

AWS 기반 실시간 보안 이벤트 자동대응

Team - Layer3
석대원 신유주 안지서 윤서원

CONTENTS

1. INTRODUCE

2. 프로젝트 개요 및 목표

3. 프로젝트 아키텍쳐

4. 보안요구사항 정의

5. 위험도 정의

6. 핵심 기능

7. 보안이벤트 설계

8. 자동 대응 시나리오

9. 알림 시스템

10. 시연 영상

11. 테스트 결과

12. 프로젝트 성과 및 개선사항

INTRODUCE



- 전체 SOAR 아키텍처 설계 및 리소스 파이프라인 통합
- IAM 보안 정책 수립 및 리소스 접근 제어(Least Privilege) 구현



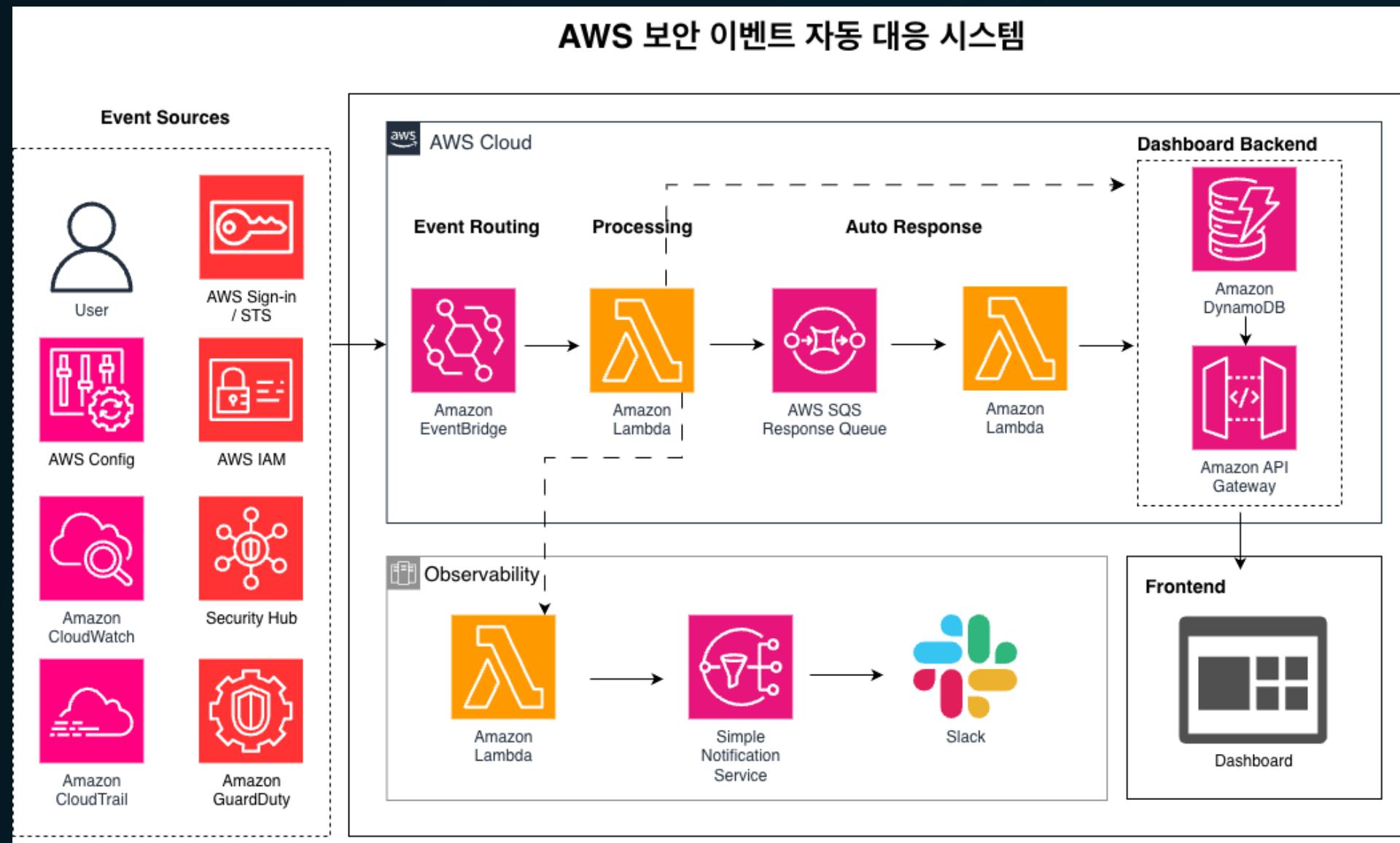
- 스토리지(S3) 보안 모니터링 (Public ACL/Policy 변경 실시간 탐지)
통합 알림 파이프라인 구축 (CloudWatch → SNS → Lambda → Slack)



