aws partner network | service delivery 솔트웨어(주) saltware

AWS 아키텍처 보안 모범 사례

장 환, SA, Saltware

2024. 7. 8.

목차

보안 디자인 원칙

강력한 Identity 관리 기반을 구현	**최소 권한 부여 원칙**을 구현하고, AWS 리소스 간의 상호 작용에 대한 인가 과정에서 적절하게 **직무 분리** 통제 적용
책임 추적성 확보	모든 변경 사항과 작업들을 **실시간 모니터링/로깅/감사**하고, 자동 대응 환경 구성
모든 계층에 보안 적용	단일 보안 계층이 아닌, **모든 계층**(Edge, VPC, ELB, EC2, OS 및 애플리케이션)에 필요한 보안 기능 적용 및 통제
보안 모범 사례 자동 적용	검증된 보안기준이 선 적용되어 버전관리되는 **템플릿을 기반**으로, 자동으로 안전하게 스케일링 환경을 지원할 수 있도록 구현
전송 중 및 유휴 시 데이터 보호	데이터를 민감도 레벨로 **분류**하고, 필요시 암호화, 토큰화 및 액세스 제어 적용
데이터로부터 사용자를 최대한 격리	관리자의 실수 방지를 위해, **자동 처리** 프로세스를 적용하고 데이터 직접 액세스 또는 수동 처리 과정을 최소화
보안 이벤트에 대한 충분한 대비	보안 사고 **대응 시뮬레이션**을 준비/실행하고, 자동화된 도구를 사용하여 탐지, 조사 및 복구 속도 향상

5가지 보안 영역

1. 아이덴티티 & 엑세스 관리
2. 탐지 통제
3. 인프라 보호
4. 데이터 보호
5. 침해 사고 대응

보안 디자인 원칙 ➔ 5 가지 보안 영역

- 강력한 Identity 관리 기반을 구현 → 1. 아이덴티티 & 엑세스 관리
- 책임 추적성 확보 → 2. 탐지 통제
- 모든 계층에 보안 적용 → 3. 인프라 보호
- 보안 모범 사례 자동 적용 → 3. 인프라 보호
- 전송 중 및 유휴 시 데이터 보호 → 4. 데이터 보호
- 데이터로부터 사용자를 최대한 격리 → 4. 데이터 보호
- 보안 이벤트에 대한 충분한 대비 → 5. 침해 사고 대응

AWS 클라우드 보안을 위해 무엇부터 할까요?

- **IAM**
- **탐지** 통제 활성화
- 보안 사고에 대한 **사전 대비**
- **자동화** 고려 및 적용

aws partner network | service delivery 솔트웨어(주) saltware

아이덴티티 & 엑세스 관리(IAM)

아이덴티티 & 엑세스 관리

SEC 1. 워크로드의 **자격증명**과 **인증**을 어떻게 관리하는가?

SEC 2. 서비스에 대한 **사용자의 접근**을 어떻게 통제하는가?

SEC 3. 서비스에 대한 **프로그램 적 접근**을 어떻게 통제하는가?

