모듈 6 - 공동 책임 모델, IAM, 규정 준수, 보안 서비스

AWS 공동 책임 모델

AWS는 사용자 환경의 일부분을 책임지고 고객은 다른 부분을 책임진다는 뜻입니다.

공동 책임 모델은 고객 책임과 AWS 책임으로 나뉩니다.

고객

- 고객 데이터
- 플랫폼, IAM, 애플리케이션
- 운영 체제, 네트워크/방화벽 구성
- 사용자 측 데이터 암호화, 서버 측 데이터 암호화, 네트워킹 트래픽 보호
- EC2 에서 실행할 운영 체제 선택, **구성 및 패치**
- **보안 그룹을 구성하는 단계**
- **사용자 계정 관리**

AWS

- 소프트웨어: 컴퓨팅, 스토리지, 데이터베이스, 네트워킹
- 하드웨어: 리전, 가용 영역, 엣지 로케이션
- 물리적인 인프라: 데이터센터의 물리적 보안, SW/HW 인프라, 네트워크 인프라, 가상화 인프라

AWS Identity and Access Management(IAM)

: AWS 서비스와 리소스에 대한 액세스를 주는 서비스입니다.

요구 사항에 따라 아래의 기능을 조합하여 권한을 구성할 수 있습니다

- **IAM 사용자, 그룹 및 역할**
- **IAM 정책**
- **다중 인증(MFA)**

권한을 부여하거나 거부하려면 IAM 정책이라고 하는 요소를 IAM 사용자라고 하는 것에 연결해야 합니다.

AWS 계정 루트 사용자

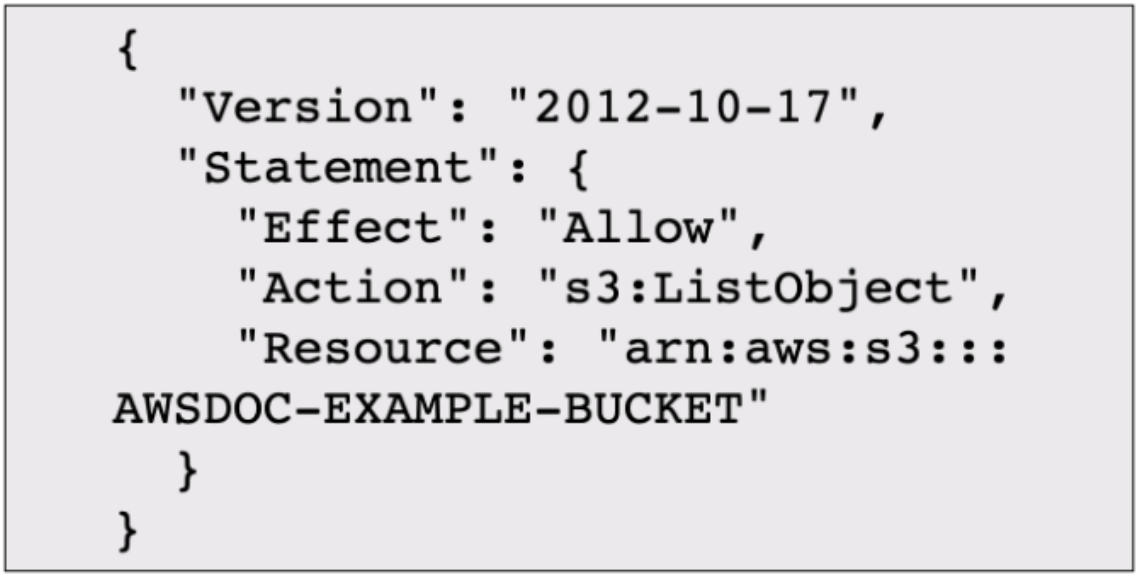
AWS 계정을 처음 만들면 루트 사용자라고 하는 자격 증명으로 시작합니다. 이 사용자는 모든 서비스 및 리소스에 대한 전체 액세스 권한을 가집니다.

IAM 사용자

사용자가 AWS에서 생성하는 자격증입니다.

IAM 사용자가 EC2 시작, S3 버킷 생성 등 특정 작업을 수행할 수 있도록 허용하려면 IAM 사용자에게 필요한 권한을 부여해야 합니다.

