# 클라우드 환경의 침해사고 탐지 및 대응 환경 구축

입문자 및 비전공자를 위한 실습 위주 워크북 제작


| | | | |
|---|---|---|---|
| **제출일** | 2025. 08. 10 | **팀명** | AWS지 말라고 했지 |
| **담당멘토** | 송수호 | **담당PL** | 우동규 |
| **팀원** | 김기원(PM), 강유림, 권도원, 김진서, 박도은, 손형은, 장희영, 조민혁 | | |

## [목차]

# 프로젝트 개요 및 소개

## 프로젝트 배경 및 필요성

최근 많은 기업들이 기존의 온프레미스(On-Premise) 환경에서 보다 유연하고 확장성이 뛰어난 클라우드 기반 인프라로 빠르게 전환하고 있다. 이와 같은 변화는 IT 운영의 효율성과 비용 절감 측면에서 다양한 이점을 제공하지만, 동시에 전통적인 보안 통제 모델이 적용되기 어려운 새로운 위협 환경을 초래하고 있다.

특히 클라우드 환경에서는 경계 기반 보안 모델의 유효성이 약화되며, 사용자 인증·인가의 복잡성과 자산 가시성 부족 문제 등으로 인해 보안 사고 발생 가능성이 증가하는 추세다. 실제로 다수의 조직이 클라우드로 전환한 이후, 구성 오류(misconfiguration), 과도한 권한 부여, 로그 수집 누락 등으로 인해 침해사고에 노출된 사례가 보고되고 있다.

그럼에도 불구하고, 현재 클라우드 환경에서의 침해사고 탐지 및 대응 역량을 기르기 위한 교육 자료는 여전히 부족하다. 기존의 기술 문서나 교육 콘텐츠는 대부분 클라우드에 대한 사전 지식을 전제로 하고 있어, 입문자나 비전공자에게는 진입 장벽이 높다. 이로 인해 실제 사고 발생 시 초기 대응 실패 및 피해 확산 가능성이 커질 수 있다.

따라서, 클라우드 환경에서 발생할 수 있는 보안 위협에 효과적으로 대응하려면, 클라우드 보안의 기초부터 침해사고 대응 절차에 이르기까지 누구나 쉽게 이해할 수 있는 체계적이고 실용적인 교육 자료가 필요하다. 본 프로젝트는 이러한 교육 격차를 해소하고, 다양한 배경을 가진 사용자들도 클라우드 보안에 대한 기본 역량을 갖출 수 있도록 지원하기 위해 기획되었다.

## 프로젝트 목표

본 프로젝트는 클라우드 환경에서 발생할 수 있는 침해사고에 효과적으로 대응할 수 있도록, 입문자와 비전공자도 쉽게 이해할 수 있는 실습 중심의 학습 콘텐츠를 개발하는 것을 주요 목표로 한다.

특히 이 콘텐츠는 클라우드 보안의 가장 기초적인 시나리오부터 심화된 침해사고 대응 과정까지 단계적으로 학습이 가능하며, 각 콘텐츠마다 해당 기술의 사용 이유 및 사용 방법을 제공하여 이론과 실습을 병행함으로써 학습의 효율성을 극대화할 수 있다. 이를 통해 학습자는 능동적으로 보안 위협을 인식하고 대응하는 역량을 키울 수 있다.

## 프로젝트 구성

### 1. AWS 서비스

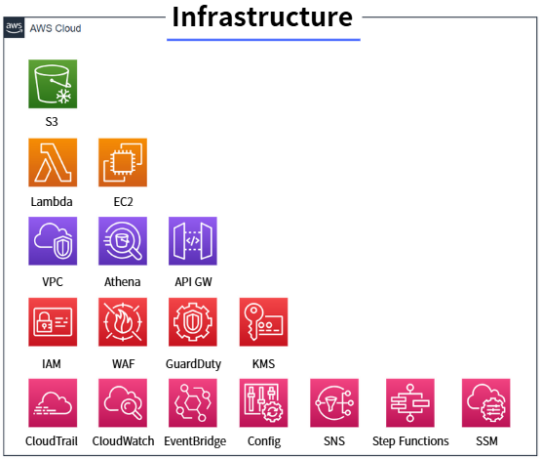


**그림 1. 프로젝트에서 사용된 주요 AWS 서비스**

본 프로젝트는 클라우드 기반 보안 환경에서 침해사고를 효과적으로 탐지하고 대응할 수 있는 자동화된 체계를 구축하기 위해 Amazon Web Services(AWS)를 주요 인프라로 채택하였다. 그림 1은 본 프로젝트에서 실제로 활용된 주요 AWS 서비스를 보여주며, AWS는 글로벌 수준의 안정성과 확장성을 제공할 뿐만 아니라, 다양한 보안 서비스와 로깅 기능, 이벤트 중심의 자동화 도구를 포괄적으로 지원함으로써 보안 사고 대응 시나리오 구현에 적합한 플랫폼이기에 해당 클라우드 서비스를 선택하였다.

### 2. Terraform


**그림 2. 프로젝트에서 사용된 IaC(Terraform)**

인프라 구성과 운영의 효율성 및 자동화 수준을 극대화하기 위해 그림 2와 같이 Terraform을 활용한 Infrastructure as Code(IaC) 방식으로 환경을 구축했다. Terraform은 선언적 구문을 통해 클라우드 자원의 생성과 변경 사항을 코드로 관리함으로써 일관된 환경 배포와 신속한 재현성 확보, 협업 기반 변경 이력 관리가 가능하다. 특히 보안 자동화와 같이 반복적인 설정 작업이 많은 환경에서는 IaC 기반의 접근 방식이 필수적이며, 운영 리스크를 줄이고 구성 오류를 예방하는 데 크게 기여한다.

# 프로젝트 내용

## 탐지 및 알림 시나리오

**표 1. 탐지 및 알림 시나리오 목록**

| 분류 | 탐지 및 알림 시나리오 |
|---|---|
| **계정 및 인증 보안** | 루트 계정 로그인 알림 |
| | 새로운 IAM User의 생성, 삭제 탐지 |
| **권한 상승 시도 또는 역할 조작** | 로그 그룹 삭제 또는 변경 탐지 |
| **네트워크 접근 제어 변경** | Security Group 정책 변경 탐지 |
| **감사 및 역할 변경** | AWS CloudTrail 비활성화 탐지 |
| **데이터/자산 공개 및 공유 행위** | S3 퍼블릭 버킷 생성 탐지 및 알림 |
| | 스냅샷 / 자원 공유를 통한 은폐 및 유출 시도 시나리오 |
| | 계정에 생성된 AMI를 외부에 공개로 등록하거나 외부 계정에 공유하는 시도 탐지 |

표 1은 본 프로젝트에서 정의한 탐지 및 알림 시나리오의 목록을 제시하며, 각 시나리오는 클라우드 환경에서 실제로 발생할 수 있는 기본적인 보안 위협 요소들을 주제로 구성되었다. 프로젝트에서는 총 8가지의 대표적인 보안 위협 시나리오를 선정하여 직접 구현하였으며, 각 시나리오는 AWS 환경에서 탐지 조건 설정, 이벤트 트리거, 알림 절차까지 포함하는 실행 가능한 형태의 워크북으로 제작되었다.