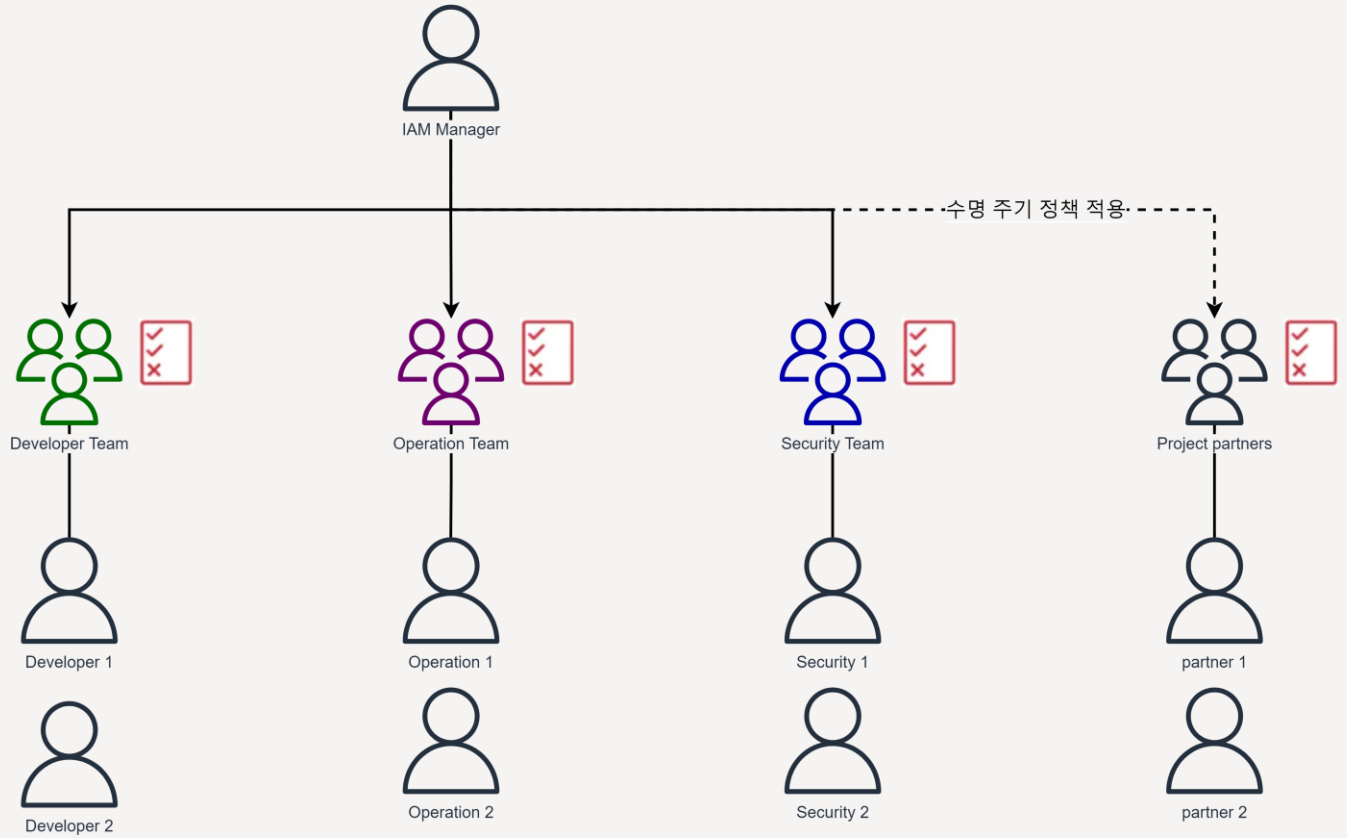
SEC 1. 워크로드의 자격증명과 인증을 어떻게 관리하는가?

모범사례

1. 법규, 규정, 회사 내규 등에 맞는 **IAM 요건** 정의.
2. AWS **루트 사용자**에 대해 MFA적용, 엑세스 키 삭제, 사용 최소화.
3. SW 또는 HW 방식의 **MFA**를 통해 추가 접근통제 적용.
4. 자동화 도구를 통한 접근통제 적용과 **불법 접근에 대한 리포팅** 체계 수립.
5. 최소 길이, 복잡도, 재사용 제한 등 **패스워드 규칙** 적용.
6. 정기적인 **자격증명 교체** 정책 적용.
7. 주기적으로 자격증명의 **관리 수준을 감사**.

AWS IAM 사용자 그룹화

IAM 요건에 맞춰 사용자를 그룹화하고 최소 권한의 원칙을 적용하여 보안성을 확보



SEC 2. 서비스에 대한 사용자의 접근을 어떻게 통제하는가?

모범사례

1. 불법 접근을 막기 위한 **직무 기반 접근 통제** 요건을 명확히 확립.
2. **최소 권한** 부여 원칙 적용.
3. 책임 추적성 및 직무 분리 원칙을 위해 **개인 별** 자격증명 부여.
4. 사용자 인사 이벤트에 연동하여 자격증명 및 권한의 **라이프 싸이클** 관리 프로세스 적용.
5. **미사용** 권한, **비활성** 자격증명에 대한 자동화된 적발, 감사 프로세스 적용.
6. 어카운트 간 접근에 **IAM 역할 수임** 기능 적용.

