step function 오케스트레이터가 사용할 여러 람다 함수를 배포
AWS Security Hub	핵심. 고객에게 AWS 보안 상태에 대한 포괄적인 보기를 제공
AWS Step Functions	핵심. AWS 시스템 관리자 API 호출을 통해 문제 해결 문서를 호출하는 오케스트레이터를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

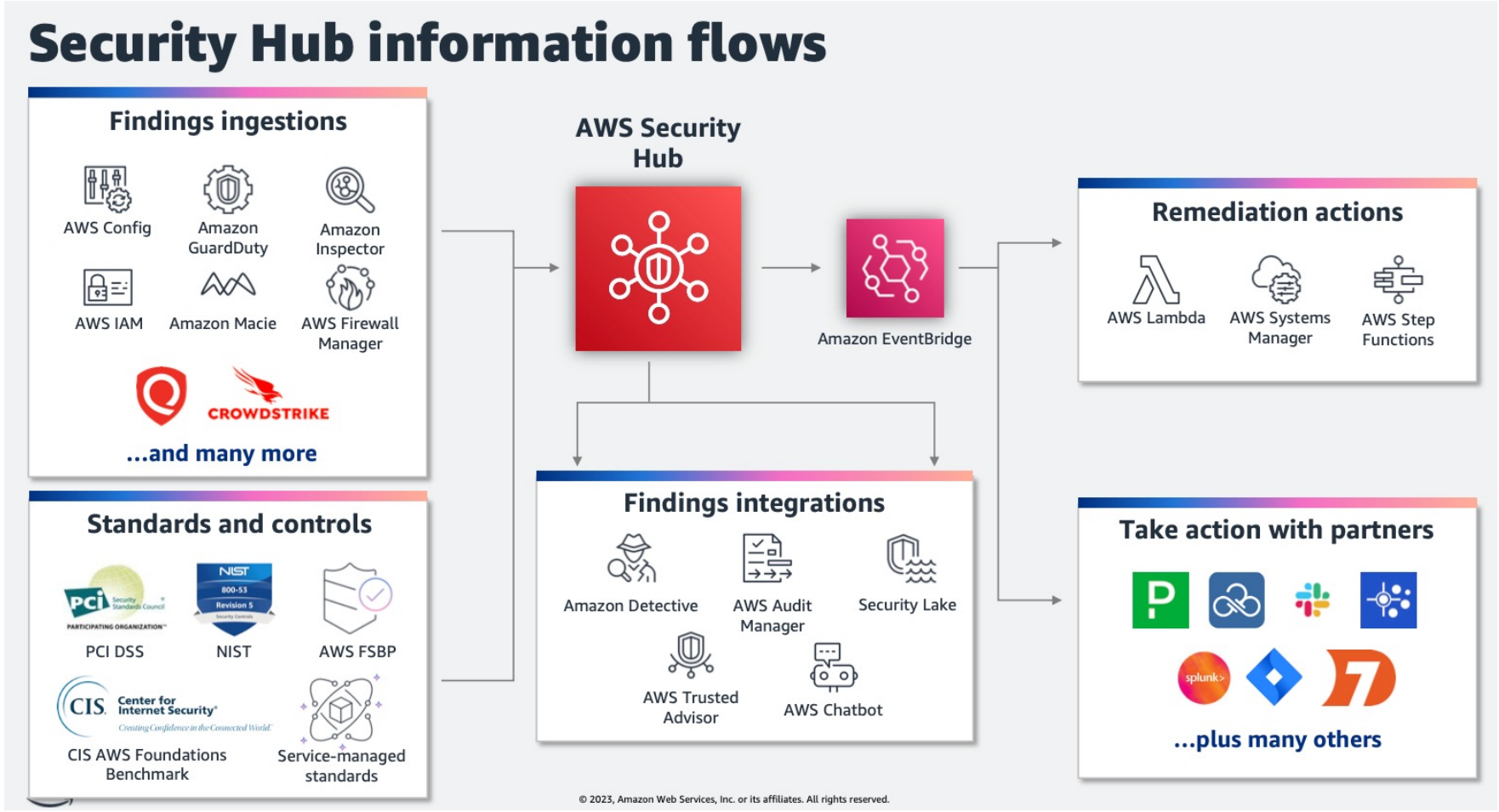
표준화된 결과 형식 및 교차 리전 간 집계

규제 및 특정 프레임워크에 부합하는 보안 표준 제공

자동화된 대응, 수정 및 강화 조치

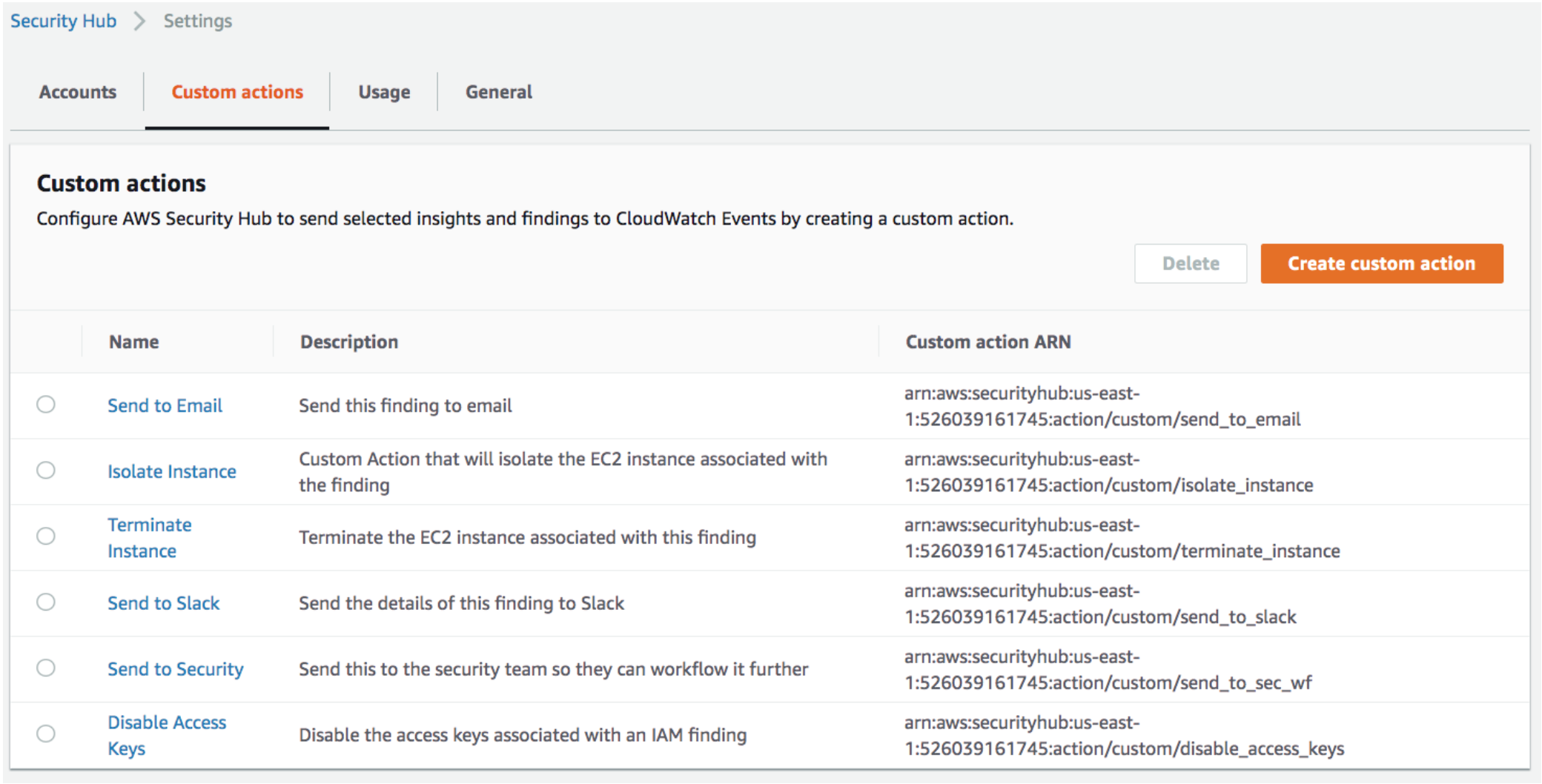
2023년 아홉번째 - 참가자 사례발표 - Security Hub 9월 21일
Security Hub 어디까지 써봤니?- 김대곤(AWS)

