

AWSSOME DAY
ONLINE CONFERENCE

강의 4: 보안

장기웅
테크니컬 트레이너
AWS





인프라 보호

AWS는 보안을 가장 중요하게 생각합니다



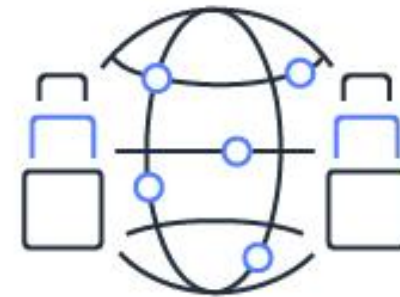
보안을 고려한
설계



지속적
모니터링



고도의
자동화

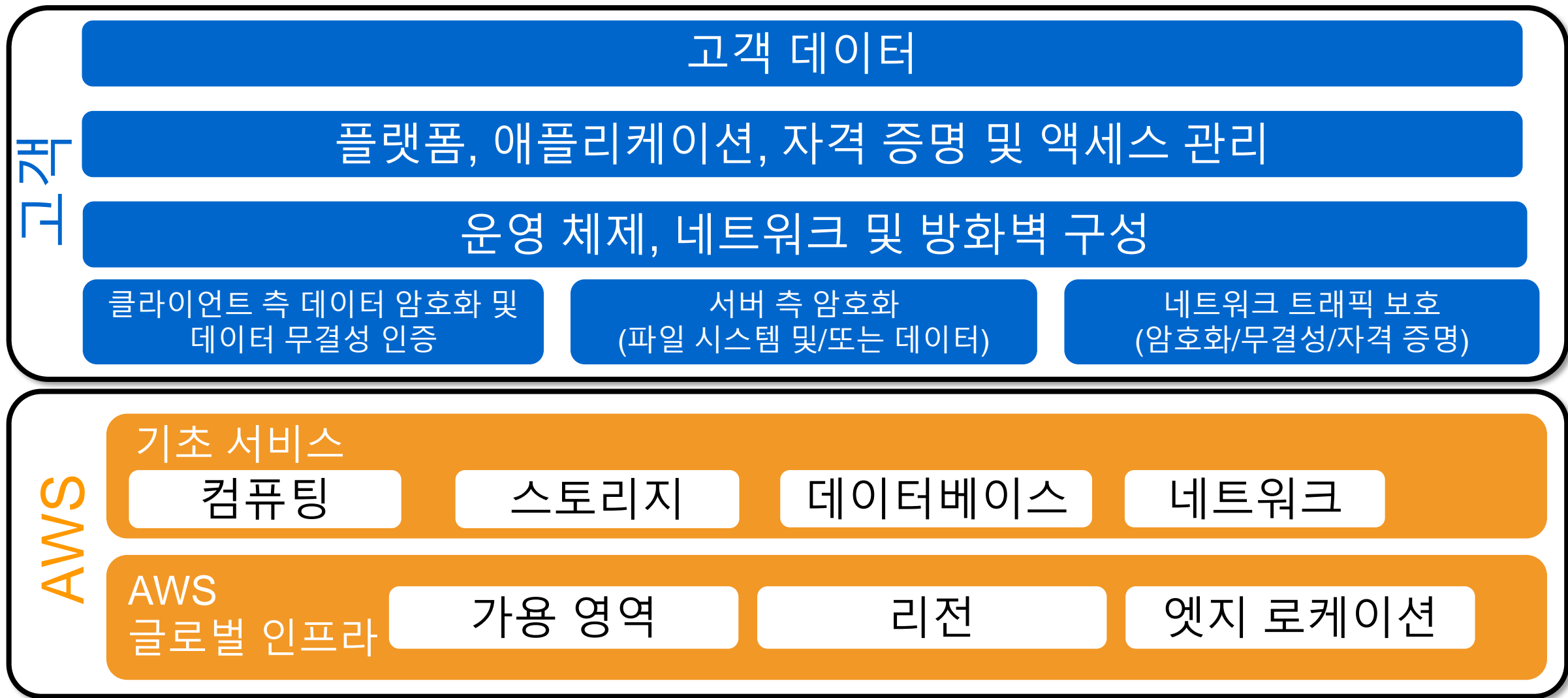


높은
가용성



엄격한
인증

AWS 책임 공유 모델



클라우드의 보안

호스트, 네트워크, 소프트웨어, 시설
AWS 글로벌 인프라 보호는 최고 우선 순위
타사 감사 보고서 제공

AWS

기초 서비스

컴퓨팅

스토리지

데이터베이스

네트워크

AWS
글로벌 인프라

가용 영역

리전

엣지 로케이션

클라우드에서의 보안

고객

고객 데이터

플랫폼, 애플리케이션, 자격 증명 및 액세스 관리

운영 체제, 네트워크 및 방화벽 구성

클라이언트 측 데이터 암호화 및
데이터 무결성 인증

서버 측 암호화
(파일 시스템 및/또는 데이터)

네트워크 트래픽 보호
(암호화/무결성/자격 증명)

고려 사항

- 무엇을 저장해야 하는가
- 어떤 AWS 서비스를 사용해야 하는가
- 어느 리전에 저장해야 하는가
- 콘텐츠 형식과 구조는 어떻게 되는가
- 누가 액세스할 수 있는가

토론: 누가 무엇을 책임집니까?

