Cloud Security Auto-Remediation Architecture

Subtitle: Event-driven security automation system to detect and automatically remediate insecure cloud configurations in real time

Tech stack: Terraform · GitHub Actions · AWS CloudTrail · EventBridge · Lambda

Name: SeokHyun Yoo

Role: Security Automation / Cloud Security

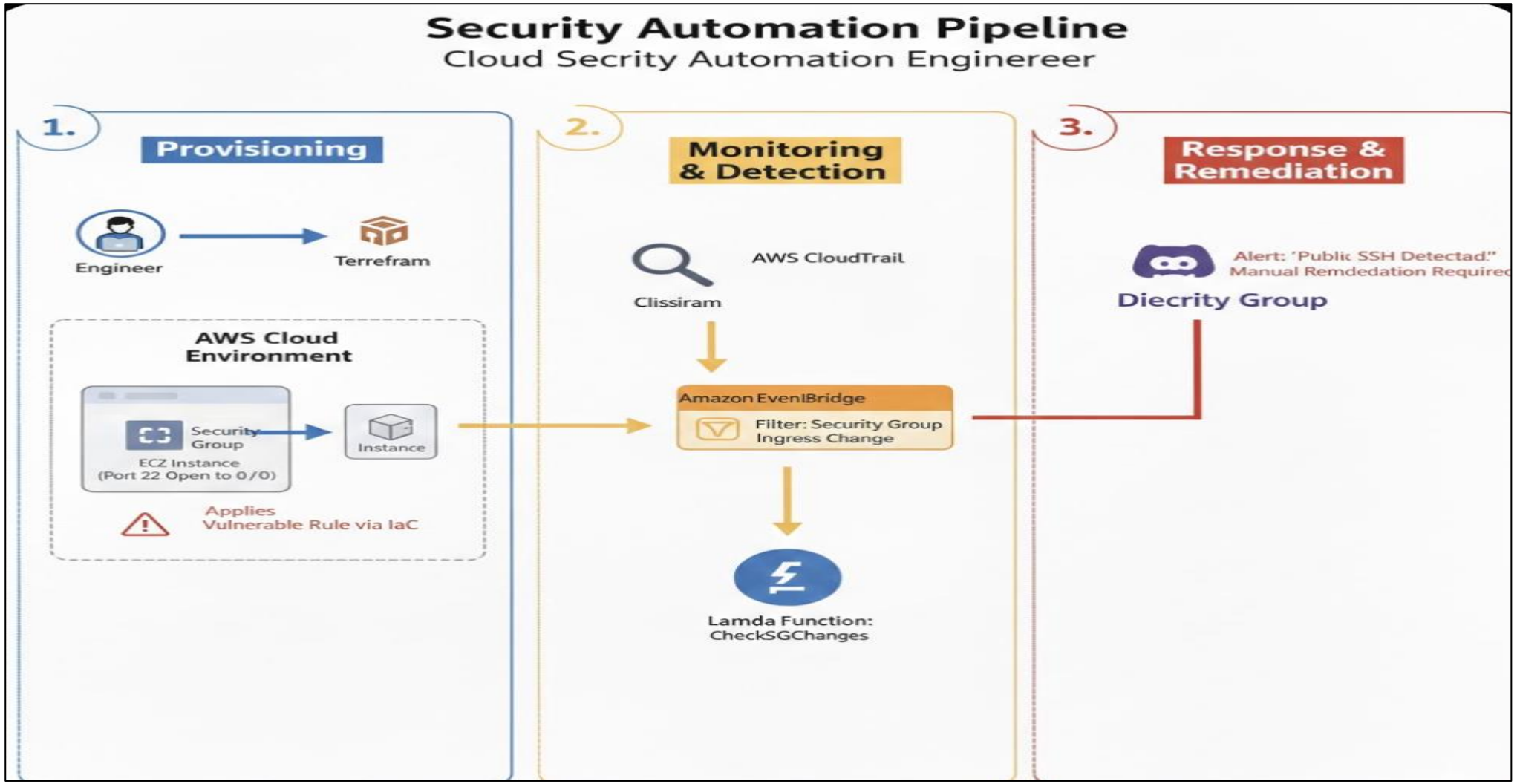
Keywords: CI/CD, IaC, Event-driven Security Automation

Problem Definition

- **현실 문제**
- 클라우드 환경에서 **Security Group 0.0.0.0/0 SSH 오픈**은
- 침해사고의 **가장 빈번한 초기 침투 벡터**