- 계정 보안(Root/User Login) 및 인프라 변조 시나리오 설계
AWS EventBridge 기반 탐지 룰 엔진 구축 (Account, AccessKey, SG, CloudTrail 변조 등)



프로젝트 아키텍쳐



Event Sources

CloudTrail, Config, IAM, GuardDuty, Security Hub에서 AWS 서비스 이벤트 발생

Routing

EventBridge가 사전에 정의된 Rule(패턴)에 따라 이벤트를 필터링하여 전달

Processing

lambda에서 이벤트 분석

Notification

SNS 및 API Gateway/WebSocket를 통해 대시보드로 경보 전송 & Slack 알림 발송

Remediation

SQS 트리거를 받은 Lambda가 Boto3를 이용해 격리/차단 조치 수행

Storage

모든 탐지 및 대응 이력은 DynamoDB에 저장 및 관리

보안요구사항 정의

Asset : 보호 대상으로 시스템·데이터·계정 등 핵심 요소

Threat : 자산을 공격하거나 손상시킬 수 있는 시나리오, 외부·내부 공격 및 비정상 행위

Vulnerability : 자산이 위협에 노출될 수 있는 설계적·운영적 약점

Control : 취약점을 완화하거나 해결하기 위해 필요한 기술적·관리적·운영적 조치

Compliance : 준수해야 하는 규제와 외부 기준을 중심으로, 법규 및 프레임워크 요구사항

보호해야 할 주요 자산 (Asset)	예상되는 위협 (Threat)	존재할 수 있는 취약점 (Vulnerability)	요구되는 보안 통제 (Control)	준수한 컴플라이언스 기준 (Compliance)
CloudTrail 로그	계정 탈취 (Impossible Travel)	IAM 권한 과도 부여 가능성	IAM 최소 권한 원칙 적용	ISO 27001 A.9 접근통제
AWS 계정 접근 권한(IAM)	대량 스캐닝 (Mass Scanning)	Lambda Timeout 시 대응 누락	데이터 암호화 (KMS,HTTPS/WSS)	ISO 27001 A.12 로깅 & 모니터링
Lambda 탐지/대응 로직	보안그룹 반복 오픈	CloudTrail 이벤트 지연	CloudTrail 무결성 검증	ISO 27001 A.13 네트워크 보안
Incident DB (DynamoDB)	로그 삭제 시도	WebSocket 인증/세션 미흡	WebSocket 인증+Heartbeat	NIST CSF - Detect (DE)
WebSocket 실시간 스트림	WebSocket 세션 탈취 API 오남용	이벤트 중복 처리 부족 DB 무결성 위협	Lambda 재시도 + Fail-safe 처리	NIST CSF - Respond (RS) / NIST 800-53 SI-4

위험도 정의

CRITICAL

<즉각 대응 필요>

- 즉각적인 계정 탈취
- 데이터 노출
- 서비스 파괴로 이어지는 행위
- Root 비정상 로그인
- CloudTrail StopLogging
- S3 Public Exposure
- 보안 그룹 전체 오픈(SSH/RDP)