비관리형 서비스

Amazon EC2

Amazon EBS

관리형 서비스

- Amazon RDS
- Amazon S3
- Amazon DynamoDB

운영

- 게스트 OS 패치
- 데이터베이스 패치
- 방화벽 구성
- 재해 복구
- 사용자 데이터

보안, 자격 증명 및 규정 준수 제품

AWS Artifact

AWS Certificate Manager

Amazon Cloud Directory

AWS CloudHSM

Amazon Cognito

AWS Directory Service

AWS Firewall Manager

Amazon GuardDuty

**AWS Identity and Access
Management**

Amazon Inspector

AWS Key Management Service

Amazon Macie

AWS Organizations

AWS Shield

AWS Secrets Manager

AWS Single Sign-On

AWS WAF



인증 및 권한 관리

AWS Identity and Access Management (IAM)

AWS 리소스에 대한 액세스를 안전하게 제어



IAM 사용자

AWS와 상호 작용하는 사람 또는 애플리케이션



그룹

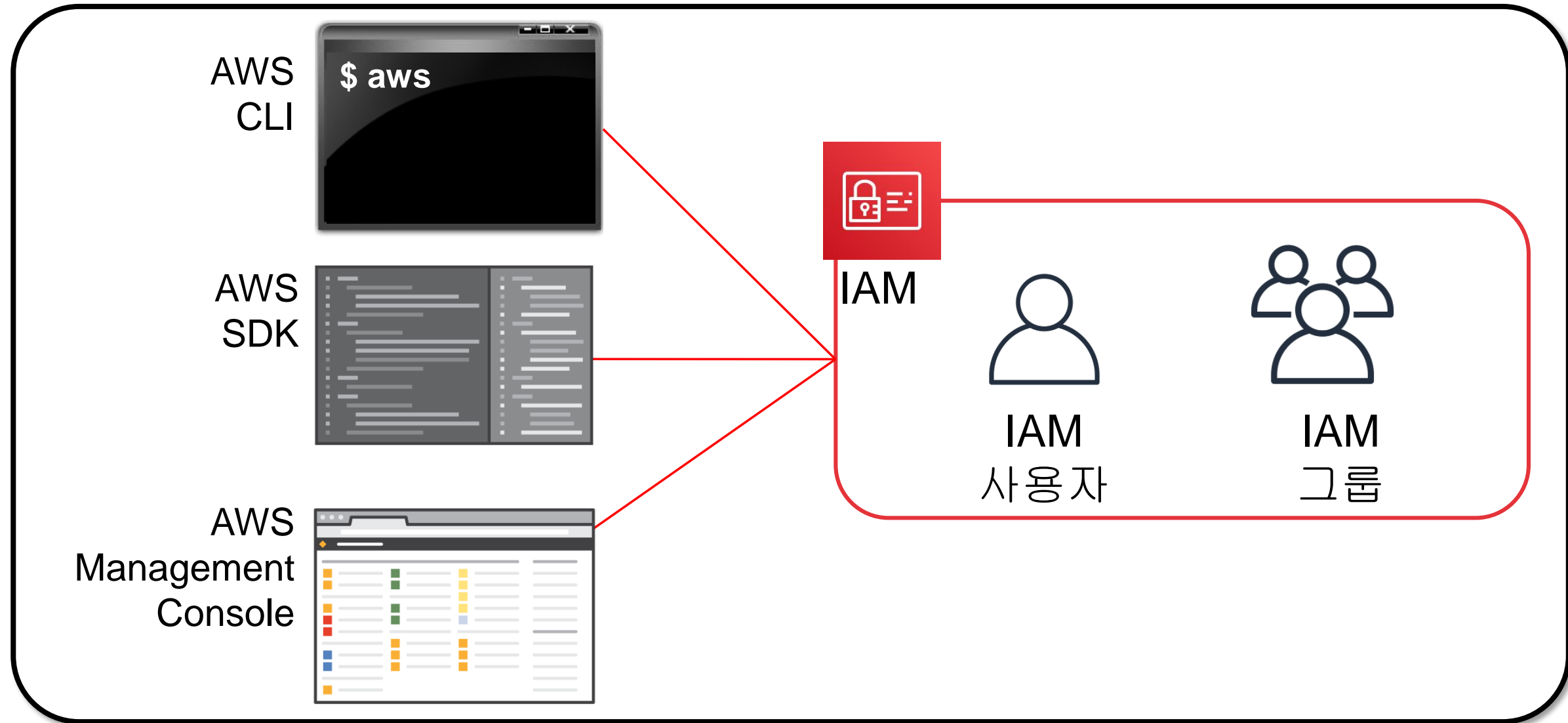
동일한 권한을 가진 사용자 모음



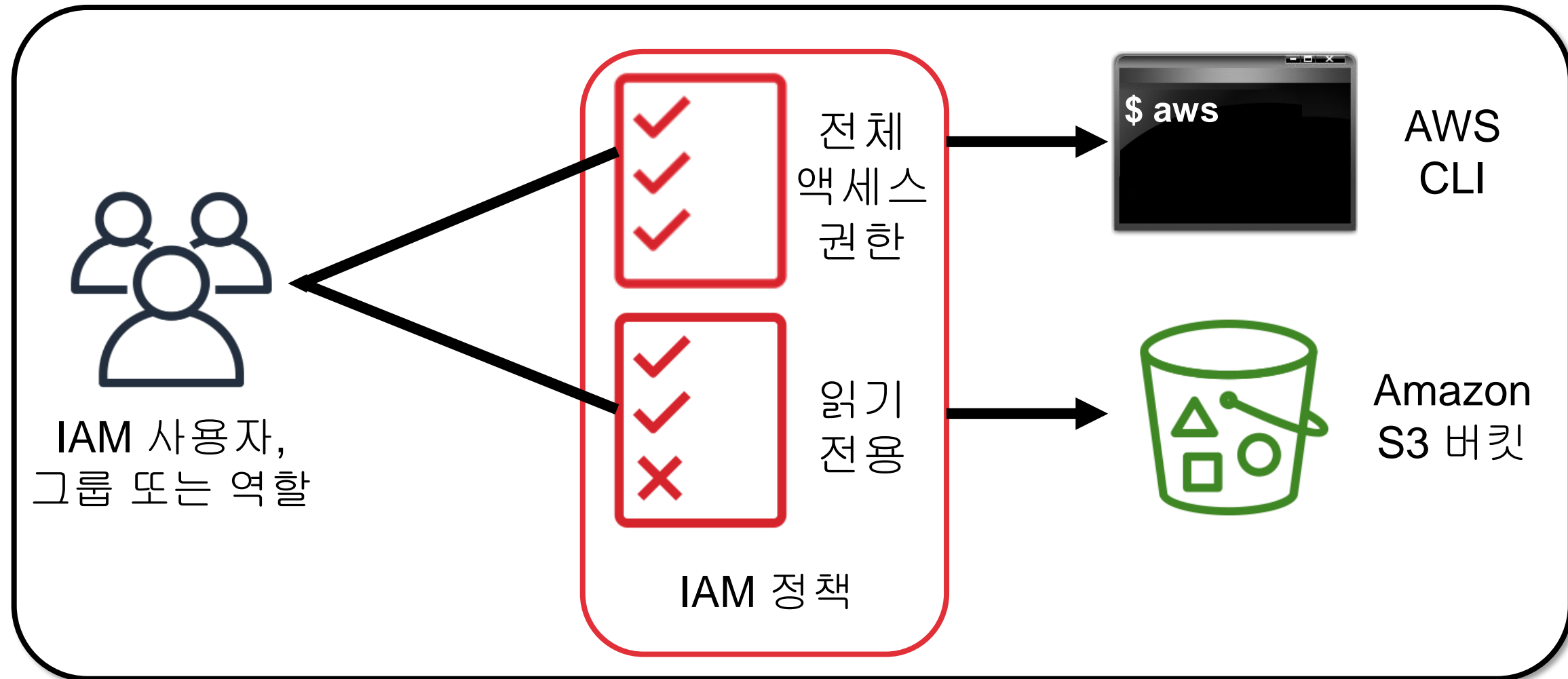
역할

엔터티가 맡을 수 있는 임시 권한

인증: 사용자 확인



권한: 할 수 있는 작업



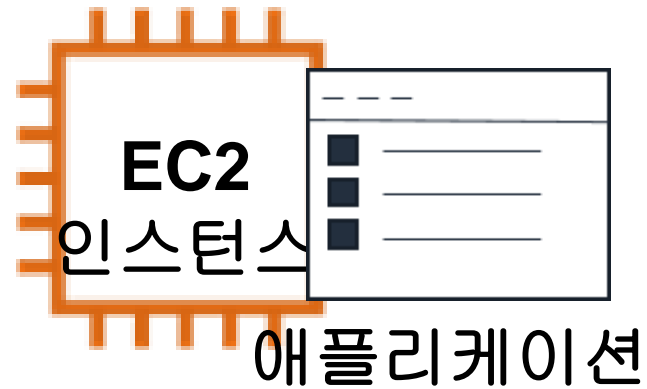
IAM 역할



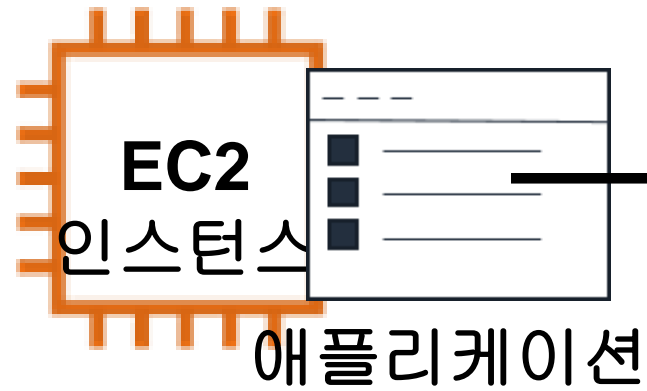
IAM 역할