이러한 시나리오 기반 구성은 학습자가 단순히 위협 유형을 이론적으로 이해하는 수준을 넘어 실제 클라우드 인프라에서 발생 가능한 보안 이벤트를 직접 탐지할 수 있는 실습 경험을 제공하는 데 목적이 있다. 이를 통해 초급 학습자도 AWS 보안 서비스의 활용 방식과 기초적인 침해 탐지 자동화 설계 원리를 자연스럽게 습득할 수 있도록 하였다.

## 1. S3 퍼블릭 버킷 생성 탐지 및 알림

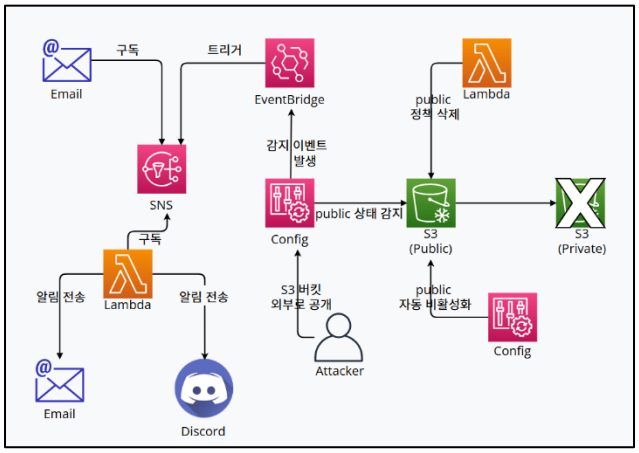


**그림 3. S3 퍼블릭 버킷 생성 탐지 및 알림 시나리오 워크플로우**

해당 시나리오는 Amazon S3 버킷이 공개(Public) 접근 설정이 되었을 때 이를 모니터링하고 탐지 가능할 수 있도록 구현했다. S3는 정적 웹 호스팅 용도, 데이터 저장 및 관리 등의 용도로 사용되며, 버킷 내부에는 중요한 비즈니스 데이터뿐만 아니라 사용자, 고객, 기업의 민감 정보가 포함될 수 있어 철저한 접근 관리가 필요하다. AWS Config 규칙과 SNS 알림을 활용하여 버킷 ACL 또는 정책이 공개 접근(Public Access)을 허용하는 경우 즉시 알림을 받도록 시나리오를 구성하였다.

그림 3은 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. 공격자가 S3 버킷을 퍼블릭 상태로 전환하려고 하면, 사전에 규칙을 설정해 두었던 Config가 이를 감지해 '규칙 비준수' 상태로 전환한다. EventBridge가 해당 이벤트를 감지하면 SNS로 전달하고, SNS는 이메일과 Lambda 함수에 알림 메시지를 전송한다. Lambda 함수는 메시지를 받아 Discord 채널로 실시간 알림을 발송한다. 또한 Lambda함수에 자동 대응을 구축하여 S3의 공개 접근이 허용된 것을 확인하게 되면 자동으로 퍼블릭 액세스 차단이 활성화되고, 버킷 정책이 제거된다.

## 2. 루트 계정 로그인 알림

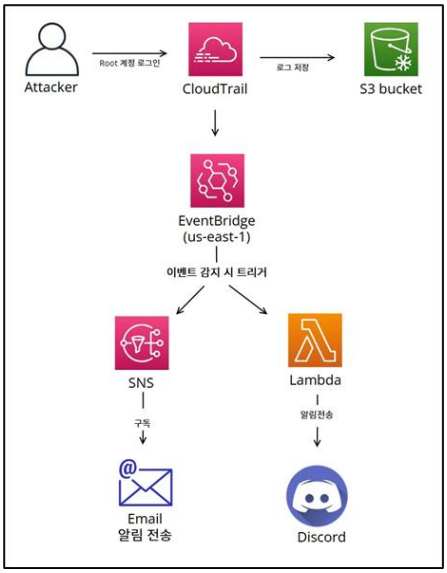


**그림 4. 루트 계정 로그인 알림 시나리오 워크플로우**

AWS 루트 계정은 모든 리소스에 대한 무제한 권한을 가지고 있기 때문에 실제 운영 환경에서 콘솔 로그인이 발생할 경우 반드시 즉시 탐지하고 관리자에게 알림을 전송하는 것이 매우 중요하다.

본 프로젝트에서는 이러한 요구를 충족하기 위해, 루트 계정 콘솔 로그인 이벤트를 CloudTrail과 EventBridge를 활용하여 실시간으로 감지하고, SNS와 Lambda를 통해 이메일 및 Discord Webhook 알림을 동시에 전송하는 자동화 체계를 구축하였다.
AWS에서 사용되는 모든 서비스는 us-east-1 리전에 구성하였으며, 루트 로그인 이벤트 수집에 사용되는 CloudTrail은 해당 리전에서만 지원되기 때문이다.

그림 4는 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. CloudTrail은 모든 루트 로그인 이벤트를 기록하고, 로그는 S3 버킷에 안전하게 저장한다. EventBridge에서 루트 로그인 이벤트를 감지하면, SNS와 Lambda를 통해 각기 이메일과 Discord에 알림이 전달된다. 이러한 프로세스는 간단한 단계별 아키텍처(CloudTrail → S3 저장 → EventBridge 감지 → SNS/Lambda 알림)로 구현되어, 각 서비스가 유기적으로 연동되는 구조를 갖췄다.

테스트 결과, 실제로 루트 계정 로그인이 발생했을 때 이메일과 Discord 모두에 알림이 정상적으로 전달되는 것을 확인하였으며, 이러한 자동화 체계를 통해 민감한 이벤트를 신속히 인지하고 실질적인 대응 기반을 마련할 수 있음을 검증하였다.

## 3. AWS Cloudtrail 비활성화 탐지

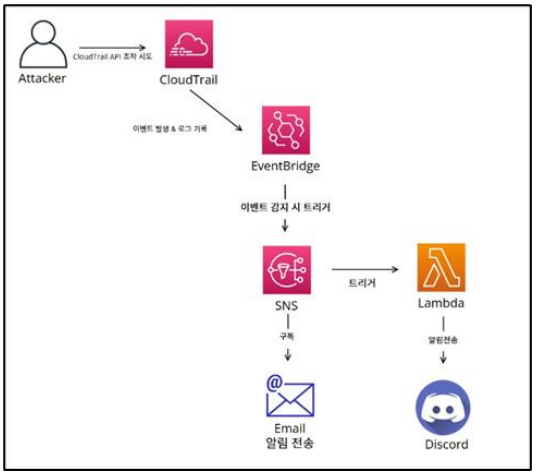


**그림 5. AWS Cloudtrail 비활성화 탐지 시나리오 워크플로우**

AWS Cloudtrail의 비활성화 및 조작 시도를 실시간으로 탐지하고, 관리자에게 즉시 알림이 전달되는 자동화 체계를 구축하였다. Cloudtrail은 AWS 내 모든 API 활동과 리소스 변경 내역을 기록하는 중요한 보안 서비스로, 로그 조작 시 심각한 위협이 발생할 수 있다.

AWS 콘솔에서 S3 버킷을 생성하고 버전 관리, 암호화, 공개 차단 등의 안전 조치를 적용했으며, Cloudtrail 트레일은 관리 이벤트와 인사이트 이벤트 기능을 활성화하고 로그 검증 기능도 함께 설정하였다. EventBridge에서는 지정한 Cloudtrail 이벤트를 감지해 SNS 주제로 전송하며, SNS는 이메일 및 Lambda에 알림을 전달한다. Lambda 함수는 Discord Webhook을 통해 실시간으로 관리자 채널에 경보를 발송한다.