AWS IAM

IAM 사용자

- **MFA 적용**
- 패스워드 정책 적용
- 주기적인 권한 감사
- 역할 수임에 대한 통제

IAM 그룹

- IAM 사용자의 논리적인 그룹
- 그룹 관리 정책 적용

IAM 역할

- IAM 사용자가 수임
- 어카운트 간 접근 시
- AWS 서비스 접근 시

IAM 정책

- 최소 권한 부여
- 상세 조건 적용
- **IAM Access Advisor & Analyzer** 활용하여 주기적인 감사

ID 및 액세스 관리

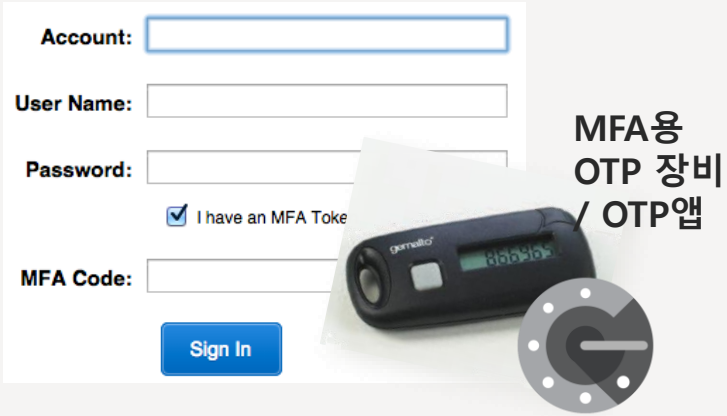
인증된 사용자에 한해 허용되는 방식으로만 리소스에 액세스할 수 있도록 하는 것을 의미

AWS 관리 콘솔

Username / Password

MFA Token (Recommended)

Signed URL (Token)



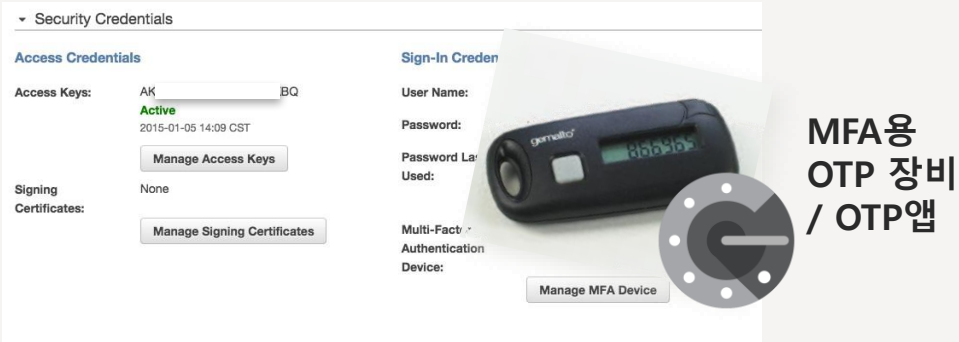
MFA용 OTP 장비 / OTP앱

API

Access/Secret Key(s)

MFA Token (Optional)

Temporary Access/Secret Key(s)