Security Hub

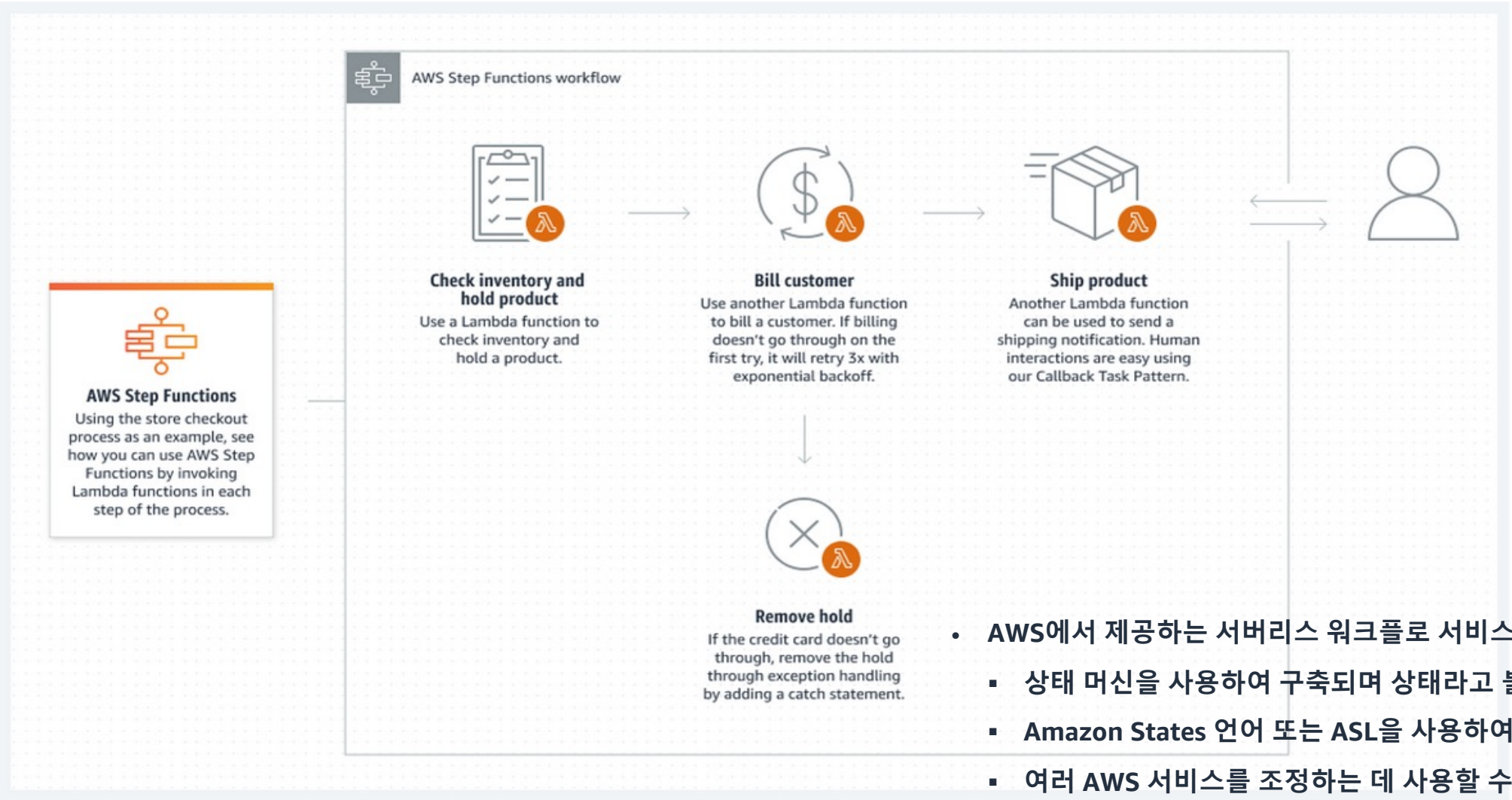


2023년 아홉번째 - 참가자 사례발표 - Security Hub 9월 21일
Security Hub 어디까지 써봤니?- 김대곤(AWS)