그림 5는 언급한 시나리오 흐름에 대한 워크플로우를 보여준다. 실제로 StopLogging, DeleteTrail, UpdateTrail, PutEventSelectors 이벤트를 발생시켜 테스트한 결과, 이메일과 Discord 알림이 즉시 정상적으로 전달되어 탐지 및 알림 체계가 효과적으로 작동함을 확인하였다. 해당 시나리오는 향후 Athena 기반 로그 분석, 추가 SIEM 연계 등 자동화 대응 체계로 확장할 수 있도록 설계되었다. Lambda 메시지 포맷과 EventBridge 규칙도 손쉽게 수정 가능해 유연하게 대응할 수 있다.

## 4. Security Group의 정책 변경 탐지

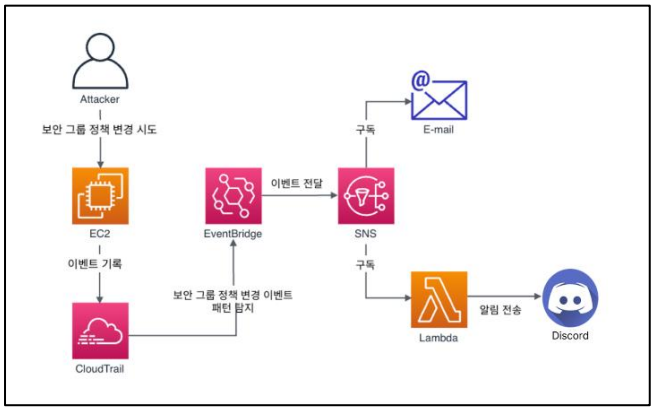


**그림 6. Security Group의 정책 변경 탐지**

해당 시나리오는 AWS 보안 그룹(Security Group)의 인바운드 및 아웃바운드의 규칙 변경을 실시간으로 탐지하고 알림을 받도록 설계하였다. 여기서 보안 그룹은 AWS의 다양한 리소스에 대한 네트워크 접근을 제어하는 역할을 하며, 인바운드 포트가 개방되거나 설정이 변경될 경우 외부 공격자에게 서비스 접근이 허용될 수 있다. 이에 따라 본 시나리오는 비인가된 접근 또는 설정 변경을 조기에 탐지하고 대응할 수 있는 자동화된 모니터링 체계를 구축하였다.

그림 6은 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. 공격자가 EC2 인스턴스에 적용된 보안 그룹의 설정을 변경하면 AWS는 해당 행위를 API 호출로 기록하며 CloudTrail을 통해 실시간으로 로그에 저장된다.

이때 접근 및 변경 사항에 따라 '*AuthorizeSecurityGroupIngress*'(인바운드 규칙 추가), '*RevokeSecurityGroupIngress*'(인바운드 규칙 제거), '*AuthorizeSecurityGroupEgress*'(아웃바운드 규칙 추가), '*RevokeSecurityGroupEgress*'(아웃바운드 규칙 제거), '*DeleteSecurityGroup*'(기존 Security Group 삭제)의 API 이벤트로 분류되어 저장된다. CloudTrail은 해당 이벤트를 JSON 로그 형태로 EventBridge에 전송한다. EventBridge는 사전에 정의된 이벤트 패턴을 기반으로 전달받은 API 호출 중 보안 그룹 변경과 관련된 이벤트만을 필터링한다. 이벤트 감지 시 EventBridge는 지정된 SNS 주제로 해당 이벤트를 전송한다. SNS는 사전에 등록된 두 엔드포인트로 탐지 메세지를 보낸다. 여기서 앤드포인트는 관리자 이메일 주소와 Discord Webhook을 연결한 Lambda 함수로 지정한다.

Lambda에 연결된 Discord 알림 메시지의 경우, 이벤트 이름, 발생 시간(KST), 보안 그룹 ID, 사용자 ARN, 소스 IP, AWS 리전, 계정 ID 등의 정보를 포함하여 Markdown 기반의 구조화된 형식으로 구현하였다.

## 5. 새로운 IAM User의 생성, 삭제 탐지

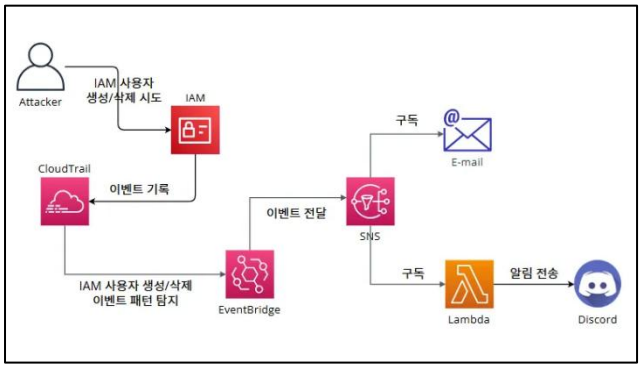


**그림 7. 새로운 IAM User의 생성, 삭제 탐지 시나리오 워크플로우**

IAM 사용자는 AWS 리소스에 대한 접근 권한을 가지므로 새로운 사용자가 생성되거나 삭제되는 행위는 보안상 중요한 이벤트이다. 승인 받지 않은 사용자 생성은 권한 남용이나 계정 탈취 등 보안 사고로 이어질 수 있으므로 이러한 행위를 탐지하고 변경 이력을 검토해야 한다. 그림 7은 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. 공격자가 IAM 사용자 생성 또는 삭제를 시도하면, 해당 기록은 CloudTrail에 자동으로 저장된다. 해당 기록 발생 시 EventBridge가 탐지 후 SNS로 이벤트를 전달하면 SNS는 구독 중인 이메일과 Lambda 함수에 알림을 전송한다. Lambda 함수는 수신한 이벤트를 필요한 데이터만 추출하여 가독성 높은 형태로 Discord 채널에 알림을 전송하는 구조이다.

## 6. 로그 그룹 삭제 또는 변경 탐지

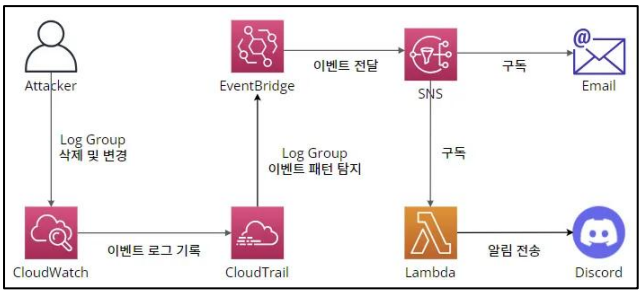


**그림 8. 로그 그룹 삭제 또는 변경 탐지 시나리오 워크플로우**

로그 그룹은 CloudWatch의 로그를 그룹화해 관리하는 컨테이너이다. 로그 그룹을 삭제하거나 보존 기간, 리소스 정책 등 로그 그룹 구성을 변경하는 행위는 정상적인 분석을 방해하거나 감사 추적을 회피하려는 악의적 의도가 있을 수 있으므로 보안상 매우 중요한 이벤트이다. 그림 8은 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. 공격자가 CloudWatch 로그 그룹을 삭제, 또는 변경 시도하면, 해당 기록은 CloudTrail에 자동으로 저장된다. 해당 기록 발생 시 EventBridge가 탐지 후 SNS로 이벤트를 전달하고, SNS는 구독

대상인 이메일과 Lambda 함수로 이벤트를 전달한다. Lambda 함수는 수신한 이벤트에서 필요한 정보를 추출하여 Discord로 알림을 전송하는 구조이다.