IAM 정책



위 사진은 IAM ID 가 AWSDOC-EXAMPLE-BUCKETDLS 인 S3 버킷의 객체에 액세스할 수 있는 권한을 허용하고 있음을 보여주고 있습니다.

IAM 그룹

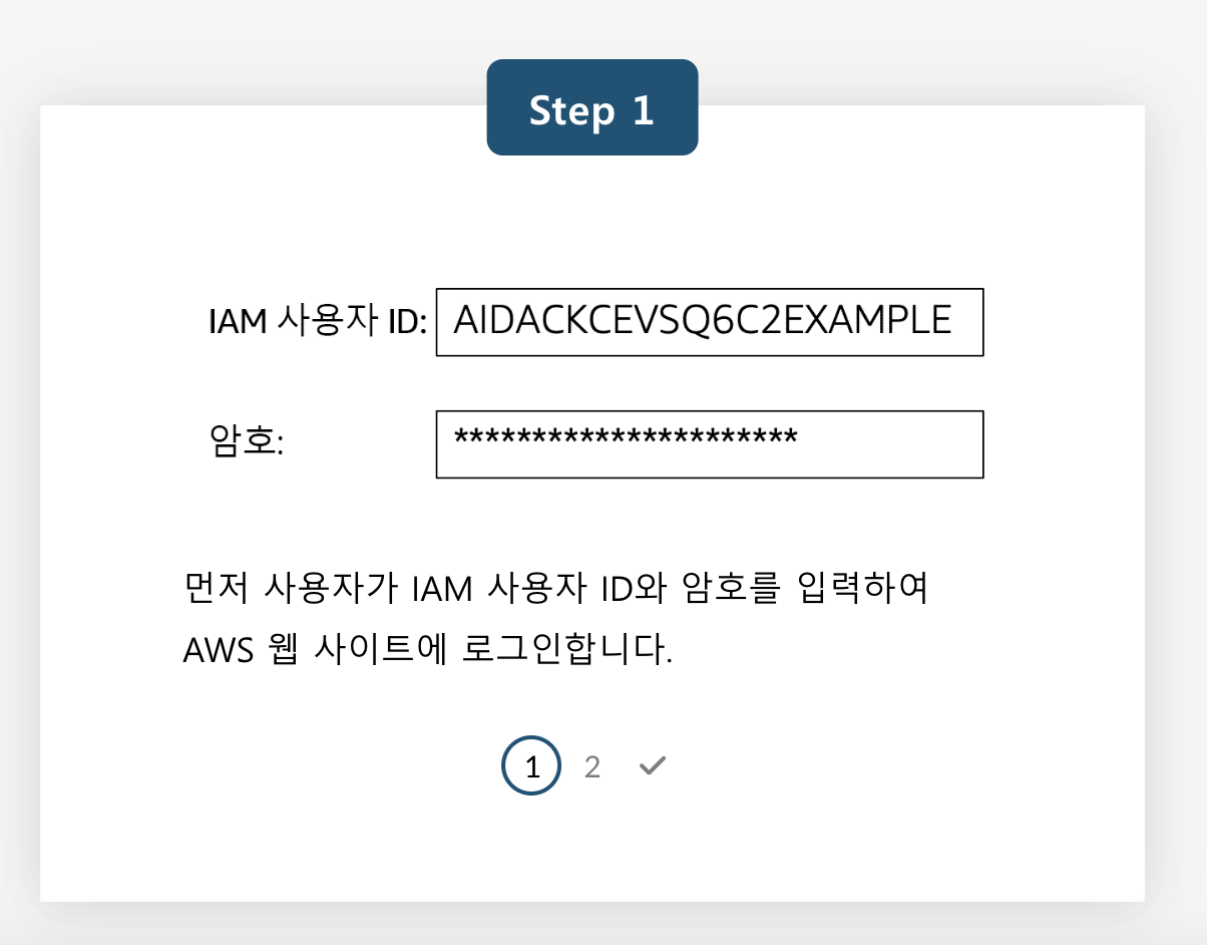
엔지니어 그룹, 사이언티스트 그룹 등 각 그룹에 대한 지정된 권한을 부여할 수 있습니다.

IAM 역할

임시로 권한에 액세스하기 위해 수임할 수 있는 자격 증명입니다.

다중 인증(MFA)

이중 로그인이라고 생각하면 됩니다.



ip/pw 입력하는 것 뿐만 아니라 인증토큰을 통해 로그인하는 방법입니다.