- IAM 사용자, 애플리케이션, 서비스는 IAM 역할을 맡을 수 있음
- 역할은 권한에 IAM 정책 사용

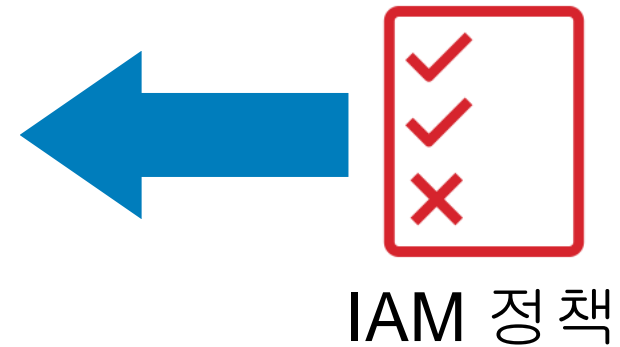
역할을 사용하여 임시 보안 자격 증명 부여



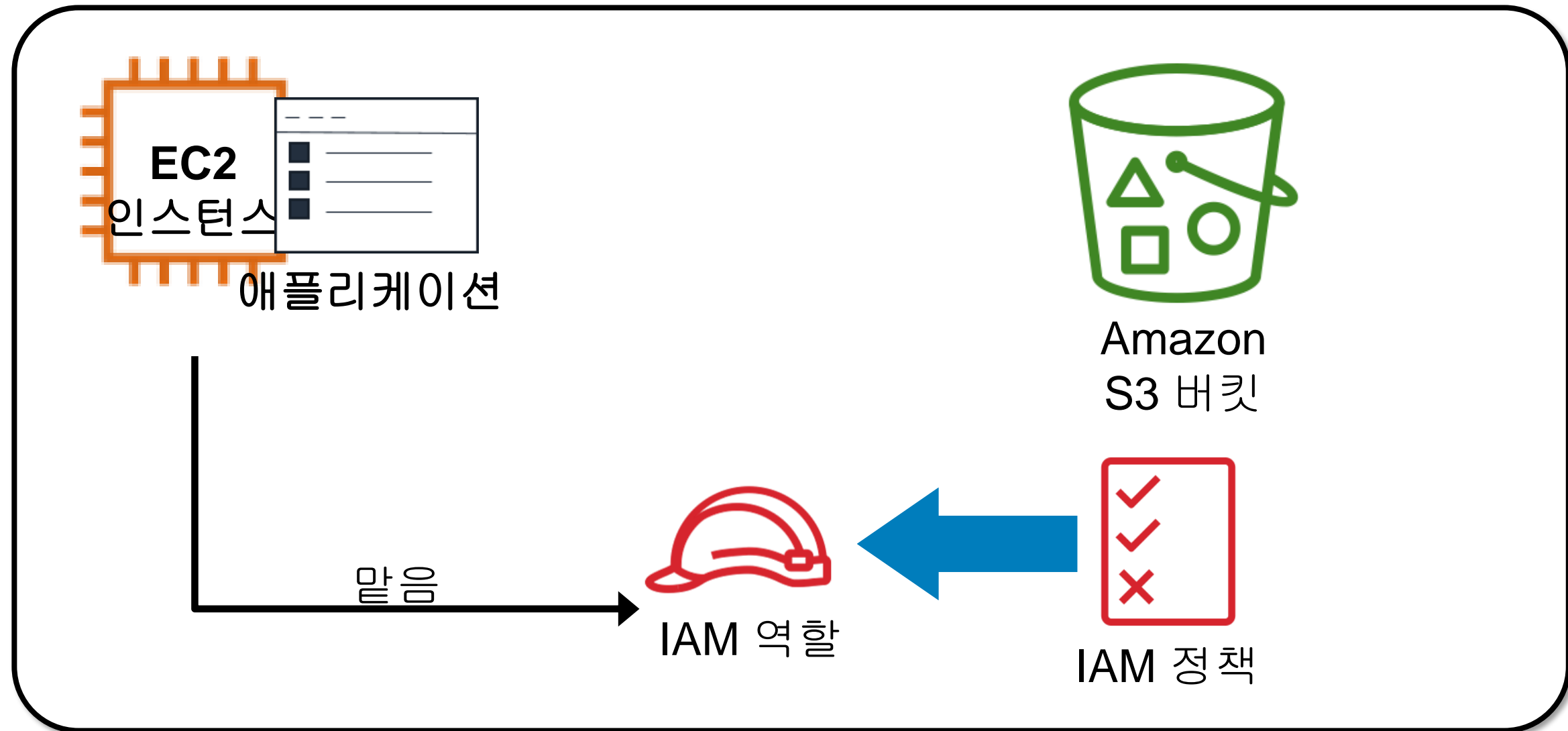
역할을 사용하여 임시 보안 자격 증명 부여



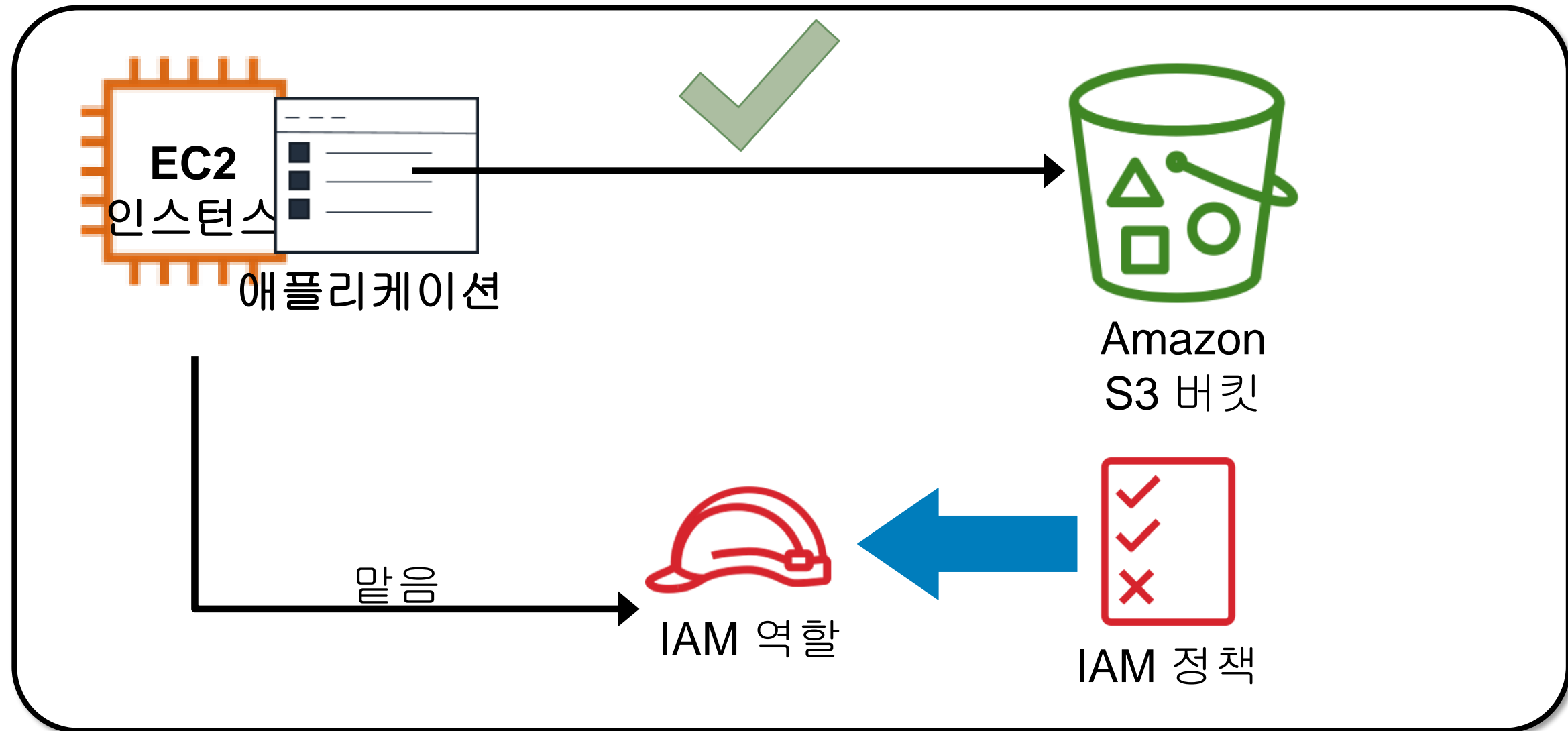
역할을 사용하여 임시 보안 자격 증명 부여



역할을 사용하여 임시 보안 자격 증명 부여



역할을 사용하여 임시 보안 자격 증명 부여



AWS 계정 루트 사용자

계정 루트 사용자는 모든 AWS 서비스에 대한 완전한 액세스 권한 가짐

Create an AWS account

Email address
newuser@example.com

Password
.....

Confirm password
.....