## 7. 스냅샷 / 자원 공유를 통한 은폐 및 유출 시도

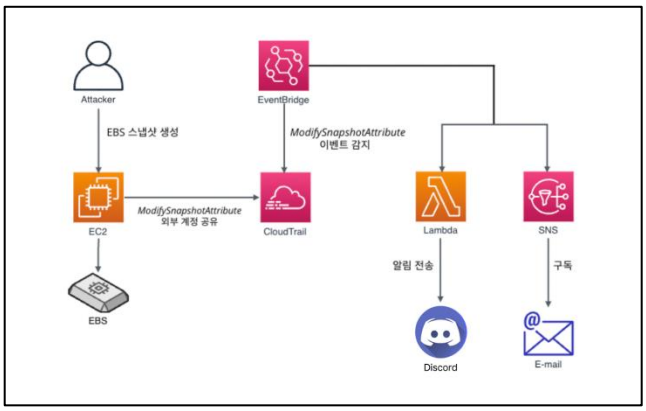


**그림 9. 스냅샷 / 자원 공유를 통한 은폐 및 유출 시도 시나리오 워크플로우**

AWS EC2 인스턴스에 연결된 EBS(Elastic Block Store) 볼륨의 스냅샷이 외부 AWS 계정과 공유되는 행위를 실시간으로 탐지하고 알림을 받을 수 있도록 본 시나리오를 구성하였다. EBS 스냅샷에서는 EC2 인스턴스의 운영체제, 애플리케이션 설정, 민감한 로그 및 사용자 데이터를 포함될 수 있으므로, 외부 계정과 공유될 경우 데이터 유출로 이어질 위험이 있다. 이에 따라 스냅샷을 무단으로 생성하거나 외부 계정으로 공유, 또는 삭제하는 행위를 자동화된 방식으로 탐지하고 이를 관리자에게 즉시 알리는 시스템을 구축하였다.

그림 9는 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. 공격자가 EBS 스냅샷을 생성, 삭제 또는 외부 계정과 공유 시 해당 API 호출이 CloudTrail을 통해 이벤트로 기록된다. 이때 CloudTrail은 이 기록을 JSON 형식으로 EventBridge에 전달하며, 이벤트 패턴에 따라 'CreateSnapshot'(EBS 볼륨 스냅샷 생성), 'ModifySnapshotAttribute'(기존 스냅샷 삭제), 'DeleteSnapshot'(EBS 스냅샷 공유 설정 변경)로 필터링하여 감지한다. 감지된 이벤트는 SNS 및 Discord Webhook이 연결된 Lambda 함수로 전달한다. SNS는 지정된 앤드포인트인 관리자 이메일로, Lambda 함수는 Discord 채널로 알림을 전송한다.

## 8. 계정에 생성된 AMI를 외부에 공개로 등록하거나 외부 계정에 공유 시도 탐지

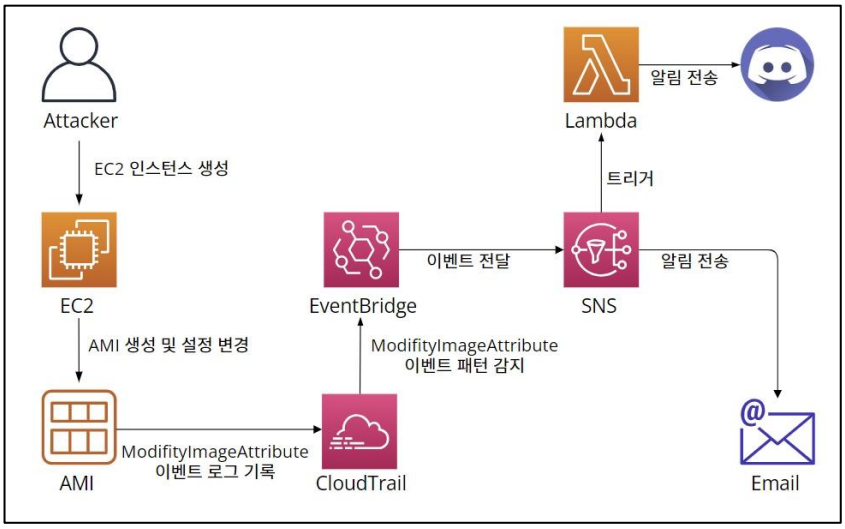


**그림 10. 계정에 생성된 AMI를 외부에 공개로 등록하거나 외부 계정에 공유 시도 탐지 시나리오 워크플로우**

본 시나리오는 Amazon EC2에서 생성한 AMI(Amazon Machine Image)가 외부에 퍼블릭으로 등록되거나 외부 계정에 공유되는 보안 위협을 탐지할 수 있도록 구현하였다. AMI는 서버 설정, 애플리케이션, 보안 구성 등이 포함된 이미지로, 내부 시스템 구성 정보가 포함되어 있을 수 있어 외부 공개 시 심각한 보안 사고로 이어질 수 있는 위험성을 지닌다. 이를 예방하기 위해 AMI 속성이 변경되며 외부에 퍼블릭 등록되거나 특정 AWS 계정에 공유되는 이벤트를 실시간으로 감지하고, Email 및 Discord를 통해 알림을 전송하는 구성으로 시나리오를 구축하였다.

그림 10은 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. EC2 인스턴스에서 생성된 AMI가 외부에 퍼블릭으로 등록되거나 외부 계정에 공유되는 보안 위협을 방지하기 위해 CloudTrail로 AMI 속성이 변경되는 이벤트(ModifyImageAttribute) 이벤트를 기록하고, 이벤트 중 launchPermission 속성이 포함된 것만 필터링하여 SNS로 전달한다. SNS는 사전 등록된 이메일과 Lambda 함수로 알림을 발송하며, Lambda 함수는 이 정보를 바탕으로 Discord 채널에 경고를 전송한다.

## 대응 시나리오

**표 2. 대응 시나리오 목록**

| 분류 | 탐지 및 알림 시나리오 |
|---|---|
| **감사 로그 조작 탐지** | EC2 내 bash history 조작 시도 |
| **감사 로그 분석** | Athena 기반 CloudTrail 비정상 API 사용 분석 |
| **위협 인텔리전스 모니터링** | GuardDuty의 Threat IP List를 활용한 모니터링 정책 구현 |
| **웹 방화벽 정책 관리** | AWS WAF를 통해 정책 관리 시나리오 및 모니터링 정책 구현 |
| **네트워크 자동 격리** | EC2에서 위험도 높은 악성행위 확인 시 네트워크 자동 격리 |

표 2는 본 프로젝트에서 구현한 대응 시나리오 목록을 보여준다. 대응 시나리오는 기존 탐지 및 알림 시나리오보다 심화된 시나리오이다. 해당 시나리오는 기존의 단순 탐지 후 알림 하는 것을 포함하여 대응하는 절차까지 제시한다. 해당 시나리오는 5가지 보안 위협 주제로 구성 되어 있다. AWS에서 제공하는 기존 서비스에서 더욱 심화된 서비스를 직접 다루어보며 실질적인 클라우드 보안 위협 탐지 후 대응이 가능해진다. 이를 통해 학습자는 보안 위협을 탐지하고 대응할 수 있는 역량을 갖출 수 있다.