AWS Organizations

회사에 aws 계정이 여러개가 있다면 중앙 위치에서 여러 계정을 통합하고 관리할 수 있는 기능입니다.

조직을 생성하면 Organizations 가 조직의 모든 계정에 대한 상위 컨테이너 루트를 자동으로 생성합니다.

서비스 제어 정책(SCP)을 사용하여 조직의 계정에 대한 권한을 중앙에서 제어할 수 있습니다.

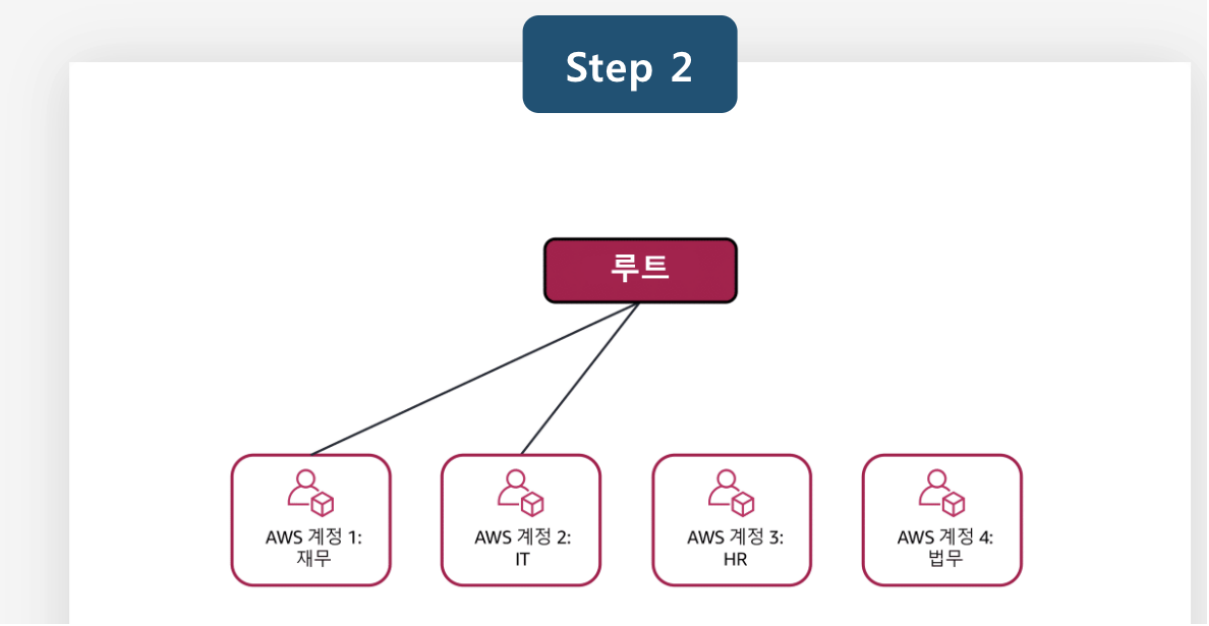
SCP

조직 루트, 개별 멤버 계정 또는 OU에 적용할 수 있습니다.