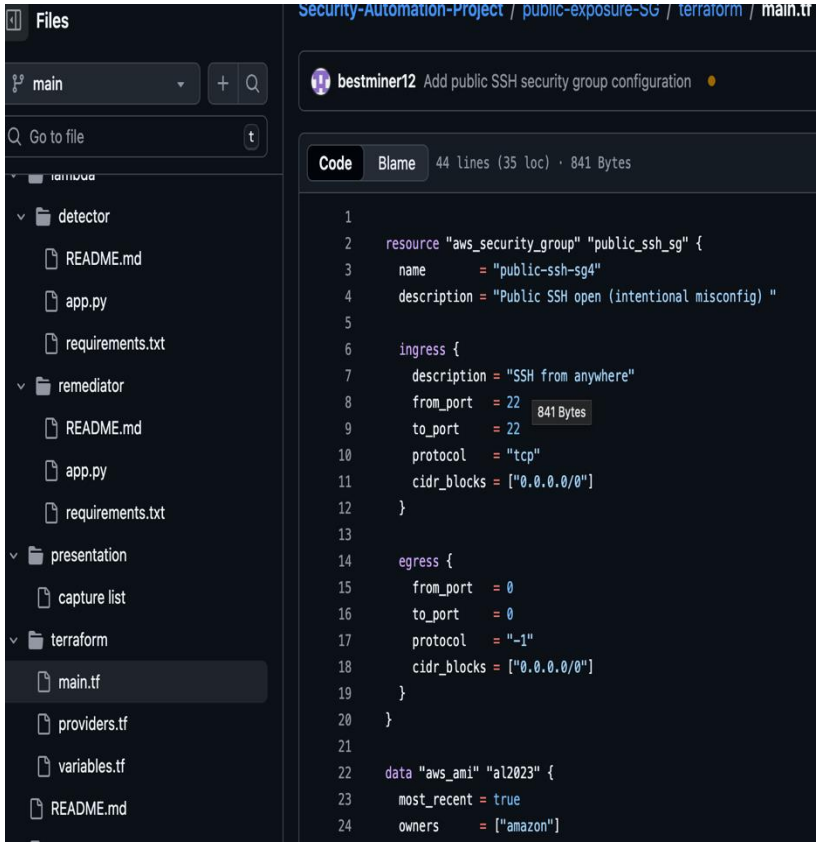
- 운영 환경에서:
- 수동 탐지 → 지연
- 수동 대응 → 휴먼 에러
- 야간/비근무 시간 → 대응 공백