## 1. EC2 내 bash history 조작 시도

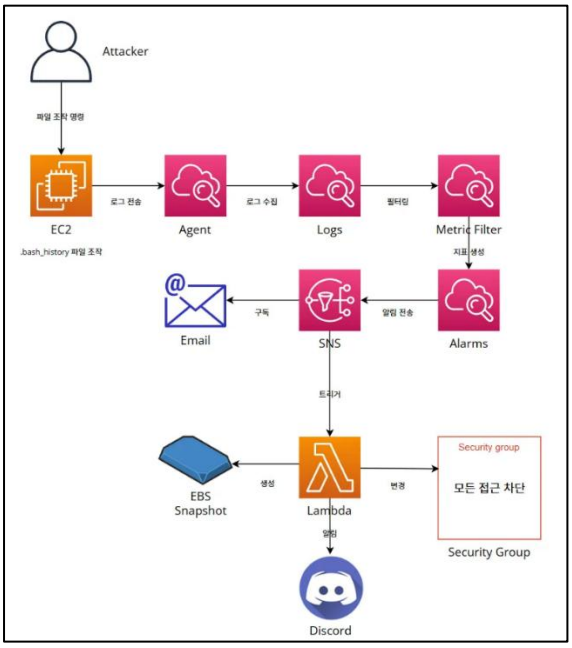


**그림 11. EC2 내 bash history 조작 시도 시나리오 워크플로우**

AWS EC2 인스턴스 내 .bash_history 파일은 명령 기록을 저장하는 중요한 로그로, 공격자가 이 파일을 삭제하거나 덮어쓰는 등의 조작을 시도할 경우 이는 흔적을 지우려는 침해 시도로 간주할 수 있다. 본 프로젝트에서는 이러한 행위를 실시간으로 탐지하고, 자동으로 관리자에게 경보를 전송하며, 즉시 대응까지 이어지는 아키텍처를 구현하였다. 그림 11은 해당 시나리오의 워크플로우를 보여준다. 시나리오의 주요 흐름은 다음과 같다. CloudWatch Agent를 EC2에 설치하여 .bash_history 파일을 실시간으로 모니터링하고, 해당 로그를 CloudWatch Logs에 전송하도록 설정하였다. Metric Filter는 history -c, echo > ~/.bash_history 등 의심스러운 명령어를 탐지하도록 구성되어 있다. 이상 행위가 체크되면 CloudWatch Alarm이 ALARM 상태로 전환되며, SNS를 통해 이메일과 Lambda 함수(Discord Webhook 포함)로 실시간 알림이 전송된다. Lambda 함수는 이벤트 발생 즉시 해당 EC2의 EBS 볼륨 전체에 대한 스냅샷을 자동 생성하고, 보안 그룹을 접근 불가(격리) 상태로 변경하여 추가 침해를 차단한다.

실제 시뮬레이션 결과, .bash_history 파일 조작 명령 발생 시 이메일과 Discord 채널에 경보는 5분 내로 전송되고, 해당 인스턴스는 자동으로 격리·백업되어 신속하고 효과적인 보안 대응이 이루어짐을 확인하였다. 해당 시나리오를 통해, EC2 내부의 주요 감사 파일 변조 시도에 대해 실시간 탐지, 경보, 자동 조치까지 연결된 안전한 운영 환경을 실질적으로 마련할 수 있음을 검증하였다.

## 2. Athena 기반 CloudTrail 비정상 API 사용 분석

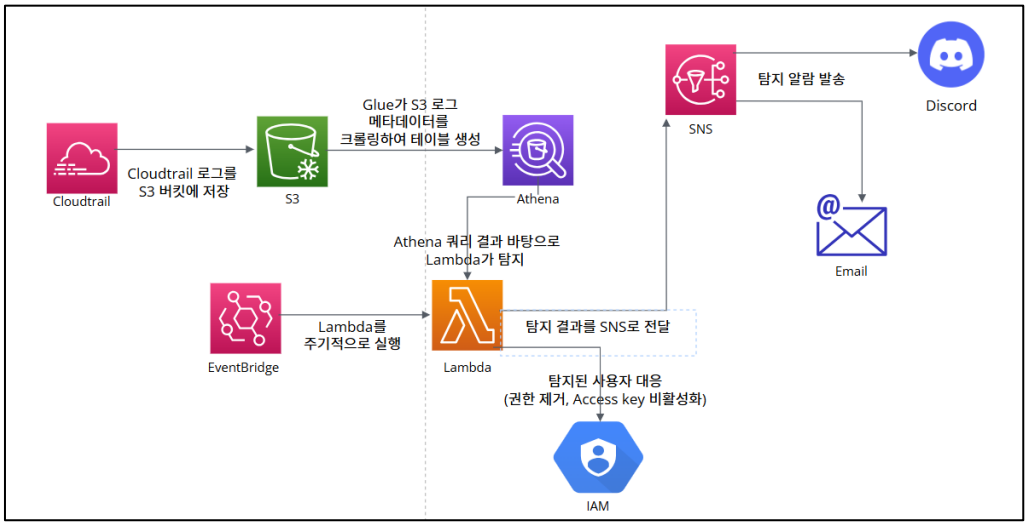


**그림 12. Athena 기반 CloudTrail 비정상 API 사용 분석 시나리오 워크플로우**

해당 시나리오는 Athena 기반 CloudTrail 로그 분석을 통해 야간 시간대의 비정상 API 호출(ConsoleLogin, CreateAccessKey 등)을 탐지하고 대응할 수 있도록 구현하였다. 그림 12는 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. 사용자가 야간 시간대인 밤 10시부터 오전 7시 사이에 AWS 콘솔에 로그인하거나, 액세스 키를 생성하는 등의 민감한 API 요청을 실행하면 해당 이벤트는 자동으로 CloudTrail 로그에 기록된다. 이 로그는 S3에 저장되고, EventBridge를 통해 일정 주기로 실행되는 Lambda 함수가 Athena 쿼리를 통해 최근 30분간의 로그를 분석한다. 분석 결과 야간 시간대에 로그인이나 액세스 키 생성과 같은 비정상 행위가 감지되면 탐지된 이벤트 정보가 정리되어 SNS를 통해 이메일로 전송되고, 동시에 Discord 웹훅을 통해 보안 알림 메시지가 전송된다.

이때 설정된 Lambda 함수가 자동 대응 기능까지 활성화한 상태라면, 알림을 보낸 후 즉시 감지된 사용자들의 IAM 권한을 모두 제거하고, 액세스 키를 비활성화하여 추가적인 피해를 방지한다. 최종적으로, 관리자나 보안 담당자는 이메일이나 Discord 메시지를 통해 어떤 사용자가 어떤 행위를 했는지, 해당 행위에 대해 어떤 대응이 이루어졌는지를 실시간으로 확인할 수 있는 구조이다.