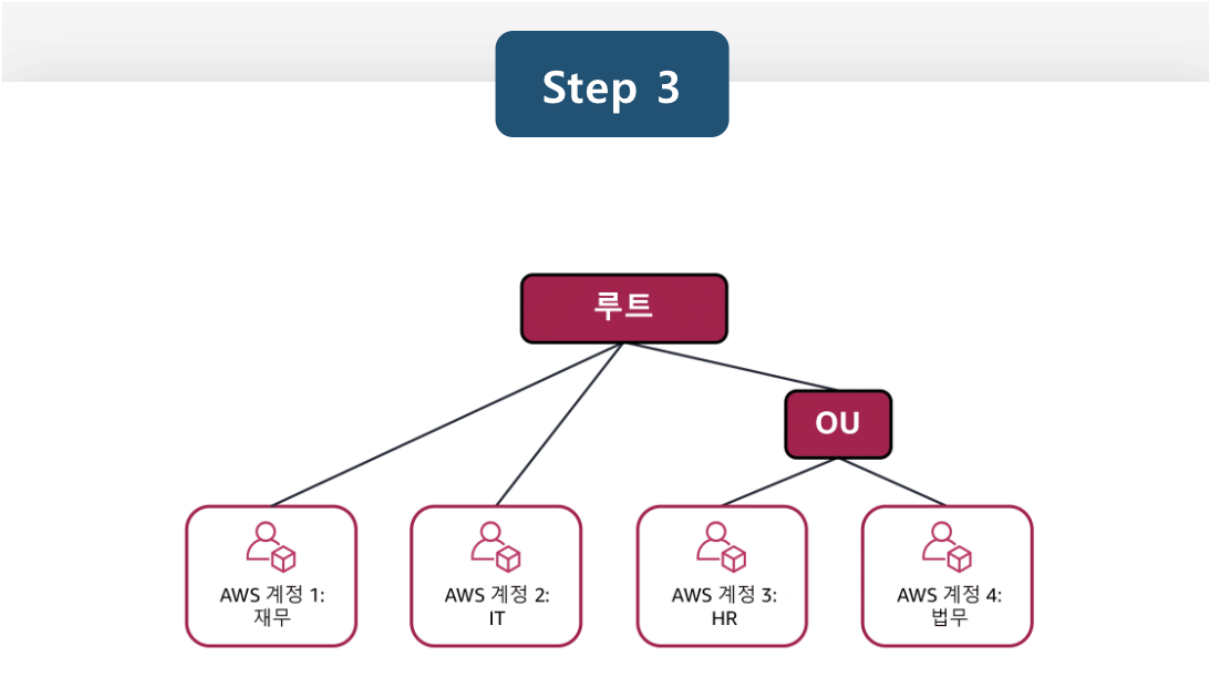
조직 단위(OU)

계정을 조직 단위로 그룹화하여 비슷한 비즈니스 또는 보안 요구 사항이 있는 계정을 손쉽게 관리할 수 있습니다.

재무, IT, HR, 법무 부서에 별도의 계정이 있다고 가정해보면 중앙 위치에서 관리할 수 있도록 조직을 만들면 루트가 설정됩니다.



재무 부서와 IT 부서는 서비스 및 리소스에 대한 액세스가 비슷하지 않다고 가정하면 위 사진과 같이 연결되고



HR과 법무 부서는 동일한 서비스 및 리소스에 액세스해야 한다고 가정하면 조직단위(OU)에 함께 배치할 수 있습니다.

AWS Artifact

Artifact는 AWS 보안 및 규정 준수 보고서 및 온라인 계약에 대한 온디맨드 액세스를 제공하는 서비스 **입니다.**

즉, 표준을 충족하였는지 확인해주는 서비스입니다.

아래 두 가지 섹션으로 구성되는데

AWS Artifact 계약

회사에서 AWS 서비스 전체에서 특정 유형의 정보를 사용하기 위해 AWS와 계약을 한다고 하면 이 서비스를 통해 수행할 수 있습니다.

AWS Artifact 보고서

개발 팀원 중 한명이 애플리케이션을 빌드하는 중 특정 규제 표준을 준수하기 위한 책임 정보가 필요하다면 이 서비스를 통해 조언해줄 수 있습니다.

고객 컴플라이언스 센터

AWS 규정 준수에 대해 자세히 알아볼 수 있는 리소스가 포함되어 있습니다.