AWS account name ⓘ
examplecorp

Continue

권장 사항



루트 사용자 액세스 키를 삭제합니다



IAM 사용자를 생성합니다



관리자 액세스 권한을 부여합니다



IAM 자격 증명을 사용하여 AWS와 상호 작용합니다



MFA 활성화

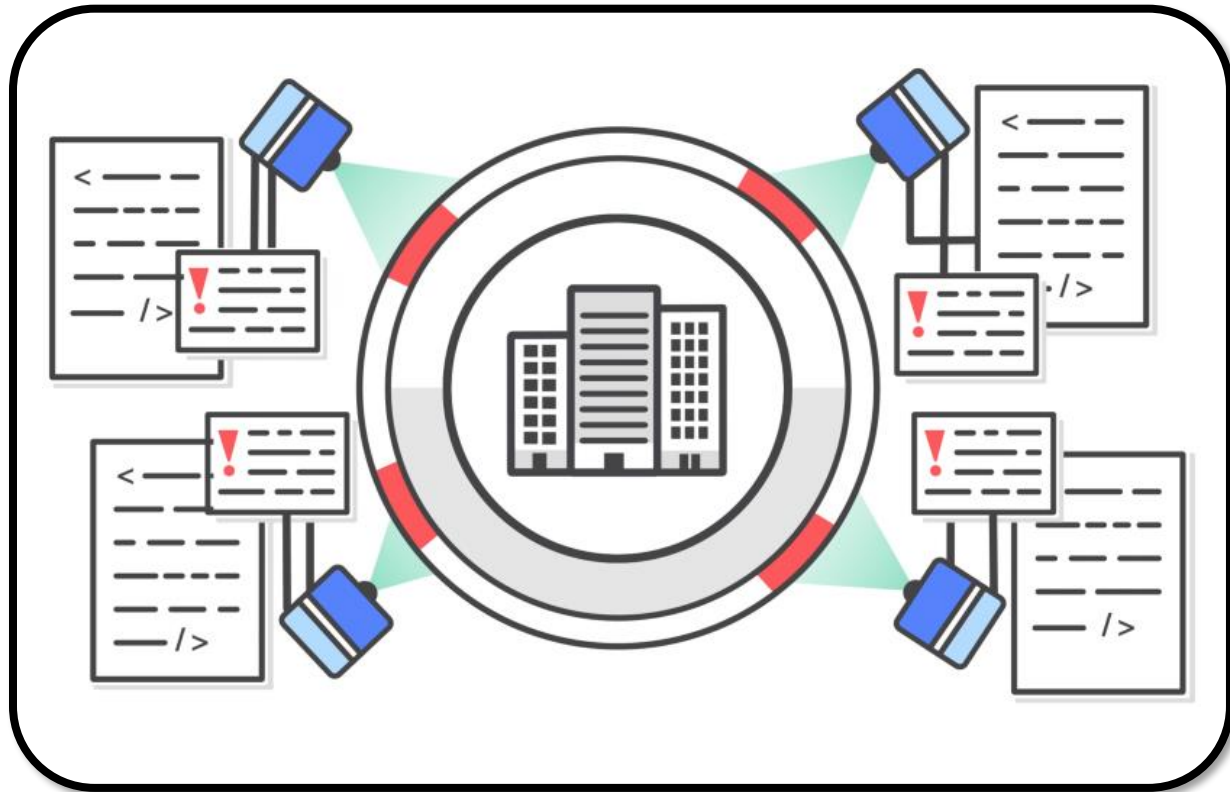
모범 사례

- AWS 계정 루트 사용자의 액세스 키를 삭제합니다
- Multi-Factor Authentication(MFA)을 활성화합니다
- IAM 사용자에게 필요한 권한만 부여합니다
- 애플리케이션에 역할을 사용합니다
- 주기적으로 자격 증명을 교체합니다
- 불필요한 사용자와 자격 증명을 제거합니다
- AWS 계정 내 활동을 모니터링합니다



보안 및 규정 준수 평가

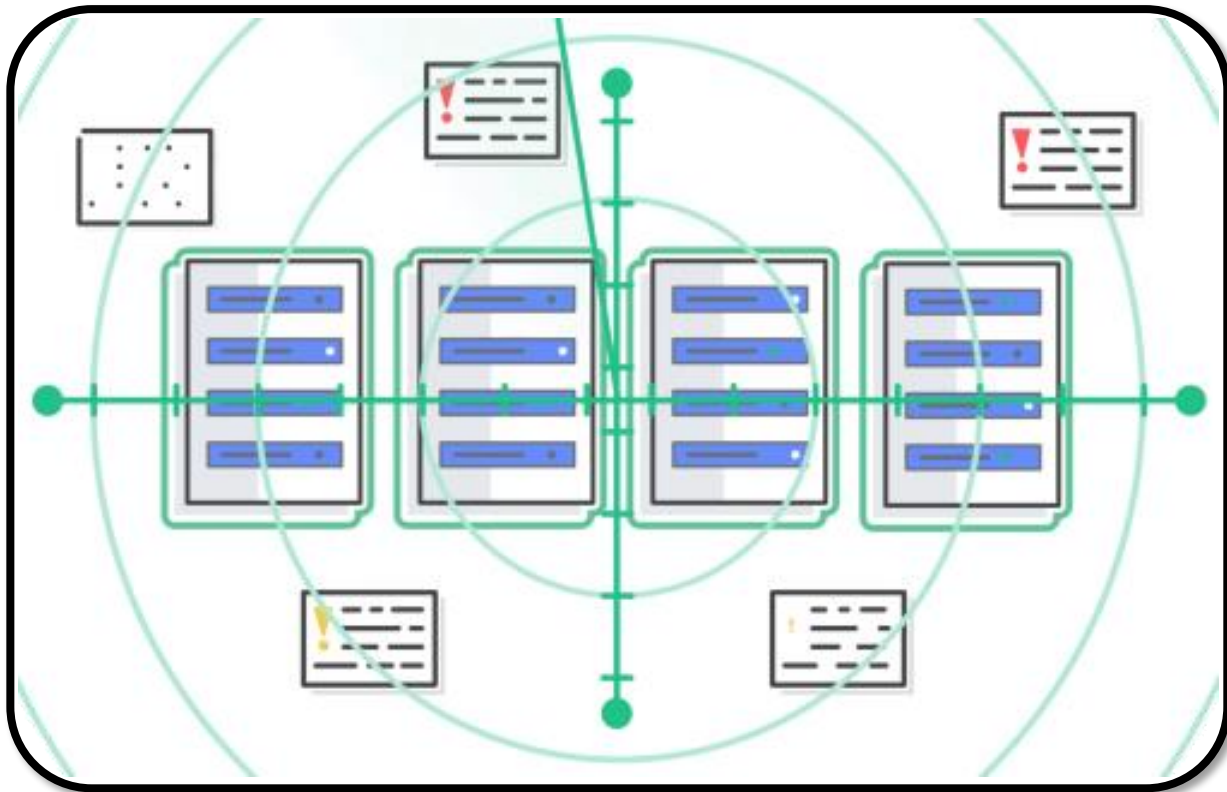
위협 평가의 어려움



- 높은 비용
- 복잡성
- 많은 시간 소요
- IT 변경 사항 추적이 어려움



Amazon Inspector란 무엇입니까?

자동화된 보안 평가 서비스



- 애플리케이션 취약성 평가
- 상세한 보안 평가 결과 목록 생성
- 보안 모범 사례 활용

Amazon Inspector 결과

Amazon Inspector - Findings					
Inspector findings are potential security issues discovered during Inspector's assessment of the specified application. Learn more.					
Add/Edit attributes			 		
<input type="text" value="Filter"/>			« < Viewing 1-10 of 24		
<input type="checkbox"/>	Severity	Application	Assessment	Rule package	Finding
<input type="checkbox"/>	▶ High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	Instance i-aac4c46f is config
<input type="checkbox"/>	▶ High ⓘ	Customer Processing	Comprehensive-Assessment	Common Vulnerabilities and Ex...	Instance i-aac4c46f is vulne
<input type="checkbox"/>	▶ High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	No password complexity me
<input type="checkbox"/>	▶ Informational ⓘ	Customer Processing	Comprehensive-Assessment	Operating System Security Best...	No potential security issues
<input type="checkbox"/>	▶ Informational ⓘ	Customer Processing	Comprehensive-Assessment	Network Security Best Practices	No potential security issues

해결 권장 사항

Finding for application - Customer Processing

Application name Customer Processing

Assessment name Comprehensive-Assessment

Rule package Authentication Best Practices

Finding Instance i-aac4c46f is configured to allow users to log in with root credentials over SSH. This increases the likelihood of a successful brute-force attack.