## 3. GuardDuty의 Threat IP List를 활용한 모니터링 정책 구현

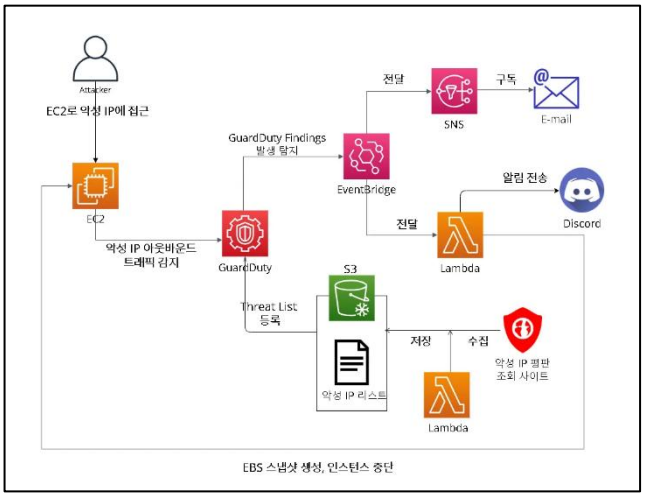


**그림 13. GuardDuty의 Threat IP List를 활용한 모니터링 정책 구현**

EC2는 웹 서버, 애플리케이션 서버, 데이터 처리, 백엔드 시스템 등 다양한 서비스의 핵심 인프라로 활용되기 때문에, 외부와의 네트워크 트래픽에 대한 보안 관리가 매우 중요하다. 이를 위해 외부 악성 IP 평판 조회 사이트에서 IP 정보를 주기적으로 자동 수집하여 GuardDuty의 위협 IP 목록에 등록하고, EC2에서 위협 IP로의 접근이 탐지되면 알림을 통해 관리자에게 전파한다. 추가로 Lambda 함수를 활용해 EC2 인스턴스 중단 및 EBS 스냅샷 생성 등 자동 대응 시나리오를 구현하여 보안 사고에 효과적으로 대처할 수 있도록 한다.

그림 13은 해당 시나리오의 워크플로우를 보여준다. 시나리오 흐름은 다음과 같다. Lambda 함수를 통해 악성 IP 평판 조회 사이트에 등록된 악성 IP를 자동으로 수집하여 S3 버킷에 저장하고, 이를 주기적으로 업데이트한다. 수집된 IP를 GuardDuty의 위협 IP 목록에 등록하고, 이후 공격자가 EC2를 탈취해 해당 위협 IP로 접근을 시도하면 GuardDuty Findings에 관련 기록이 저장된다. 이를 EventBridge에서 탐지해 SNS와 Lambda 함수로 이벤트를 전달하고, SNS와 Lambda는 각각 이메일과 Discord로 알림을 전송한다.

## 4. AWS WAF를 정책 관리 시나리오 및 모니터링 정책 구현

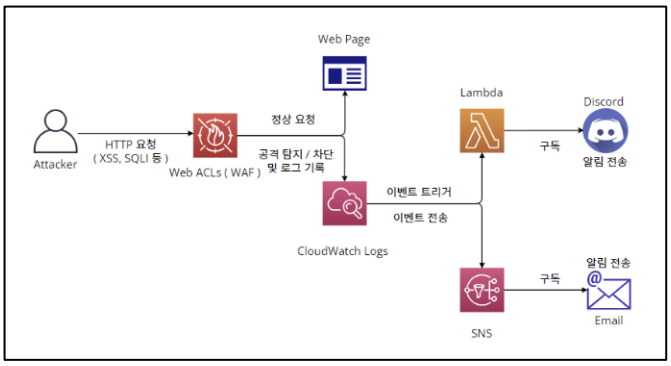


**그림 14. AWS WAF를 정책 관리 시나리오 및 모니터링 정책 구현 시나리오 워크플로우**

본 시나리오에서는 AWS 환경에서 웹 취약점 테스트용 애플리케이션(DVWA, Damn Vulnerable Web Application)을 배포하고, 이에 AWS WAF(Web Application Firewall)를 연동하여 웹 공격 시도를 탐지하고 차단하는 정책 적용 및 모니터링 체계를 구축하였다. 웹 서비스는 퍼블릭 서브넷에 위치한 EC2 인스턴스를 기반으로 구성되며 Application Load Balancer(ALB)를 통해 외부와 연결된다. 이때 ALB에 Web ACL을 연동하고, 다양한 탐지 및 차단 규칙을 적용하여 공격 시도를 실시간으로 식별하고 대응할 수 있도록 구성하였다. DVWA은 SQL Injection, XSS, 명령어 삽입 등의 다양한 취약점 테스트가 가능하며 이를 통해 WAF 정책의 효과를 실습할 수 있다. 웹 공격의 시도는 주로 HTTP 요청 헤더, URI, 쿼리스트링 등의 요소를 통해 발생하며, 이러한 요청을 탐지·차단하는 규칙을 구성함으로써 정책 기반의 방어 체계를 검증하였다.

그림 14는 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. 외부에서 공격자가 DVWA 환경에 대해 취약점을 이용한 요청을 시도하면 해당 요청은 ALB로 전달되기 전 WAF로 전달되어 검사한다. WAF(Web ACL)에는 사전에 정의된 사용자 지정 규칙 및 AWS Managed RuleSet이 적용되어 있어 해당 규칙에 부합하지 않은 요청은 차단되거나 기록된다. 차단 또는 탐지된 요청은 CloudWatch Logs에 JSON 로그 형태로 자동 저장된다. 로그에는 요청자의 IP 주소, 요청 경로, 헤더 정보, 차단 사유 및 트리거된 규칙명이 포함되며, 관리자는 이를 기반으로 공격 유형과 빈도를 파악할 수 있다. 이와 동시에 CloudWatch 로그에 연결되어 Discord Webhook을 포함한 Lambda 함수를 트리거하고 SNS에 전달하여 관리자에게 알림을 발송한다.

## 5. EC2에서 위험도 높은 악성행위 확인 시 네트워크 자동 격리

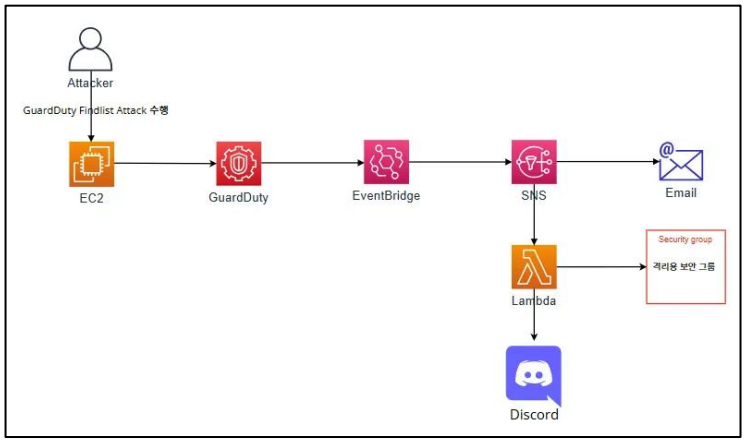


**그림 15. EC2에서 위험도 높은 악성행위 확인 시 네트워크 자동 격리**

EC2 인스턴스에서 다수의 비정상 외부 접속나 악성파일 실행 등 Severity level 7 이상의 위험 행위 발생 시 GuardDuty Findings에 해당 기록이 저장된다. 특정 탐지 유형 및 임계값 이상의 심각도로 분류된 이벤트 발생 시 해당 인스턴스를 자동으로 격리하는 아키텍처를 구현한다.