Security Hub



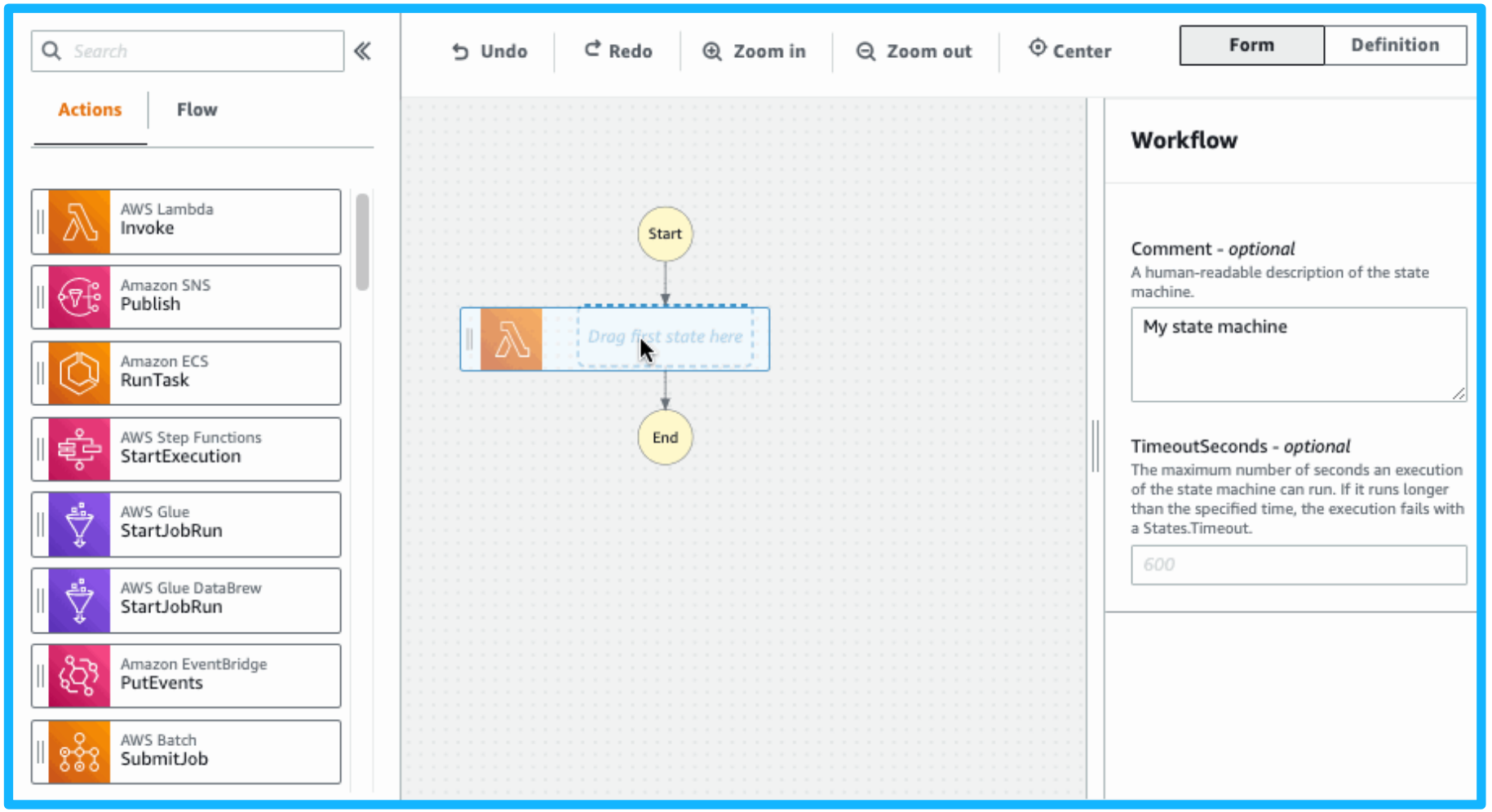
AWS Step Functions



- AWS에서 제공하는 서버리스 워크플로 서비스
  - 상태 머신을 사용하여 구축되며 상태라고 불리는 단계로 구성됩니다.
  - Amazon States 언어 또는 ASL을 사용하여 작성되었습니다.
  - 여러 AWS 서비스를 조정하는 데 사용할 수 있습니다.