Severity High ⓘ

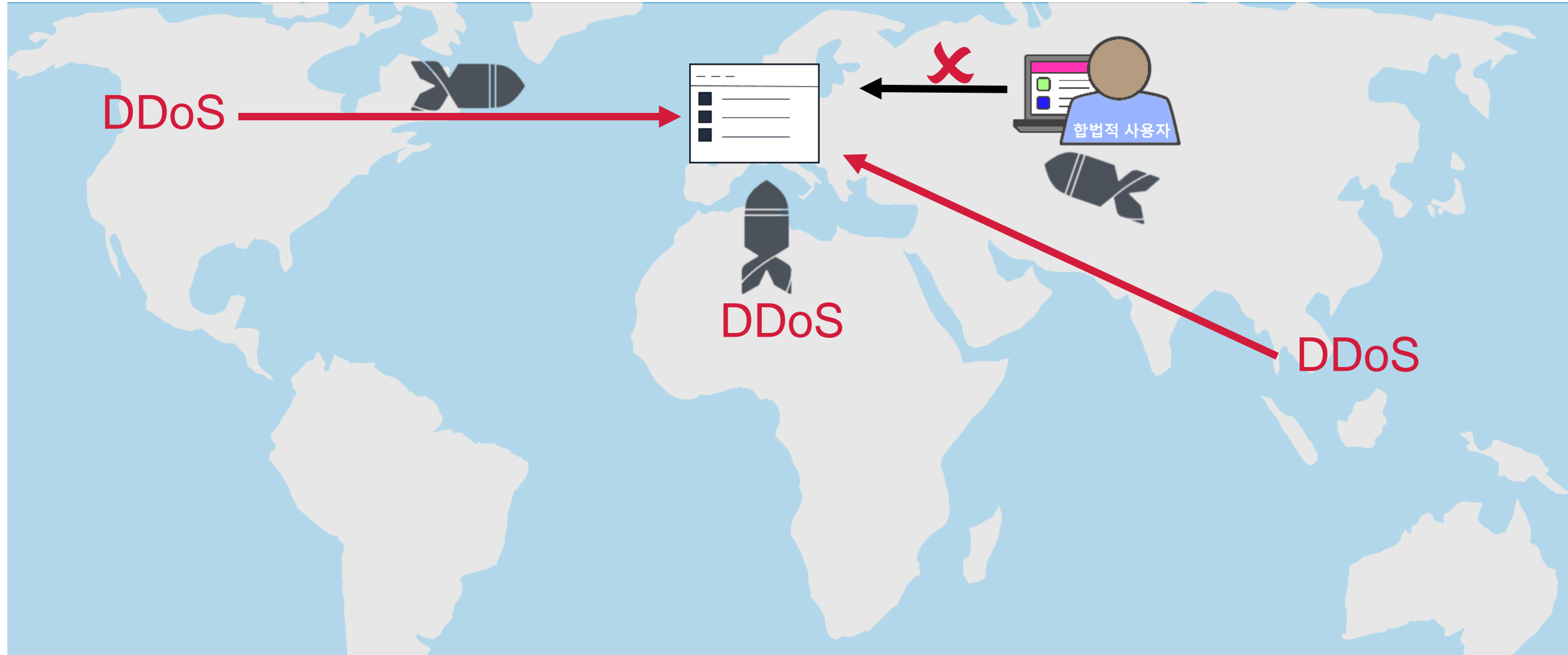
Description This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root.

Recommendation It is recommended that you configure your EC2 instance to prevent root logins over SSH. Instead, log in as a non-root user and use **sudo** to escalate.



DDoS (Distributed Denial of Service) 공격으로부터 인프라 보호

DDoS란 무엇입니까?