High-Level Architecture

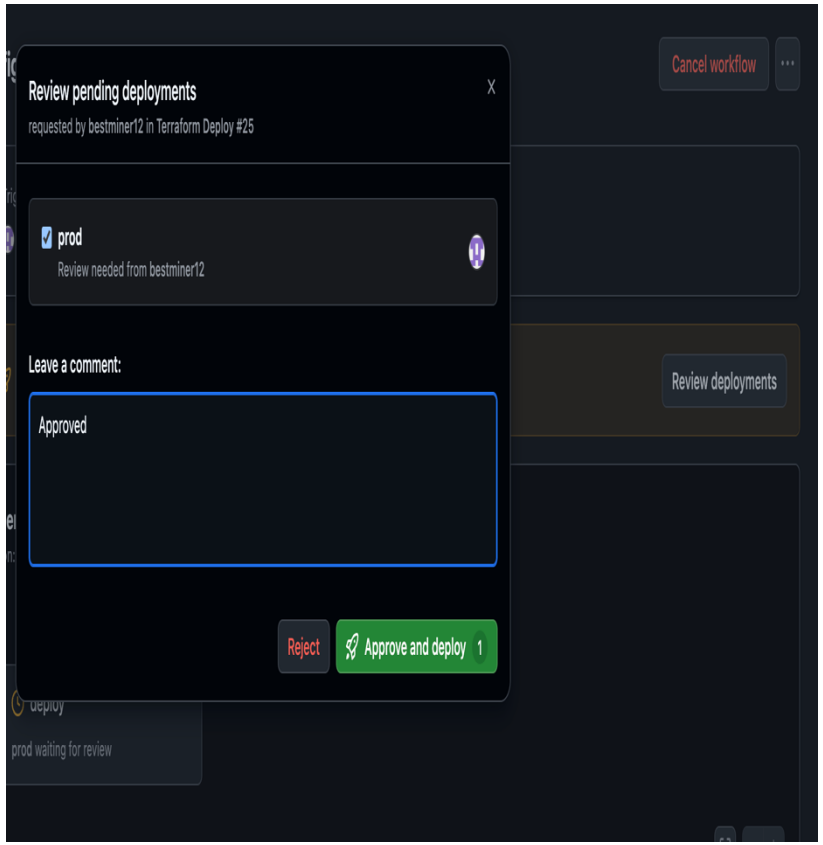


Terraform Apply, CI/CD

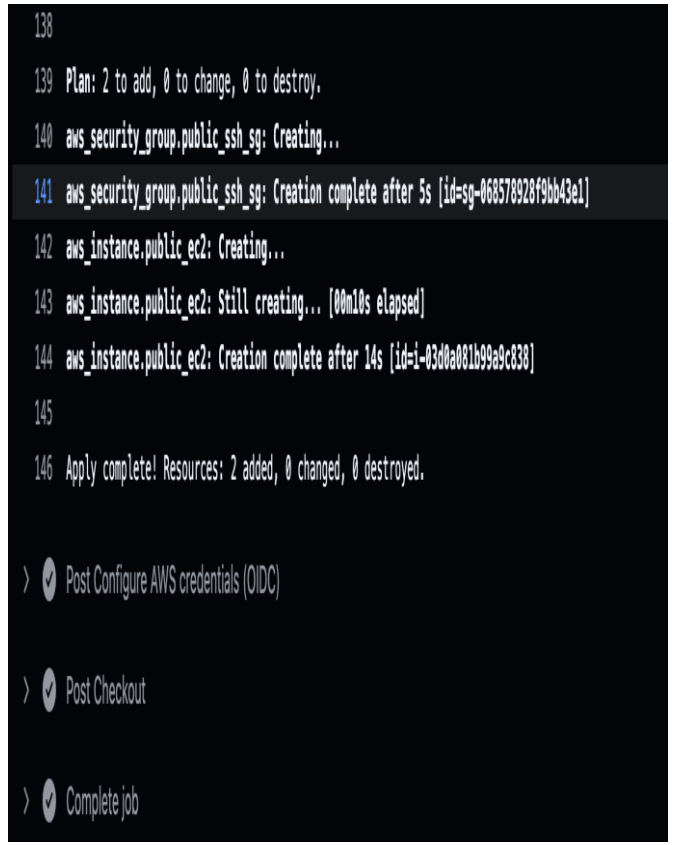
1. Terraform Code