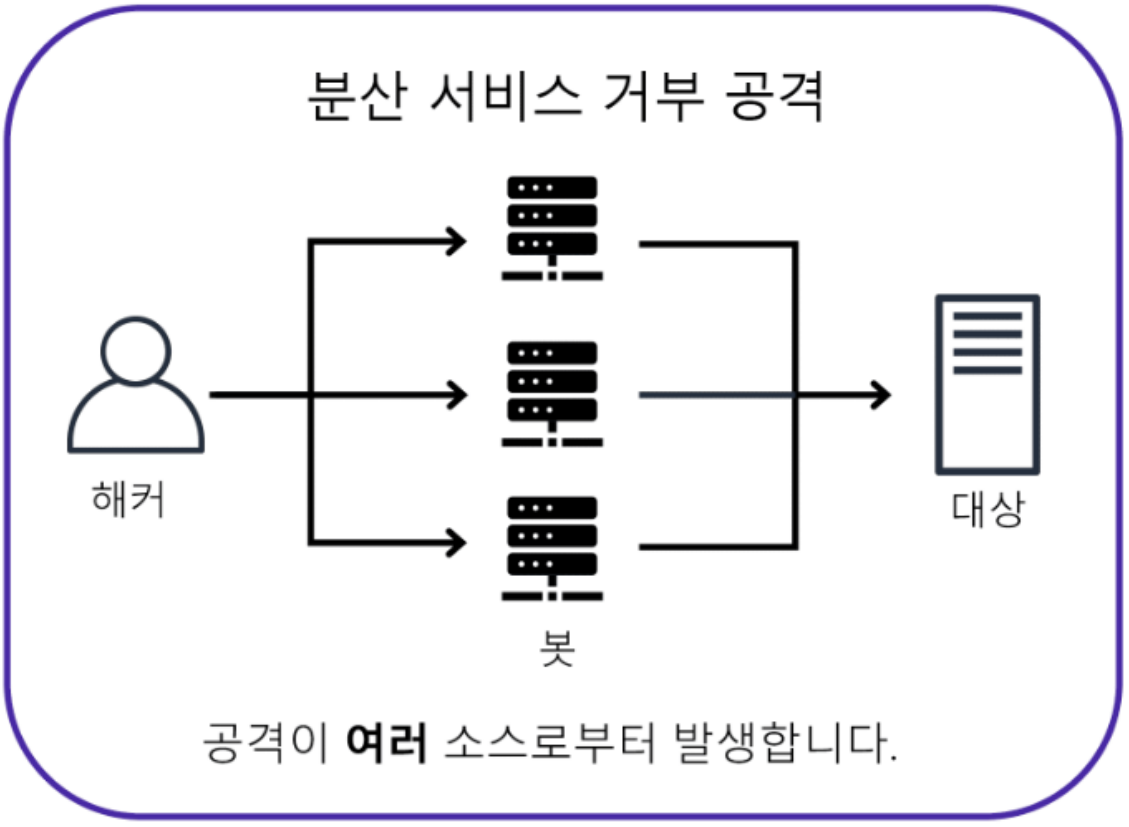
- 규정 준수에 대한 질문, 답변
- 규정 준수 개요
- 거버넌스 및 감사 과제 사례

AWS Shield

DDos 공격으로부터 보호하는 서비스입니다.

분산 서비스 거부 공격(DDos)

여러 소스를 사용하여 웹 사이트 또는 애플리케이션을 사용할 수 없게 만드는 공격입니다.



쉴드의 기능은 아래와 같은데