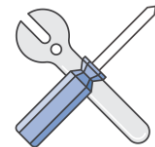
DDoS 완화의 어려움



복잡성



제한된 대역폭



아키텍처 재설계 필요



수동



성능 저하

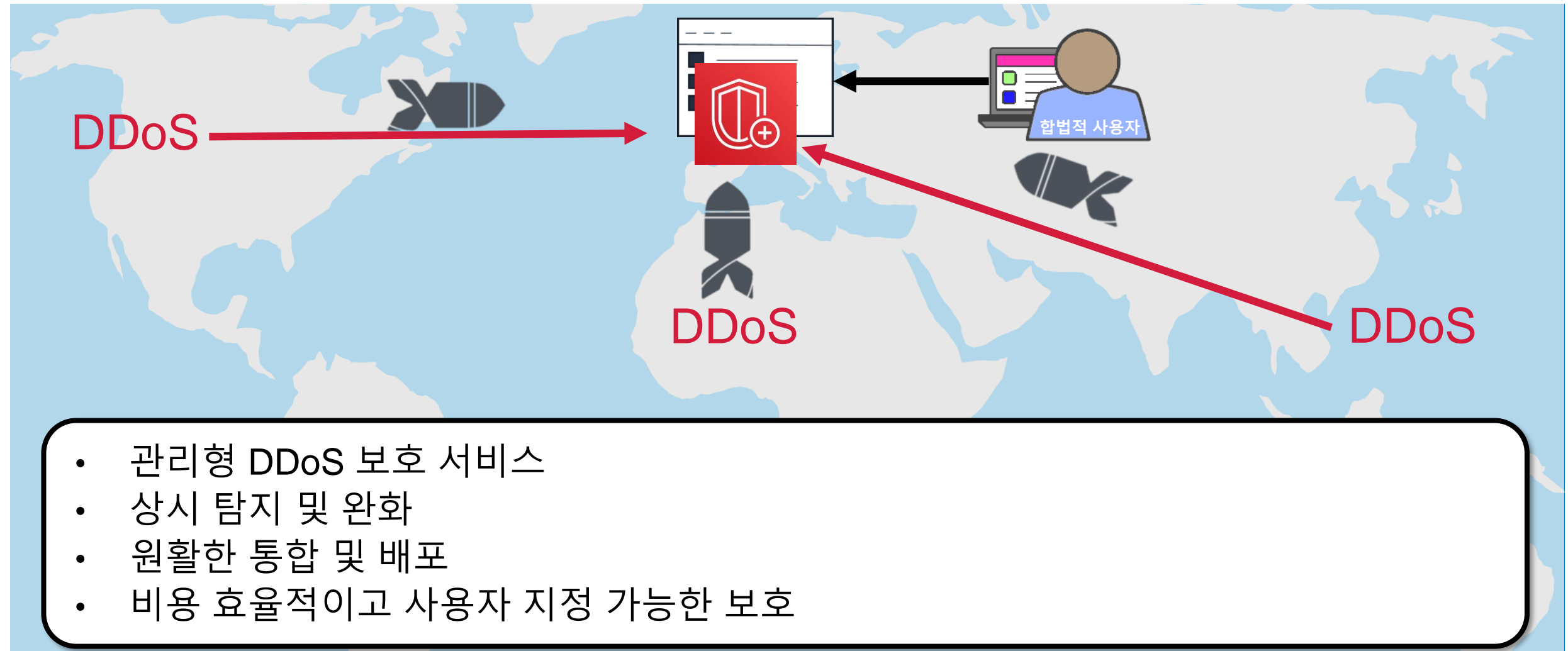


많은 시간 소요



높은 비용

AWS Shield란 무엇입니까?



AWS Shield Standard와 AWS Shield Advanced

AWS Shield Standard (추가 비용 없이 자동 활성화)

신속한 탐지
인라인 공격 완화

AWS Shield Advanced

(선택 사항)

- 향상된 탐지
- 고급 공격 완화
- 가시성 및 공격 알림
- DDoS 비용 보호
- 전문적 지원



AWS 보안 규정 준수

보증 프로그램

전 세계



미국



유럽



아시아 태평양



AWS가 고객의 규정 준수를 지원하는 방법

정보 공유

- 산업 인증
- 보안 및 제어 사례
- NDA에 따른 규정 준수 보고서

보증 프로그램

- 인증/인가
- 법률, 규정 및 개인 정보
- 준수/프레임워크

고객의 책임

인증은 고객의 책임입니다.

검토 – 설계 – 식별 – 확인

강의 4 종료

지식을 테스트해보세요

퀴즈

Q1 공동 책임 모델에서는 클라우드 보안의 어떤 측면에 대해 AWS가 책임이 있습니까?

- A. 클라우드의 보안
- B. 클라우드에 대한 보안
- C. 클라우드를 위한 보안
- D. 클라우드에서의 보안

퀴즈

Q1 공동 책임 모델에서는 클라우드 보안의 어떤 측면에 대해 AWS가 책임이 있습니까?

- A. 클라우드의 보안
- B. 클라우드에 대한 보안
- C. 클라우드를 위한 보안
- D. 클라우드에서의 보안

A가 정답입니다.

퀴즈

Q2 웹 애플리케이션이 AWS 서비스를 사용하려면 AWS 자격 증명과 권한 부여가 필요합니다. 어떤 IAM 엔티티를 사용해야 합니까?

- A. 사용자
- B. 그룹
- C. 역할
- D. MFA

퀴즈

Q2 웹 애플리케이션이 AWS 서비스를 사용하려면 AWS 자격 증명과 권한 부여가 필요합니다. 어떤 IAM 엔티티를 사용해야 할까요?

- A. 사용자
- B. 그룹
- C. 역할
- D. MFA

C가 정답입니다.

퀴즈

Q3 다음 중 보안 모범 사례는 무엇입니까? (모두 선택)

- A. 루트 사용자 액세스 키를 삭제합니다.
- B. 모든 사용자에게 동일한 암호를 사용합니다.
- C. 애플리케이션에 역할을 사용합니다.
- D. 코드에 보안 암호를 포함합니다.
- E. Multi-Factor Authentication(MFA)을 활성화합니다.

퀴즈

Q3 다음 중 보안 모범 사례는 무엇입니까? (모두 선택)

- A. 루트 사용자 액세스 키를 삭제합니다.
- B. 모든 사용자에게 동일한 암호를 사용합니다.
- C. 애플리케이션에 역할을 사용합니다.
- D. 코드에 보안 암호를 포함합니다.
- E. Multi-Factor Authentication(MFA)을 활성화합니다.

A, C, E가 정답입니다.

감사합니다!