2. Approval-based CD

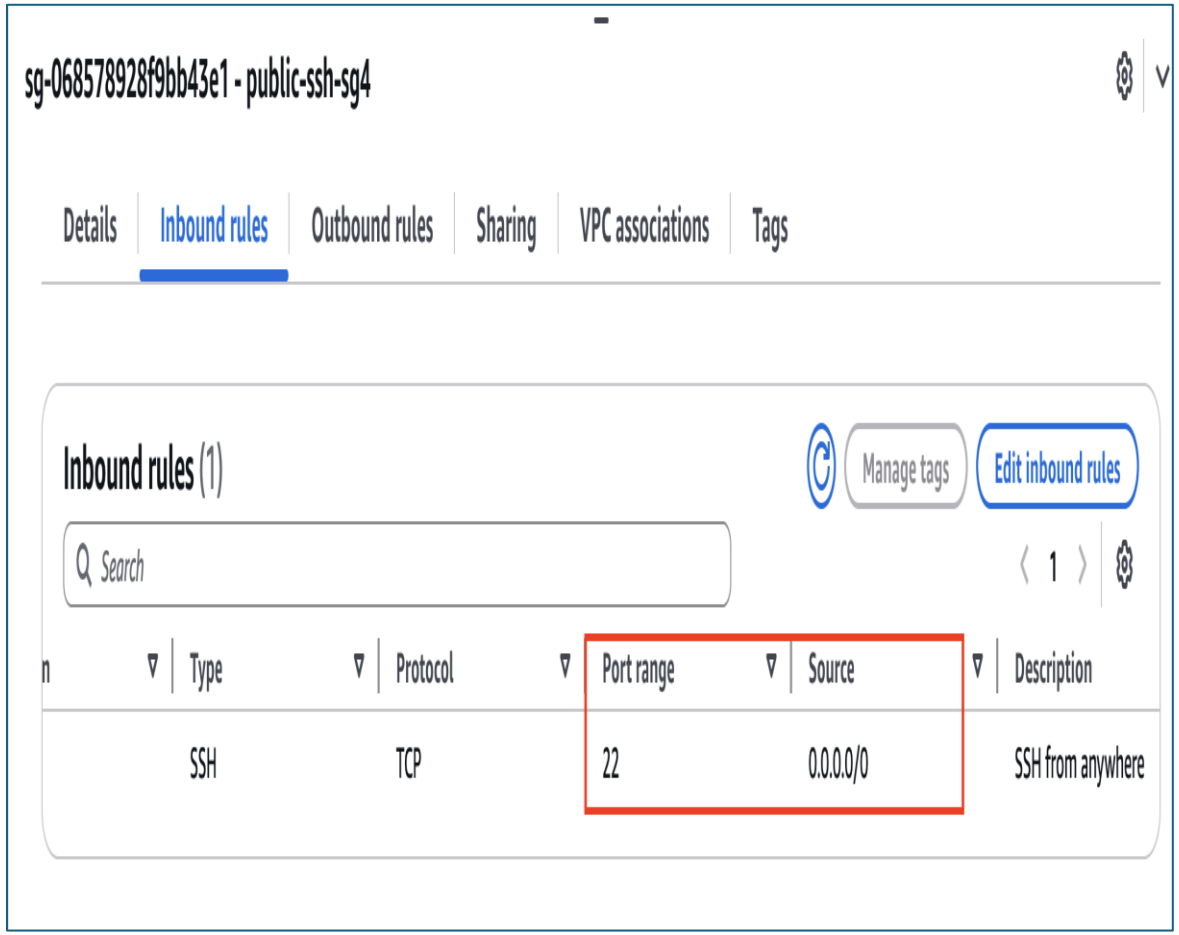


3. Resource deploy

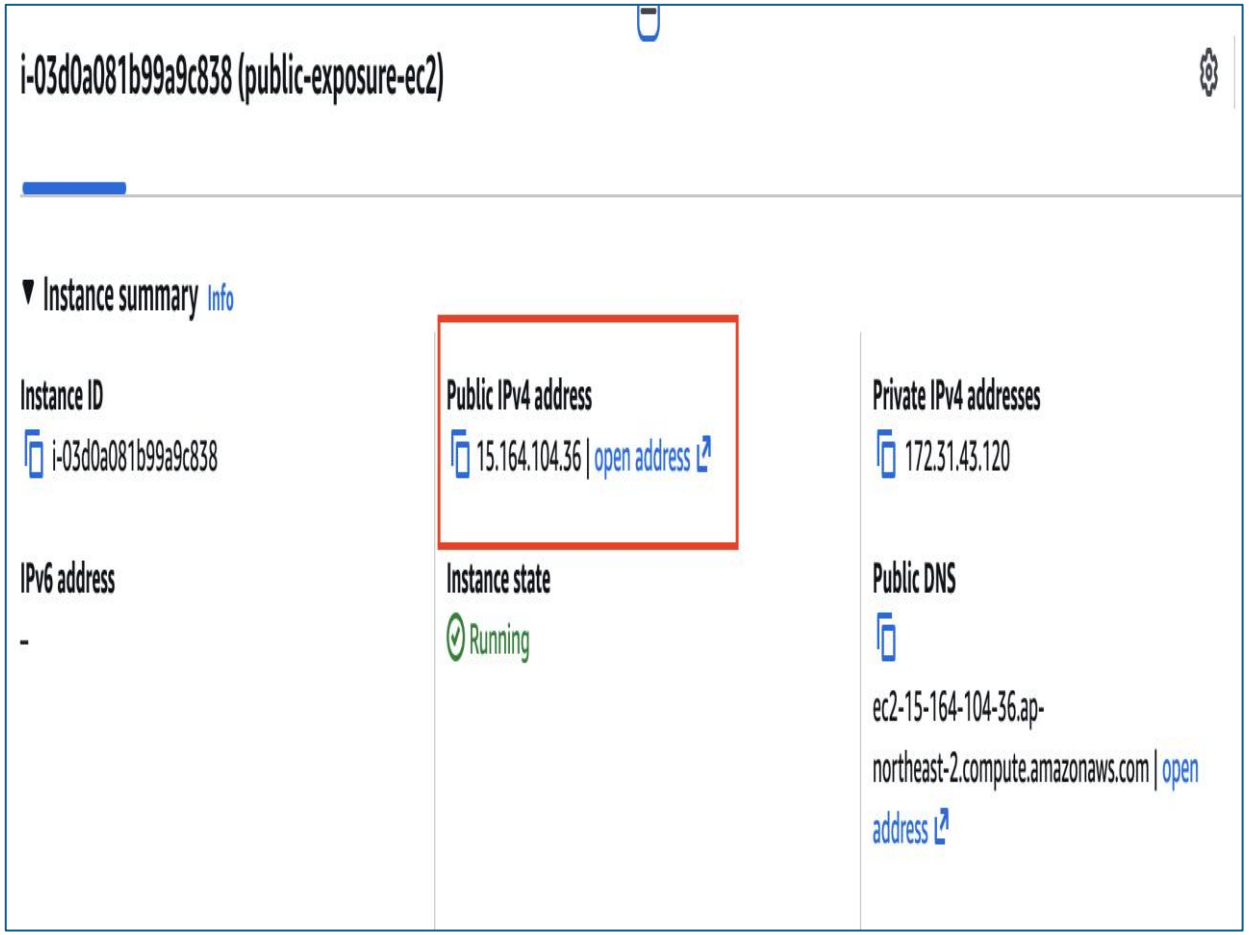