그림 15는 해당 시나리오의 워크플로우를 보여준다. 시나리오의 흐름은 다음과 같다. 공격자가 EC2 인스턴스를 탈취해 위험한 행위를 시도하면 GuardDuty Findings에 관련 기록이 저장된다. EventBridge는 이러한 이벤트를 감지하여, 지정한 탐지 유형과 임계값 이상의 심각도에 해당하는 경우 SNS로 이벤트를 전송한다. SNS는 구독 대상인 이메일과 Lambda 함수로 이벤트를 전달하며, Lambda 함수는 Discord로 알림을 전송해 관리자에게 위험 발생을 알린다. 동시에 위협이 감지된 EC2 인스턴스의 보안 그룹을 인바운드, 아웃바운드 트래픽이 모두 차단된 격리용 보안 그룹으로 변경하여 자동으로 격리 조치를 수행한다.

## 심화 탐지 및 대응 시나리오

**표 3. 심화 탐지 및 대응 시나리오 목록**

| 분류 | 심화 탐지 및 대응 시나리오 |
|---|---|
| 계정 인증 및 보안 | GuardDuty Malware Protection 악성 파일 탐지 및 대응 자동화 |
| 감사 및 역할 변경 | AWS WAF 공격 과탐 모니터링 및 자동화 차단 진행 |

표 3은 본 프로젝트에서 구현한 심화 탐지 및 대응 시나리오의 목록을 제시하며, 이는 기존 대응 시나리오보다 더 높은 수준의 자동화와 실무 연계성을 갖춘 고급 시나리오들로 구성되어 있다. 이 시나리오들은 기존의 수동적 보안 대응 절차를 자동화하는 데 중점을 두고 있으며, AWS Systems Manager, Step Functions 등과 같은 AWS의 고급 자동화 서비스를 적극적으로 활용하였다. 이러한 기술을 통해 단순한 경고 알림을 넘어, 실시간 위협 대응 조치까지 자동으로 수행될 수 있도록 설계되었다. 또한 본 프로젝트에서는 Sumo Logic과 같은 상용 SIEM(Security Information and Event Management) 도구를 통합하여, 실제 운영 환경에서 발생할 수 있는 보안 위협을 효과적으로 수집·분석하고 자동 대응하는 실전형 시나리오를 구현하였다. 학습자는 이와 같은 심화 시나리오를 직접 구성하고 테스트함으로써, 현업 환경에서 요구되는 수준의 클라우드 보안 자동화 설계 및 구현 역량을 실질적으로 체득할 수 있다.

### 1. GuardDuty Malware Protection 악성 파일 탐지 및 대응 자동화

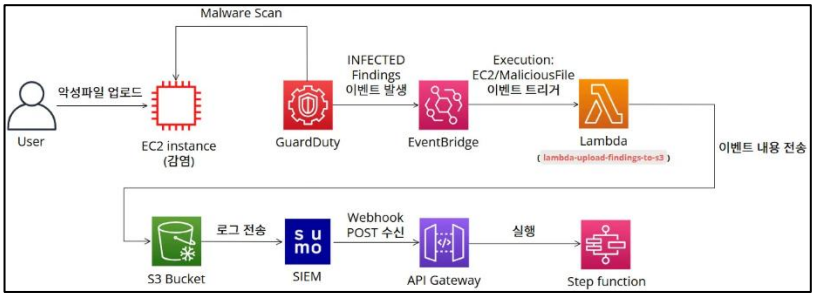


**그림 16. GuardDuty Malware Protection 악성 파일 탐지 및 대응 자동화 워크플로우**

해당 시나리오는 SIEM(Sumologic) 모니터링 과정에서 GuardDuty Malware Protection 결과 중 INFECTED로 확인된 인스턴스를 식별하고 API GW(GateWay)를 통해 Step function에 감염된 인스턴스의 정보를 보내, 지정된 절차에 맞게 침해사고 대응 아키텍처를 자동화하는 시나리오이다. 그림 16은 해당 시나리오의 워크플로우를 보여준다. 주요 흐름은 위와 같이 사용자를 통해 악성파일에 감염된 EC2 인스턴스가 존재하면 GuardDuty의 Malware Scan을 통해 해당 인스

턴스의 감염 여부를 파악하고 기록한다. 이때 EventBridge를 통해 GuardDuty에 기록된 이벤트 중 INFECTED(감염) 이벤트가 발생하면 이를 Lambda로 보내 SIEM(Sumologic)과 연동된 S3에 저장하고, SIEM(Sumologic)에서 해당 이벤트를 모니터링 할 수 있게 한다. SIEM(Sumologic)에서도 INFECTED(감염) 이벤트가 모니터링되면 감염된 EC2 인스턴스의 ID를 API GW(GateWay)를 통해 Step function에 보내, 자동으로 미리 설정한 Lambda를 실행시켜 대응을 진행한다.

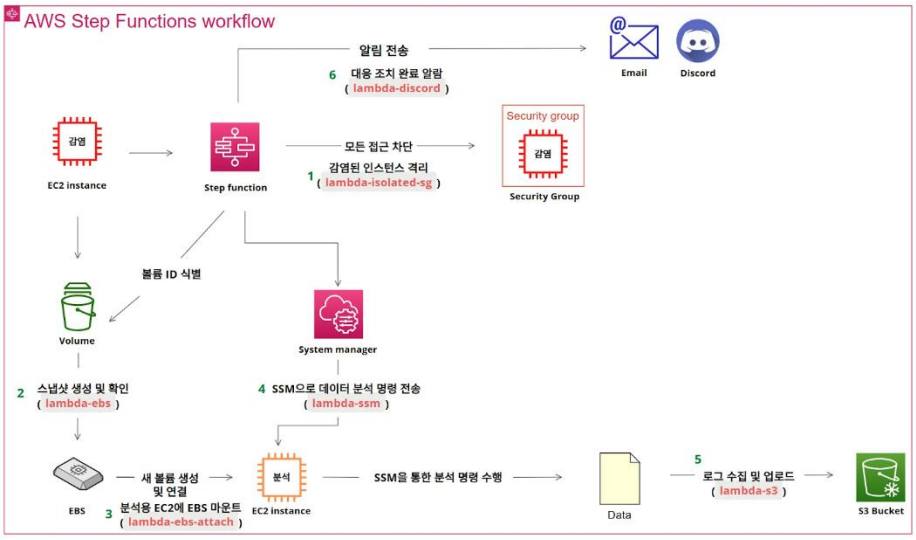


**그림 17. 시나리오에서 사용된 Step Functions의 워크플로우**

대응은 그림 17과 같이 6단계의 순서로 구성되어 있다. 우선 앞서 설명한 것처럼 API GW(GateWay)를 통해 SIEM(Sumologic)에서 전달받은 EC2 인스턴스의 ID를 통해 해당 인스턴스를 미리 생성해둔 인바운드 및 아웃 바운드가 차단된 보안그룹으로 변경하여 격리를 진행한다. 이후 격리된 인스턴스의 볼륨ID를 식별하고 해당 인스턴스의 스냅샷을 찍어 EBS 볼륨을 생성한다. 생성된 EBS 볼륨을 Private 네트워크에 위치한 분석용 EC2 인스턴스에 마운트한 뒤, NAT Gateway를 통해 SSM 명령을 전달하여 마운트된 EBS 볼륨의 데이터를 수집하고 S3 버킷에 전송·저장한다. 위 과정이 다 끝나면 사용자의 Email과 Discord로 "대응 조치가 완료되었다"는 알람을 전송한다.