AWS Step Functions

✓ **Workflow Studio: Low-code visual designer**



Workflow Studio는 드래그 앤 드롭 방식의 시각적 빌더입니다.

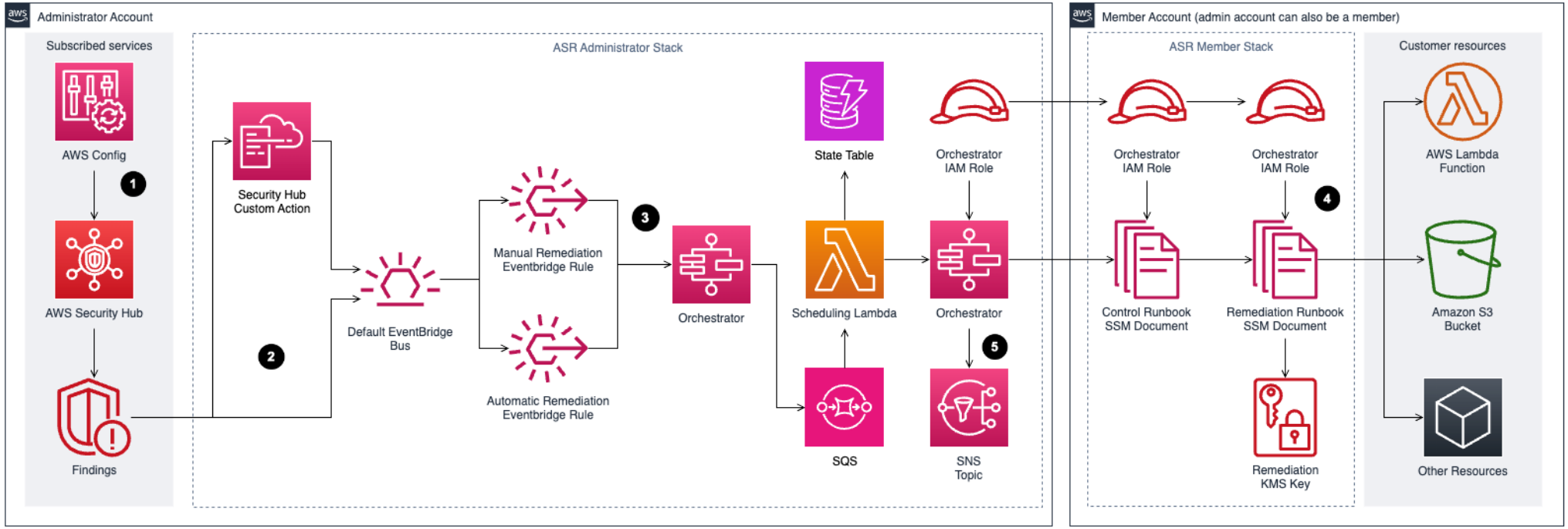
새로운 개발자를 위한 첫 번째 워크플로를 구축하는 시간이 단축됩니다.