AWS Shield Standard

모든 AWS 고객을 자동으로 보호하는 무료 서비스입니다.

AWS Shield Advanced

상세한 공격 진단 및 정교한 DDos 공격을 탐지하는 기능을 제공하는 유료 서비스입니다.

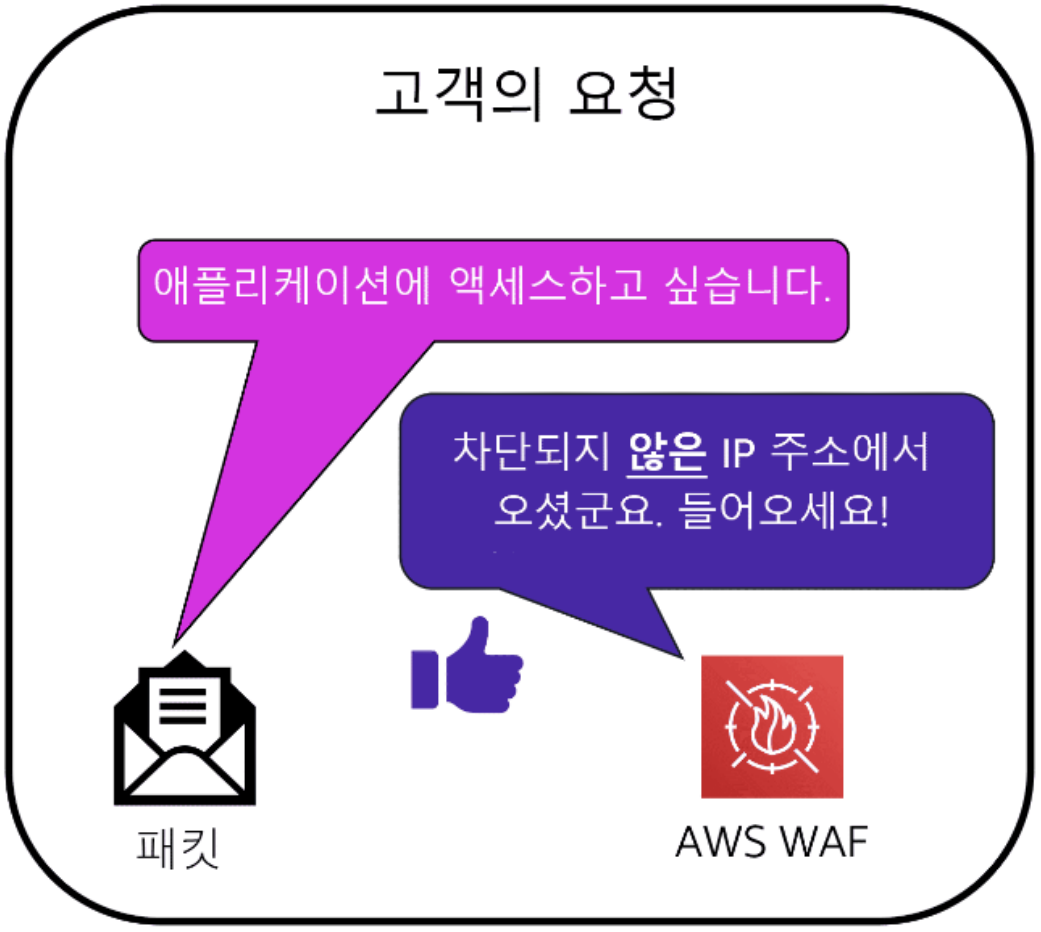
사용자 지정 규칙을 작성하여 AWS WAF와 통합할 수 있습니다.