HIGH

<자동 대응 권장>

- 공격 징후 식별
- 심각한 설정 오류
- 비정상 국가 로그인
- AccessKey 오용
- DoS 스캐닝 탐지

MEDIUM

<알림 중심>

- 위험 가능성 존재
- 즉각적인 영향 적음
- 과도한 IAM 권한
- SG 이상 식별

LOW

<기록 위주>

- 위험도 낮음
- 즉각적인 영향 거의 없음
- 일반 사용자 로그인
- 리소스 생성 이벤트

핵심 기능

Task #1

위험도 기반 실시간 탐지

- Critical / High / Medium / Low로 분류
- CloudTrail & GuardDuty 기반 이벤트 패턴 매칭

Task #2

34개 탐지 시나리오 적용

- 자동 대응 (Auto Remediation)
- Critical 위협 즉시 자동 차단
- Root 로그인 / CloudTrail 무력화 / S3 Public / SSH 전체 오픈
- High → 조건부 대응 + 알림
- Medium / Low → 기록 중심

Task #3

실시간 모니터링 대시보드

- WebSocket 즉시 알림
- 위험도 색상 표시
- NEW → PROCESSING → MITIGATED 상태 흐름 표시

보안 이벤트 설계

영역	총 시나리오 (개수)	CRITICAL	HIGH	MEDIRM	LOW
IAM	9	Root 비정상 접근 MFA 제거	Impossible Travel	과도 권한	일반 로그인
NETWORK	10	SSH/RDP 전체 오픈	스캐닝 탐지	포트 이상	SG 일반 변경
S3	7	Public ACL/정책	권한 이상 부여	객체 권한 오류	이벤트 기록
LOGGING	6	Stop Logging	Trail 변조	설정 변경	일반 로그

자동대응 시나리오

IAM 로그인 3회 실패 → 자동 권한 제거

조건

동일 사용자 10분 내 로그인 실패 3회

탈지

CloudTrail ConsoleLogin

대응

IAM Policy Detach 수행

알림

WebSocket → Dashboard 실시간 반영

비정상 지역(국가 이동) 로그인

조건

A국 → 10분 내 B국 로그인

탈지

CloudTrail SignIn + 지리정보 비교

대응

계정 보호(정책 분리 or Alert Only)