MFA용 OTP 장비 / OTP앱

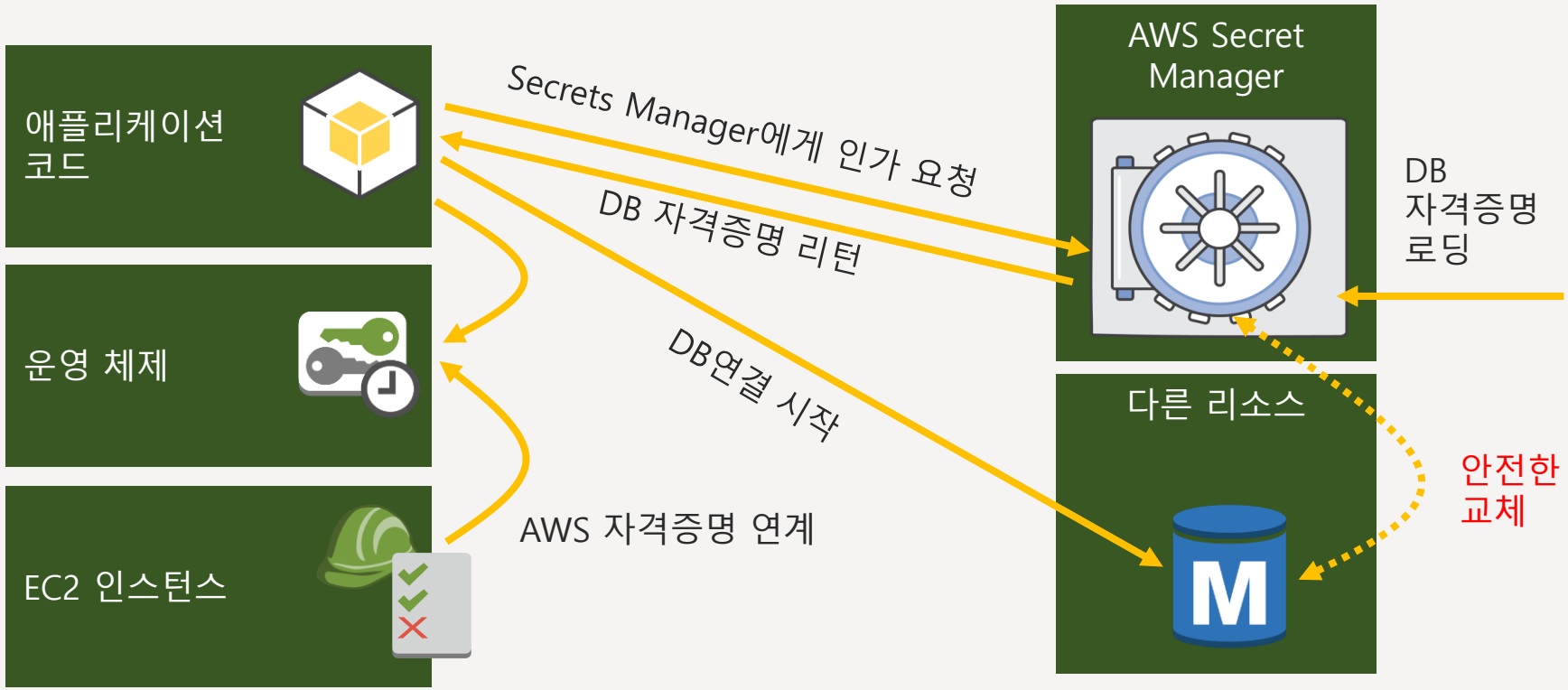
SEC 3. 서비스에 대한 프로그램 적 접근을 어떻게 통제하는가?

모범사례

1. 프로그램적으로 **접근하는 모든 유형**과 요건을 명확하게 정의.
2. 불법적인 접근을 차단하기 위해 **최소 권한**으로 프로그램 접근이 이루어 지도록 통제.
3. **미사용** 권한, **비활성** 자격증명에 대한 자동화된 적발, 감사 프로세스 적용.
4. 람다, EC2 환경 등 프로그램적으로 접근하는 모든 주체들에 대해 **개별 자격증명** 부여 원칙 적용.
5. IAM 사용자 대신 IAM 역할 수임 기능 활용.
6. 서비스 또는 시스템에 의해 **로테이션** 되는 임시 자격증명을 통해 인증 구현.

AWS Secret Manager

모든 형태의 자격증명들에 대한 신뢰할 수 있고 **안전한 자동 교체 기능**을 제공




aws partner network
service delivery
솔트웨어(주)
saltware
탐지 통제

탐지 통제

SEC 4. 보안 이벤트들을 어떻게 **탐지**하고 **조사**하는가?

SEC 5. 계속되는 보안 위협에 어떻게 **대처**하고 있는가?

SEC 4. 보안 이벤트들을 어떻게 탐지하고 조사하는가?

모범사례

1. 법규, 규정, 회사내규 등에 맞는 **로그 보존** 및 접근통제 요건 정의.
2. 필요한 메트릭을 수집하고 잠재적인 보안 위협을 **식별할 수 있는 기준**을 정의하기.
3. 경보를 받을 **관리자**를 지정하고, **대응 지침**을 수립하기.
4. 애플리케이션 로그, AWS 서비스 로그, 리소스 로그 등 필요한 모든 곳에 **로깅 기능**을 구성.
5. 모든 로그들을 중앙에서 **수집**하여 이상징후, 악의적인 행위, 침해를 **자동 분석**하는 환경 구성.
6. 보안 관련 핵심 지표, 메트릭 등이 빠짐없이 모니터링 되고, 기준에 따른 **자동 경보** 발령 구성.
7. 침해사고 대응 절차 상의 에스컬레이션 등, 다양한 보안 이벤트 유형의 **조사 프로세스** 개발하기.