추가 보안 서비스

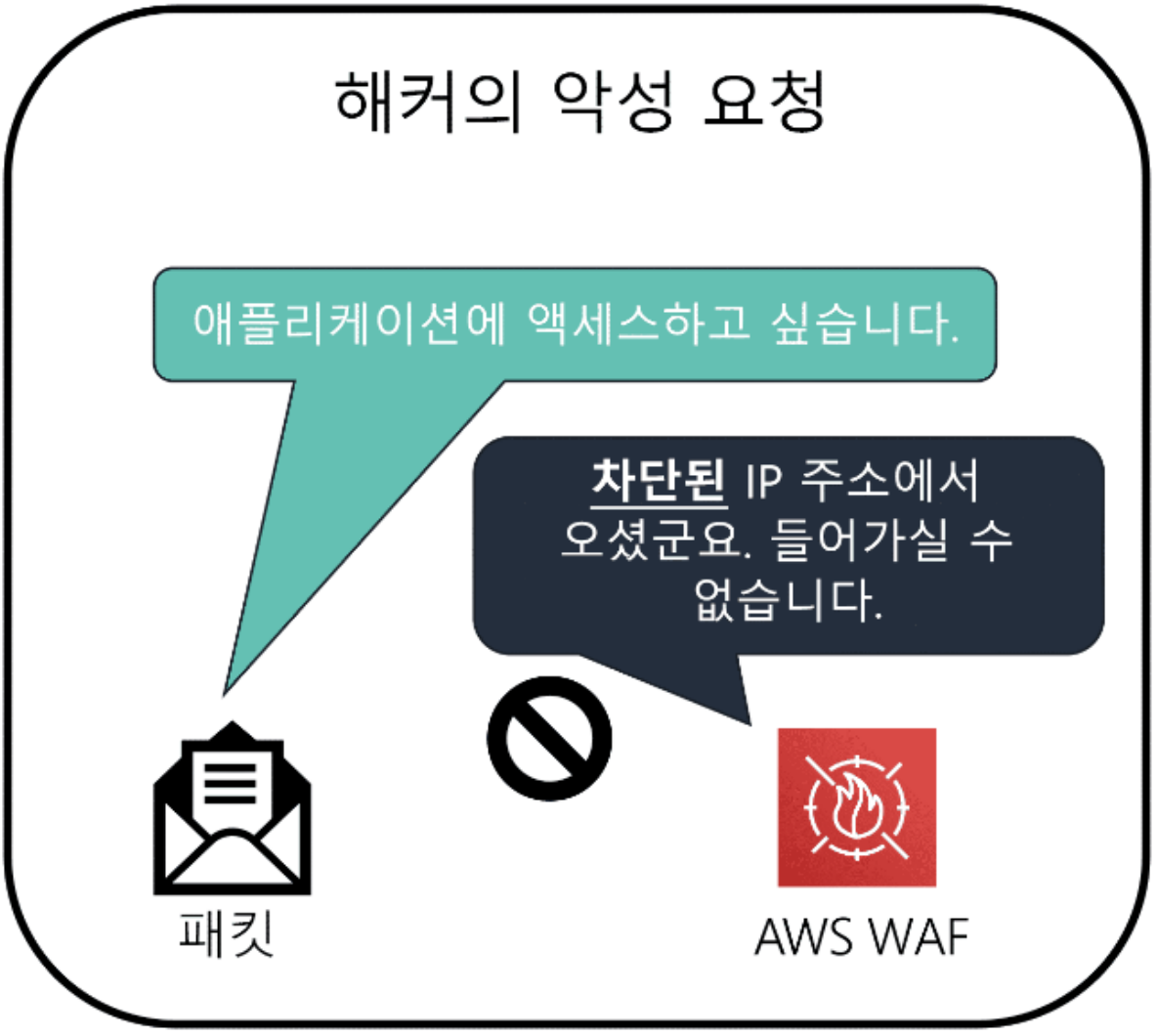
AWS WAF

웹 애플리케이션으로 들어오는 네트워크 요청을 모니터링할 수 있는 웹 애플리케이션 방화벽입니다.

Amazon CloudFront 및 Application Load Balancer와 함께 작동하며 리소스를 보호하기 위해 웹 액세스 제어 목록(ACL)을 사용합니다.



웹 ACL에서 지정한 차단 IP 주소가 접근하려고 하면 WAF가 액세스를 거부합니다.



AWS Key Management Service(AWS KMS)

암호화 키를 사용하여 암호화 작업을 수행할 수 있습니다.

> 💡 암호화 키: 데이터 잠금(암호화) 및 잠금 해제(암호 해독)에 사용되는 임의의 숫자 문자열

이 서비스를 사용하여 암호화 키를 생성, 관리, 사용할 수 있습니다.

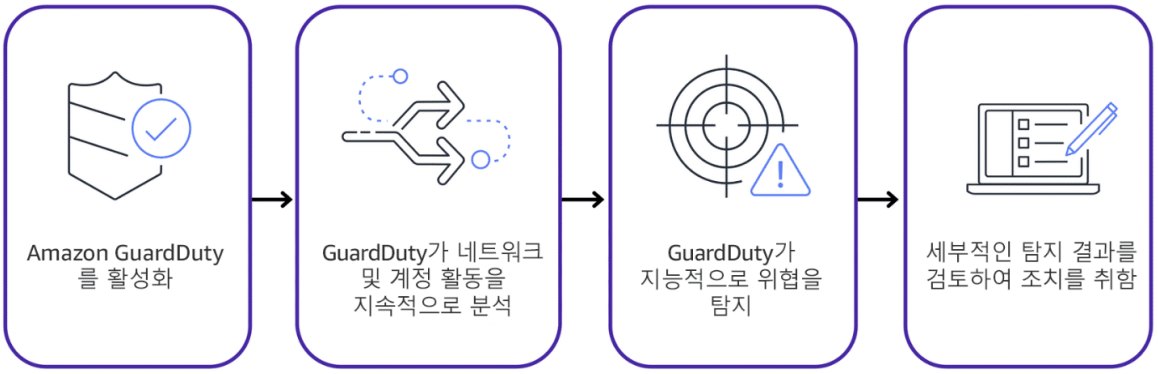
Amazon Inspector

자동화된 보안 평가를 실행하여 애플리케이션의 보안 및 규정 준수를 개선할 수 있는 서비스입니다.

예를 들어 개발자가 개발해야할 여러 애플리케이션을 수동 평가하기엔 시간이 많이 걸리니 이 서비스를 이용하여 자동 보안 평가를 수행하는 것입니다.

Amazon GuardDuty

인프라 및 리소스에 대한 지능형 위협 탐지 기능을 제공하는 서비스입니다.



이 서비스를 활성화하면 네트워크 및 계정 활동을 모니터링하여 추가 보안 소프트웨어를 배포하거나 관리할 필요가 없습니다.

탐지 결과를 검토할 수 있고, 결과에 대한 응답을 자동으로 문제 해결 단계를 수행할 수 이도록 Lambda 함수를 구성할 수 있습니다.

끝