알림

WebSocket → Dashboard 실시간 반영

자동대응 시나리오

Security Group 고위험포트 0.0.0.0/0 허용

조건

인바운드 SSH 전 구간 오픈

탐지

SG AuthorizeSecurityGroupIngress 이벤트

대응

해당 규칙 자동 삭제

알림

WebSocket → Dashboard 실시간 반영

S3 Public 정책 생성 → 자동 비활성화

조건

PublicAccessBlock 비활성화, public 정책 적용

탐지

EventBridge S3 Policy Change

대응

Lambda 정책 삭제

알림

WebSocket → Dashboard 실시간 반영

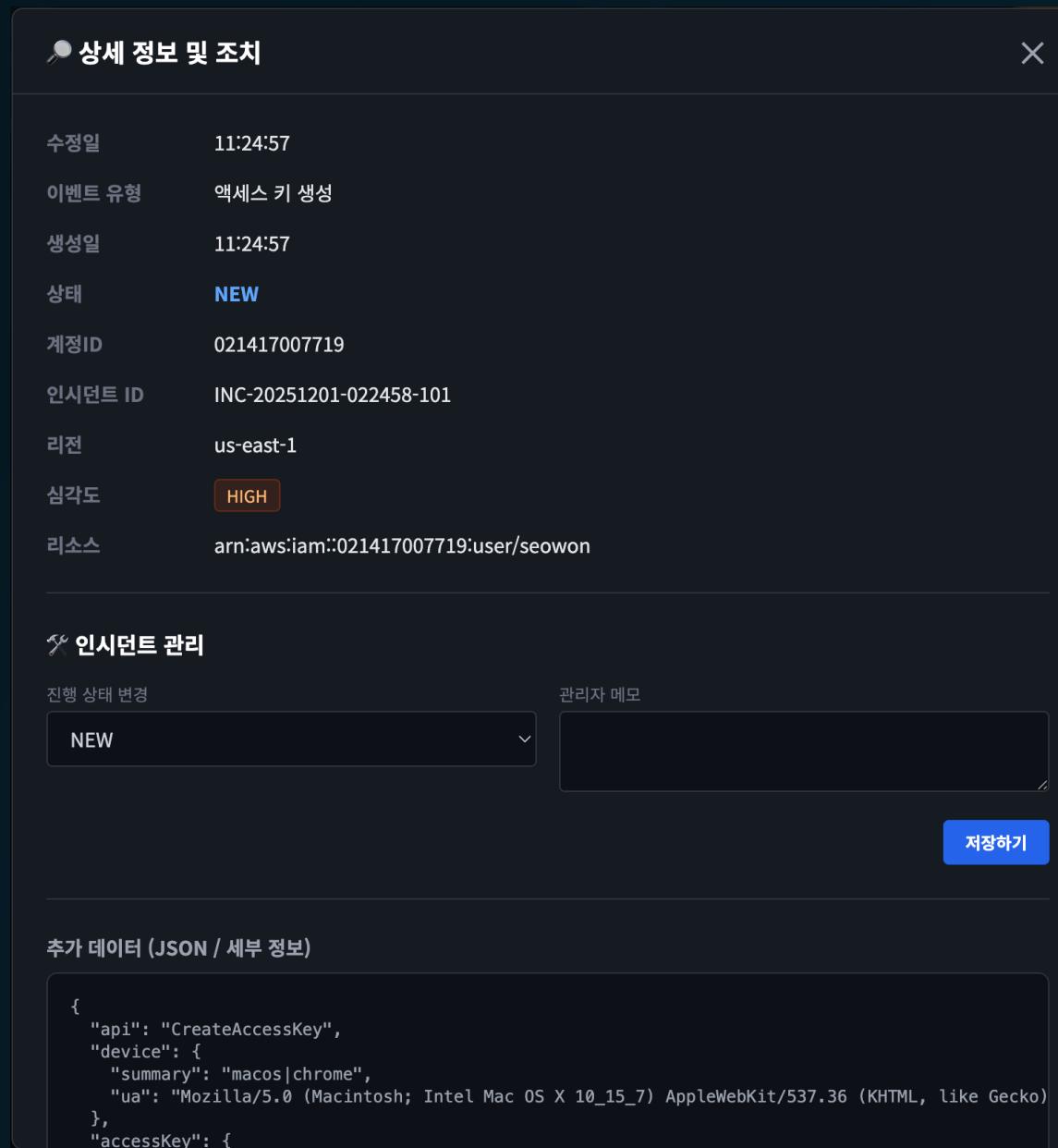
알림시스템



- 대응 상태를 지표와 그래프로 시각화
- 발생한 보안 이벤트, 자동대응 로그를 시간 순으로 표시
- 따로 DB에 저장하여 실시간 로그와 지난 로그 확인 용이 및 별도 관리 가능