AWS Console Resource check

1. SG opend to any public ssh port

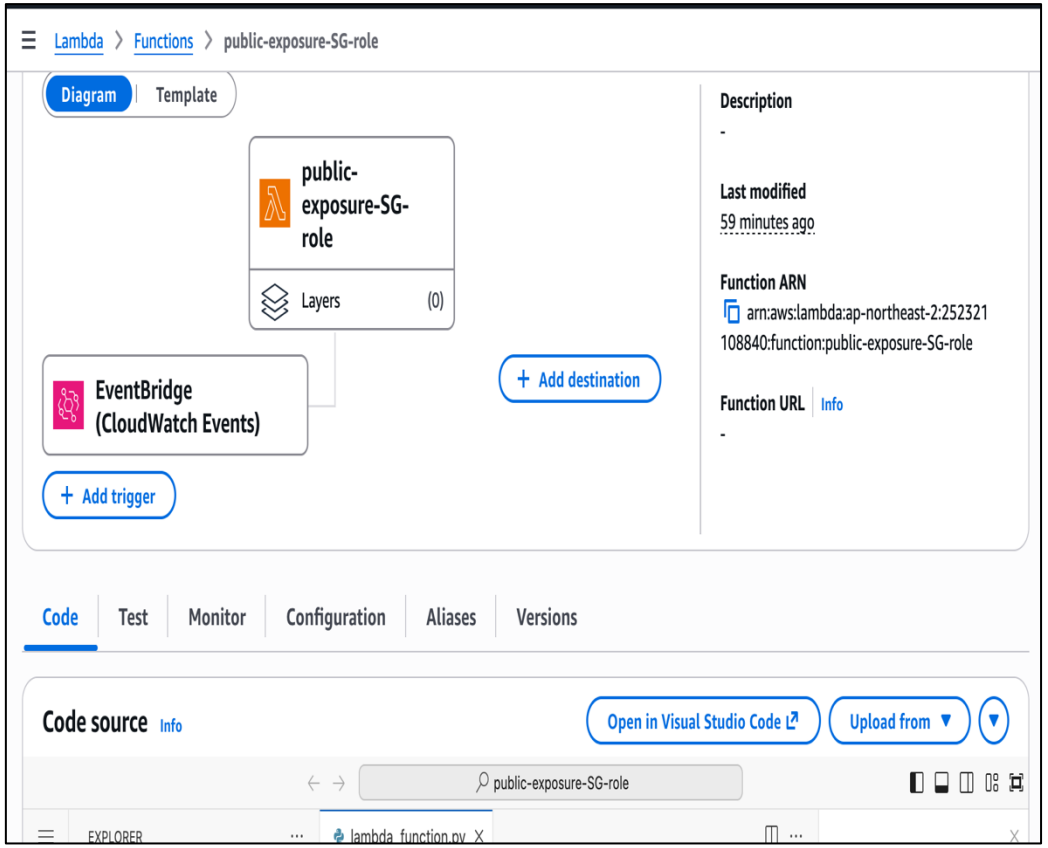


2. EC2 setting public IP

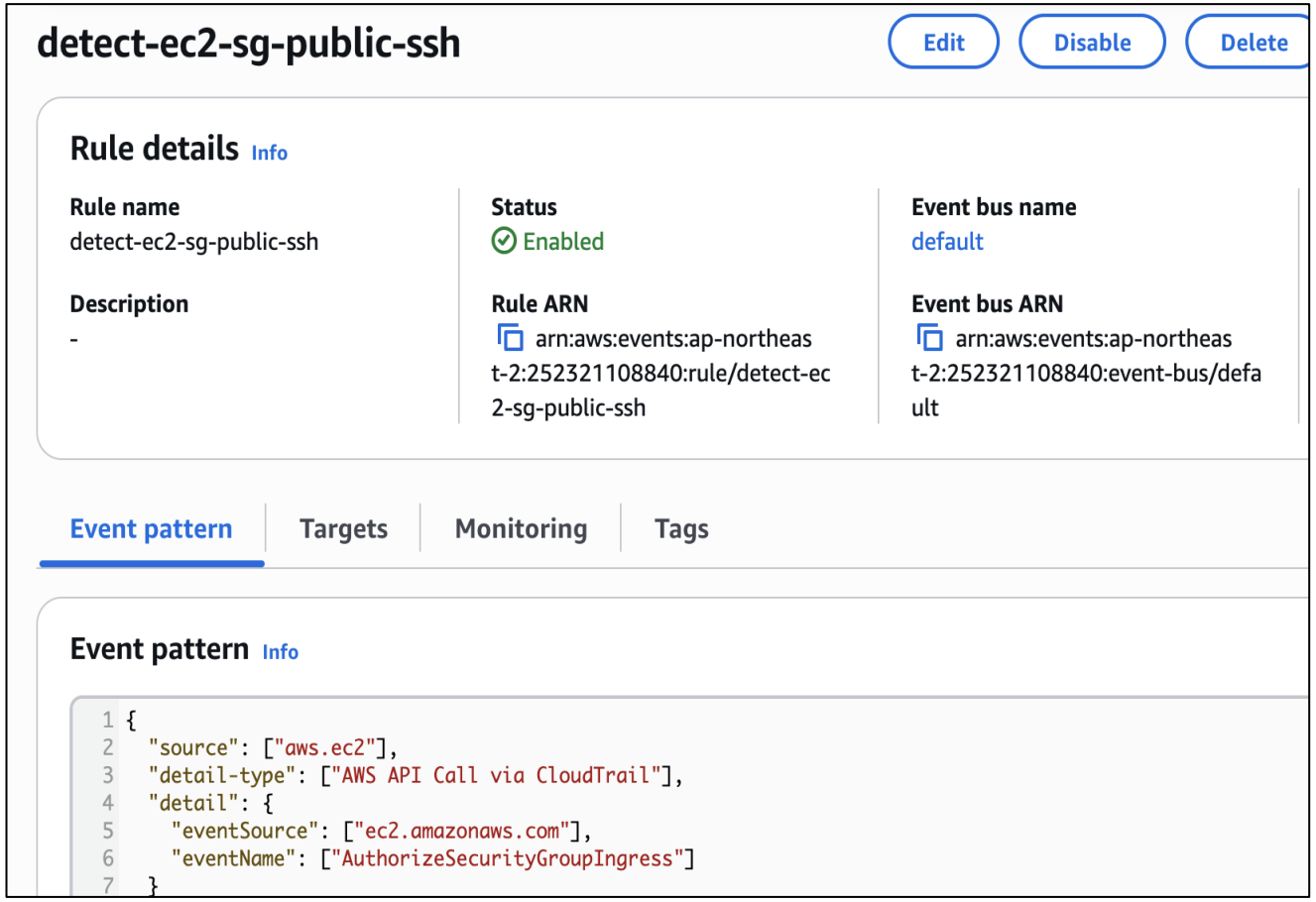