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

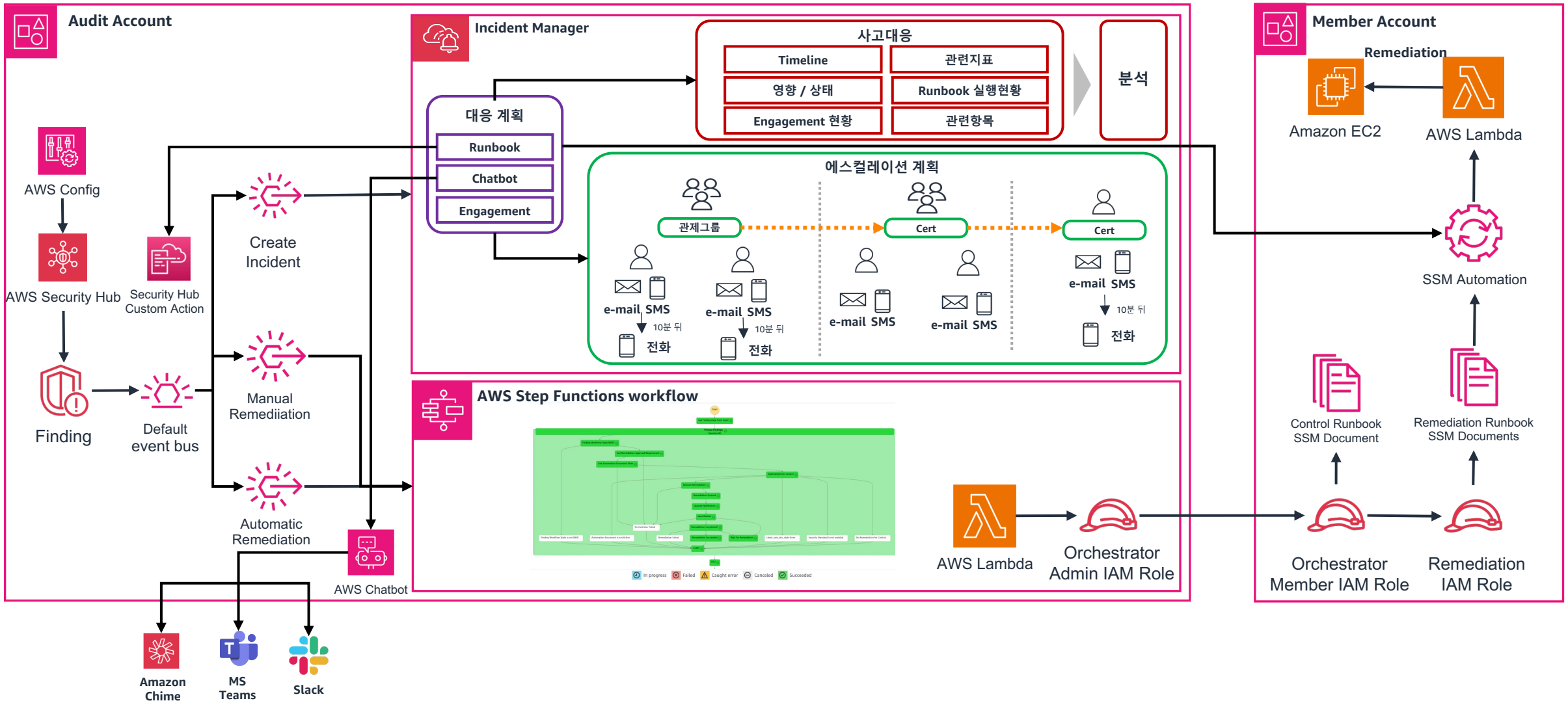
✓ **AWS Security Hub와 함께 작동하고 보안 위협에 대한 업계 규정 준수 표준 및 모범 사례를 기반으로 사전 정의된 대응 및 해결 조치를 제공하는 추가 기능입니다.**



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 분분 별로 분리도 가능
  - 이메일, 문자, 전화가 정말 잘옵니다 (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
  - 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
- 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

Thank you!