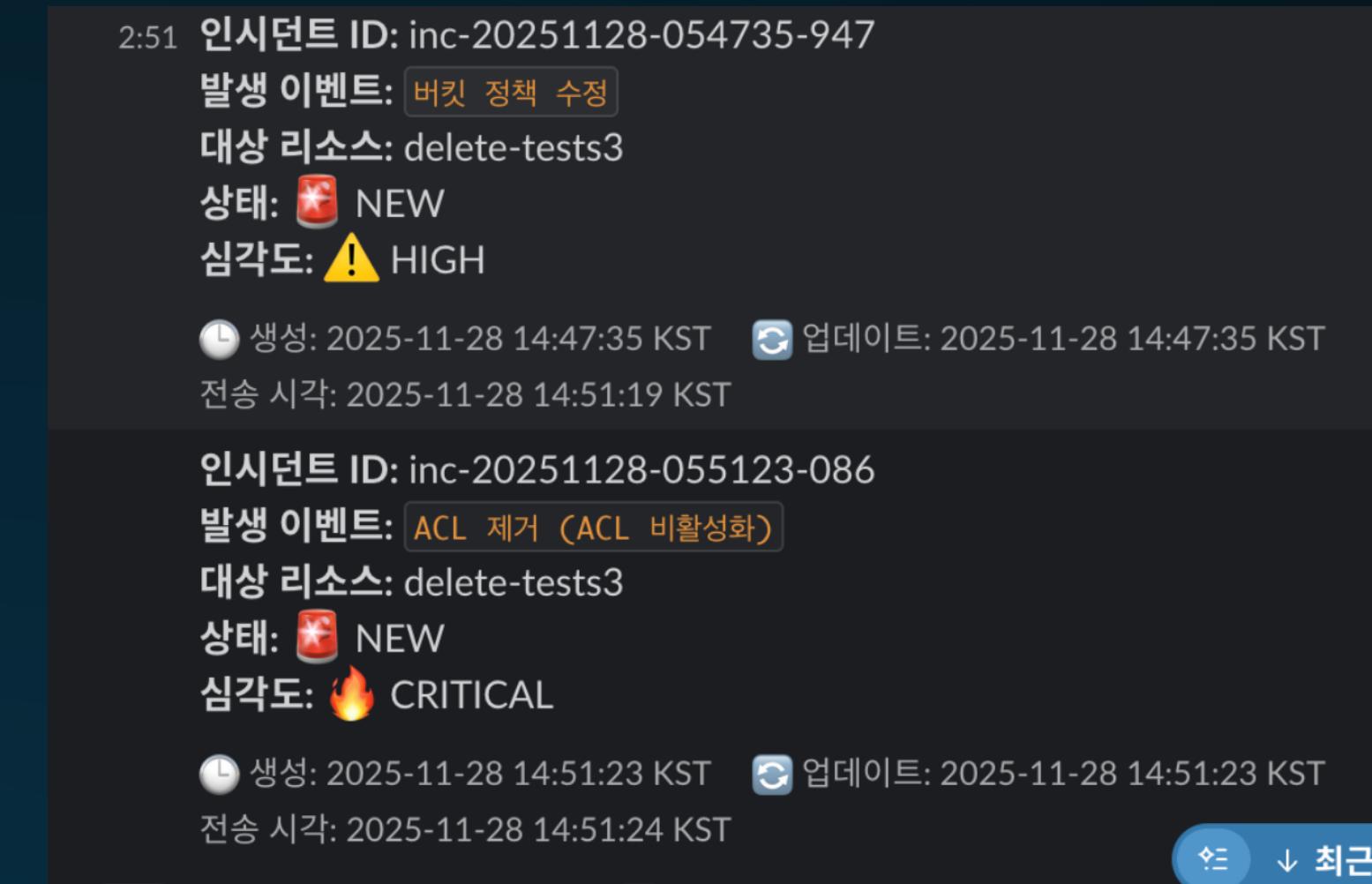
인시던트 이력 관리 (History)						
인시던트 ID	이벤트 유형	리소스	심각도	상태	알림 상태	메모
inc-20251201-022459-348	사용자 태그 추가	user:test_seowon	LOW	NEW	SENT	-
INC-20251201-022458-101	액세스 키 생성	arn:aws:iam::021417007719:user/seowon	HIGH	NEW	SENT	-
inc-20251201-022414-978	액세스 키 삭제	accessKeyId:AKIAQJ7ENTJT2ZSITEWD	MEDIUM	NEW	SENT	-
inc-20251201-022356-160	액세스 키 상태 변경	accessKeyId:AKIAQJ7ENTJT2ZSITEWD	MEDIUM	NEW	SENT	-
inc-20251201-022246-110	사용자 태그 추가	user:test_user_1	LOW	NEW	SENT	-
INC-20251201-022246-903	액세스 키 생성	arn:aws:iam::021417007719:user/seowon	HIGH	NEW	SENT	-
inc-20251201-022135-851	사용자 태그 추가	user:test_seowon	LOW	NEW	SENT	-