Lamda, Event bridge setting

1. Detecting Lamda setting

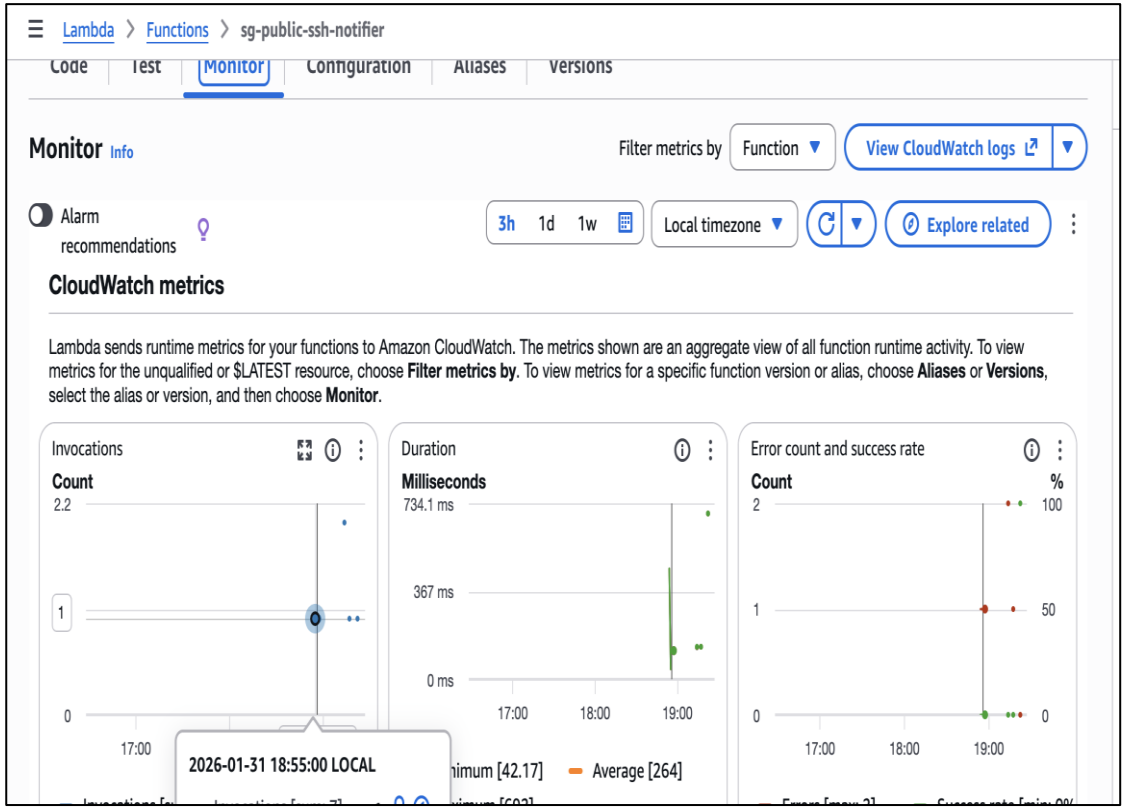


2. Event bridge setting