## 2. AWS WAF 공격 과탐 모니터링 및 자동화 차단 진행

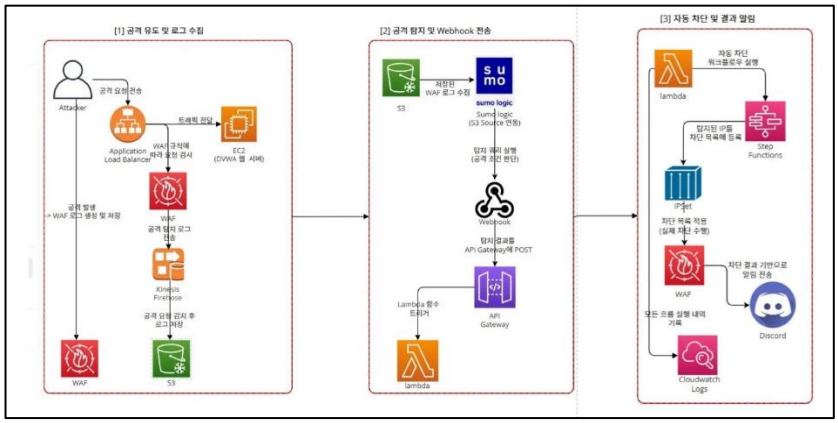


**그림 18. AWS WAF 공격 과탐 모니터링 및 자동화 차단 진행**

해당 시나리오는 AWS WAF에서 발생한 단기간 내 과다 탐지(과탐) 이벤트를 SIEM(Sumologic)을 통해 모니터링하고, 일정 조건 이상 발생 시 공격 출발지 IP를 자동 차단하는 시나리오이다. 그림 18은 해당 시나리오의 워크플로우를 보여준다. 시나리오의 주요 흐름은 다음과 같다. 공격자가 공격 요청을 전송하면 ALB(Application Load Balancer)가 해당 요청을 EC2 인스턴스에 전달하는데, 이때 WAF가 이를 탐지하고 기록 및 공격 검사를 수행한다.

공격 로그로 판별되면 Kinesis Firehose를 통해 SIEM(Sumologic)과 연동된 S3에 해당 탐지 로그를 저장한다. 이후 SIEM(Sumo Logic)에서도 탐지 쿼리를 통해 과탐 이벤트가 모니터링 되면 API GW(GateWay)를 통해 Step Function을 실행해주는 lambda로 공격자의 IP를 보낸다. 해당 lambda를 통해 Step Function을 실행하여 WAF의 차단 IP Set에 앞서 전달받은 공격자의 IP를 추가해준 뒤, 적용시켜 해당 공격자를 차단한다. 또한 공격자의 IP를 통해 AbuseIPDB에 등록된 IP 정보를 확인하여 해당 IP 정보를 추출한다. 구체적으로는 해당 IP로부터 Country, ISP/Hosting Info, Abuse Score를 추출하여 Email 및 Discord로 알람을 보내 사용자가 이를 확인할 수 있도록 하였다.

# 프로젝트 결론

## 프로젝트 요약 및 성과

### 1. 워크북 작성

**그림 19. 프로젝트 결과물(워크북)을 확인할 수 있는 QR 코드**

본 프로젝트의 핵심 산출물 중 하나는 클라우드 보안 입문자를 위한 워크북이다. 실무에서 자주 발생하는 침해사고 시나리오를 기반으로 단계 별 실습이 가능하도록 구성된 워크북은 복잡한 클라우드 인프라 환경에 대한 이해를 돕고, 초보자도 실제 보안 프로세스를 따라가며 학습할 수 있도록 설계되었다. 워크북은 탐지 → 알림 → 대응의 흐름에 따라 구성되며 각 단계는 AWS 서비스, SIEM 연동, 자동화된 대응까지 전 과정을 다룬다. 사용자는 이를 통해 클라우드 보안 아키텍처를 설계하고, 상황에 따라 보안 정책을 확장하거나 시나리오를 응용하는 경험을 할 수 있다. 이처럼 실습 기반의 교육 자료는 기존의 이론 중심 보안 교육과 차별화되며 실무 적용 가능성을 고려한 역량 중심 학습 방식으로 작성하였다.

### 2. 클라우드 역량 검증

프로젝트 기간 동안 팀원들은 실습 중심의 학습을 통해 클라우드 보안에 대한 실질적인 역량을 강화하였다. 특히, AWS 기반의 인프라 설계, 보안 탐지 구성, 자동화된 대응 흐름을 구현하는 과정에서 Terraform을 활용한 IaC 환경 구성, Sumo Logic을 통한 SIEM 연동, Lambda, Step Functions, SSM 기반의 자동화 대응 시나리오 개발 등 실무와 밀접한 기술들을 직접 설계하고 운용하였다. 그 결과, 팀원 전원이 AWS Cloud Practitioner 시험에 응시하였으며, 이 중 5명이 자격증을 취득하였다. 이는 본 프로젝트가 단순한 결과물 제작에 그치지 않고, 팀원들의 역량을 강화했다는 지표로 볼 수 있다.

## 프로젝트 개선 방안

프로젝트 수행 과정에서 자동화 흐름의 복잡성, 실시간 알림 지연 등 몇 가지 도전 과제를 확인하였다. 향후에는 다양한 유형의 침해 시나리오를 기준으로 대응 단계를 추가하고, 상황에 따라 격리 등을 유연하게 적용할 수 있도록 시나리오를 확장해 나갈 계획이다. 또한

워크북은 GitBook 기반으로 오픈소스로 공개하고, Terraform IaC 코드와 함께 제공하여 실제 환경에서 쉽게 적용할 수 있도록 하며, 외부 사용자의 피드백을 반영해 시나리오 구성과 대응 로직을 지속적으로 개선할 예정이다.

## 마무리 및 소감

본 프로젝트는 단순히 보안 기능을 구현하는 데 그치지 않고, 입문자 관점에서 클라우드 보안 시나리오를 설계하고 학습할 수 있는 환경을 구축했다는 점에서 큰 의미가 있다. 특히, '보안 전문가가 클라우드 환경을 잘 모르면 누구도 책임을 명확히 질 수 없다'는 문제의식을 바탕으로 시작된 이 프로젝트는 책임 주체의 명확성과 자동화된 보안 대응 환경의 필요성을 다시 한번 인식하게 해주었다. 협업과 반복 실습을 통해 실무 감각을 익힐 수 있었으며, 나아가 누구나 접근 가능할 수 있는 보안 학습 환경 조성을 위한 첫걸음을 내디뎠다는 점에서 본 프로젝트의 의의는 매우 크다.

## 참고 문헌


1. https://docs.aws.amazon.com/ko_kr/
2. https://docs.aws.amazon.com/ko_kr/guardduty/latest/ug/guardduty_finding-types-ec2.html
3. https://docs.aws.amazon.com/whitepapers/latest/aws-overview/introduction.html
4. https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/getting-viewing-bill.html
5. https://developer.hashicorp.com/terraform/tutorials
6. https://arxiv.org/abs/2205.10676
7. https://help.sumologic.com/
8. https://it.chosun.com/news/articleView.html?idxno=2023092134387
9. https://www.etnews.com/20231221000342