상세정보 및 조치



- 보안 이벤트 클릭 시 상세화면 확인 가능
- 진행 상태 및 메모 수정 가능
- 생성일, 이벤트 유형, 상태, 심각도 확인 가능
- 스크롤 하여 추가 상세 데이터를 json형태로 확인 가능

알림시스템 (Slack)

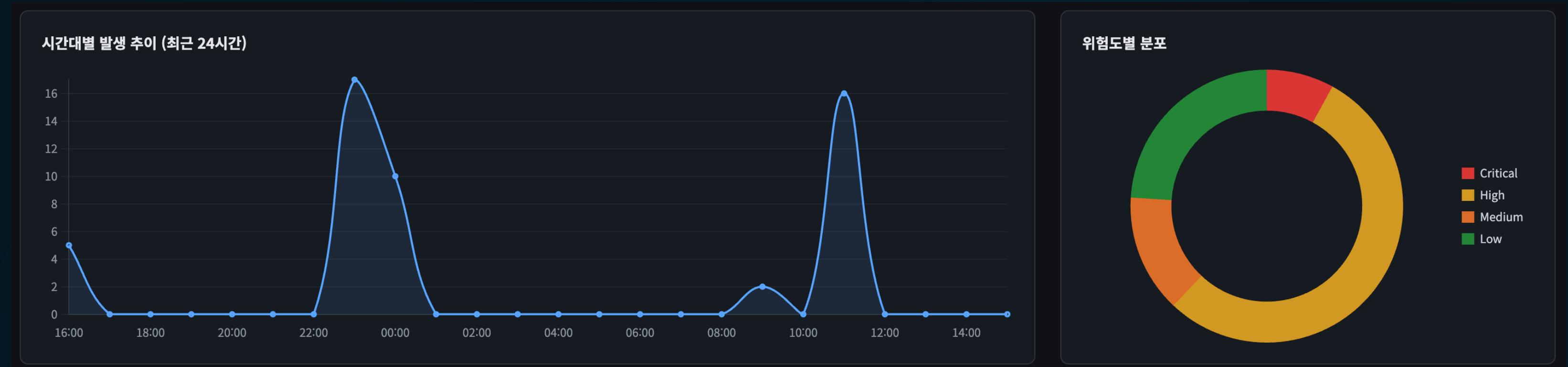


시연 영상

Layer 3 팀 결과물 시연 영상

팀원 : 석대원, 신유주, 안지서, 윤서원

테스트 결과



Critical Severity

탐지 성공률: 100%
자동 대응 성공률: 100%
MTTR: 2~4초

High Severity

탐지 성공률: 100%
일부 자동 대응은 조건부 처리
(AccessKey 이상, 보안그룹 이상 등)
알림/대시보드 반영 정확

기술적 트러블 슈팅과 프로젝트 성과



01. 기술적 트러블 슈팅

- WebSocket 세션 관리 최적화
 - 유저 상태 지속 시 연결이 끊기는 문제를 해결하기 위해 Heartbeat(ping/pong) 메커니즘 도입
 - 클라이언트(JS) 단에 자동 재연결(Auto-Reconnect) 로직을 구현하여 끊김 없는 모니터링 환경 제공
- 대규모 트래픽 처리를 위한 비동기 버퍼링
 - 보안 로그 폭주 시 Lambda 스로틀링 발생 방지
 - Amazon SQS를 중간에 배치하여 트래픽을 대기열에서 안정적으로 처리하는 아키텍처 구현



02. 프로젝트 성과

- 고속 대응 체계: 보안 위협 탐지부터 격리까지 MTTR 5초 미만 달성
- 안정적 아키텍처: SQS 버퍼링 및 Serverless 도입으로 대용량 트래픽 처리 안정성 및 비용 효율성 동시 확보
- 실시간 관제 환경: Websocket 기술을 활용하여 새로고침 없는 Zero-Delay 모니터링 대시보드 구축

Q&A