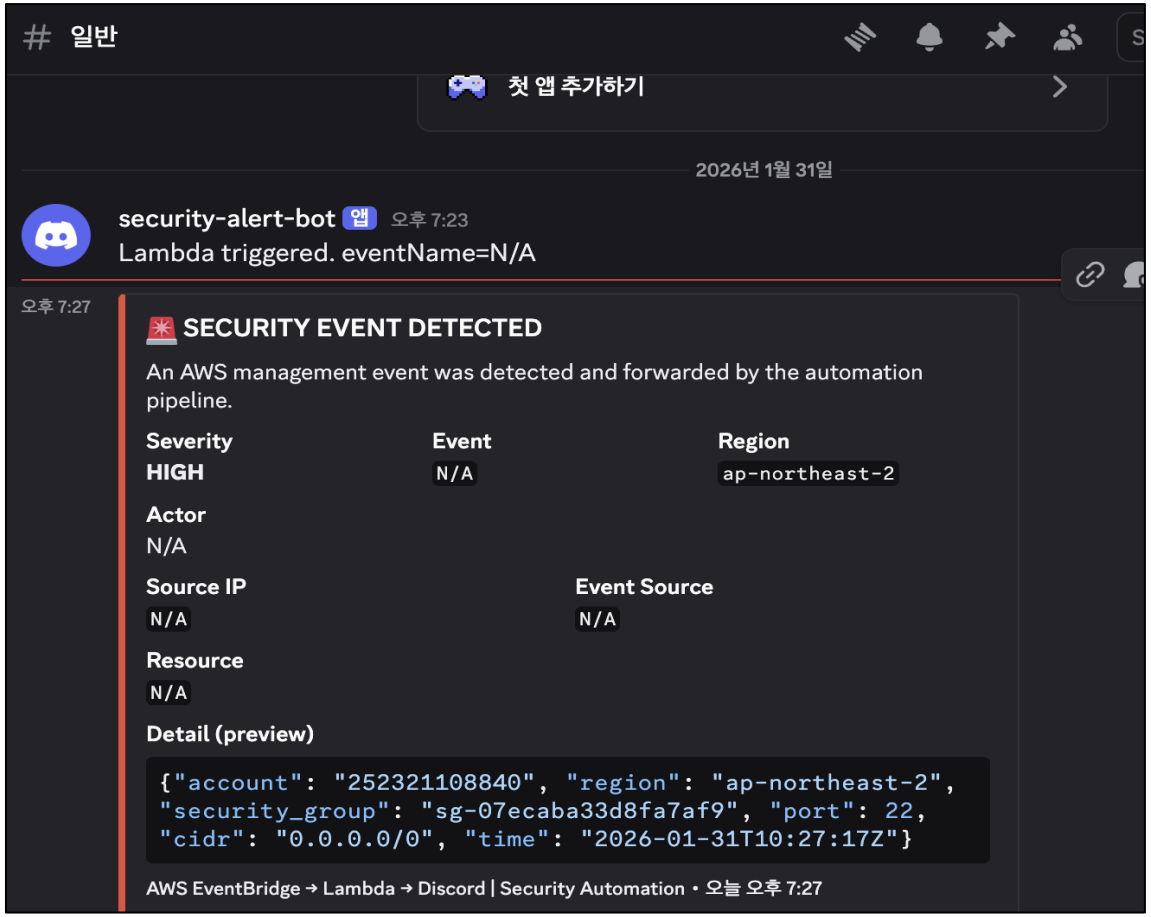


Send alert info to discord

1. Notifier lamda setting

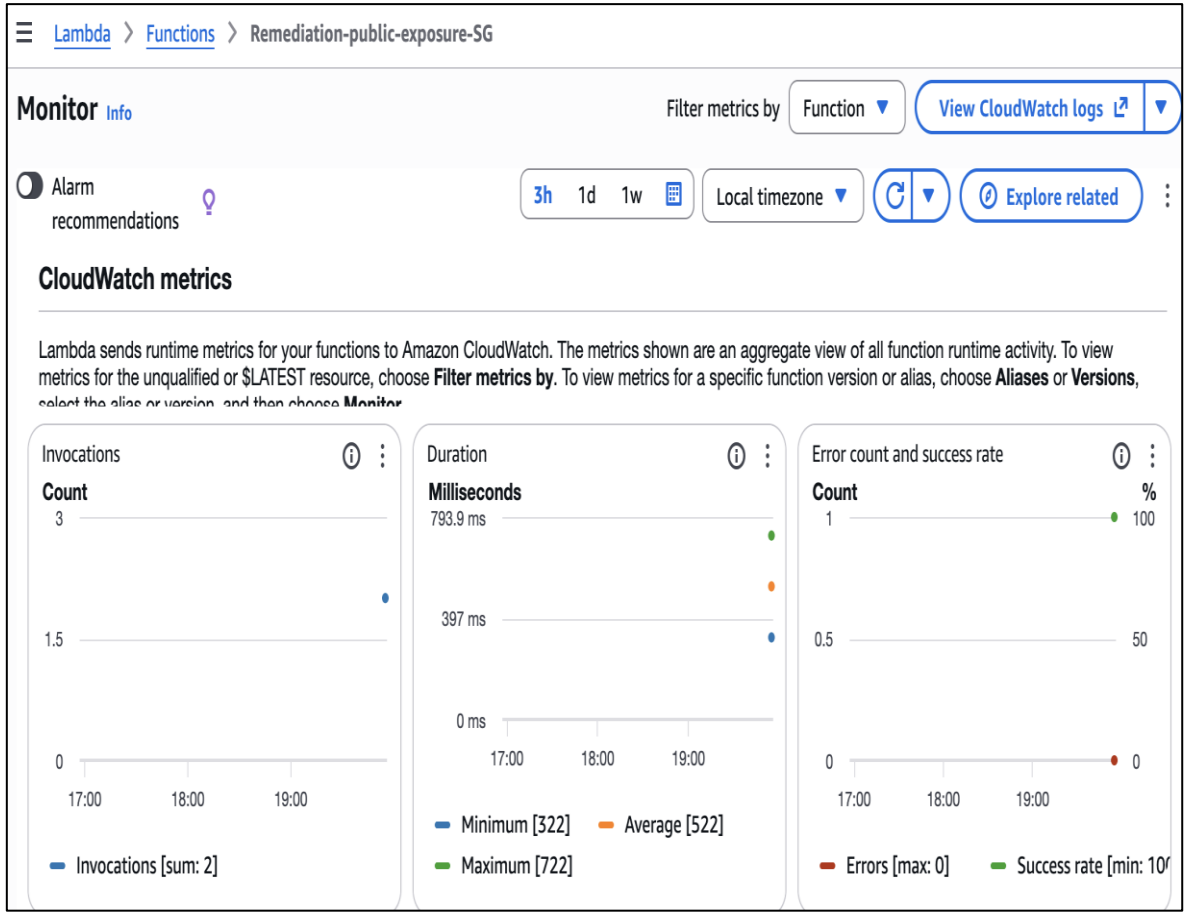


2. Send alert to discord



Automated Remediation (Security Group Hardening)

1. Remediation Lambda Configuration



2. Analyst-Driven Remediation Decision