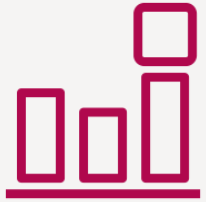
메트릭 & 로깅

Amazon CloudWatch

- 메트릭 & 필터
- 경보 & 통지
- AWS 서비스 연계
- 커스텀 연계

Amazon CloudWatch Logs

- 모니터링 & 로그 저장
- 경보 & 통지
- AWS 서비스 연계
- 커스텀 연계



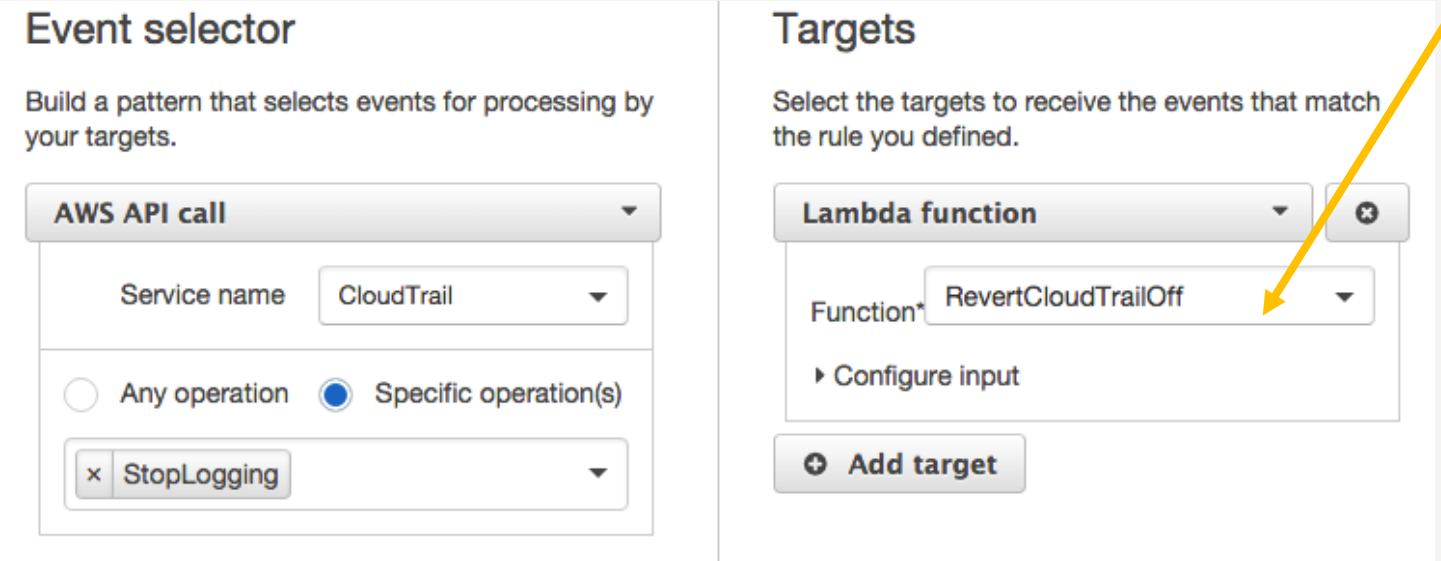
Amazon CloudWatch Events

- **자동 대응 규칙**
- AWS 서비스 연계
- 커스텀 연계

CloudWatch Events

Detect malicious API and automate response.

If trail.delete { trail.enable & email.security_team}



Example: Amazon S3 Bucket Activity
Example: Security Group Configuration Changes
Example: Network Access Control List (ACL) Changes
Example: Network Gateway Changes
Example: Amazon Virtual Private Cloud (VPC) Changes
Example: Amazon EC2 Instance Changes
Example: EC2 Large Instance Changes
Example: CloudTrail Changes
Example: Console Sign-In Failures
Example: Authorization Failures
Example: IAM Policy Changes

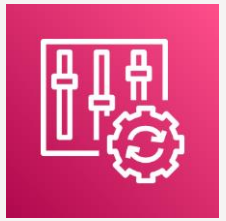
보안 이벤트 탐지

AWS CloudTrail

- **암호화 & 무결성 체크**
- 아카이빙
- CloudWatch Events 규칙 연계

Amazon GuardDuty

- 지능형 위협 탐지
- **상시 모니터링** 및 분석
- AWS service 연계

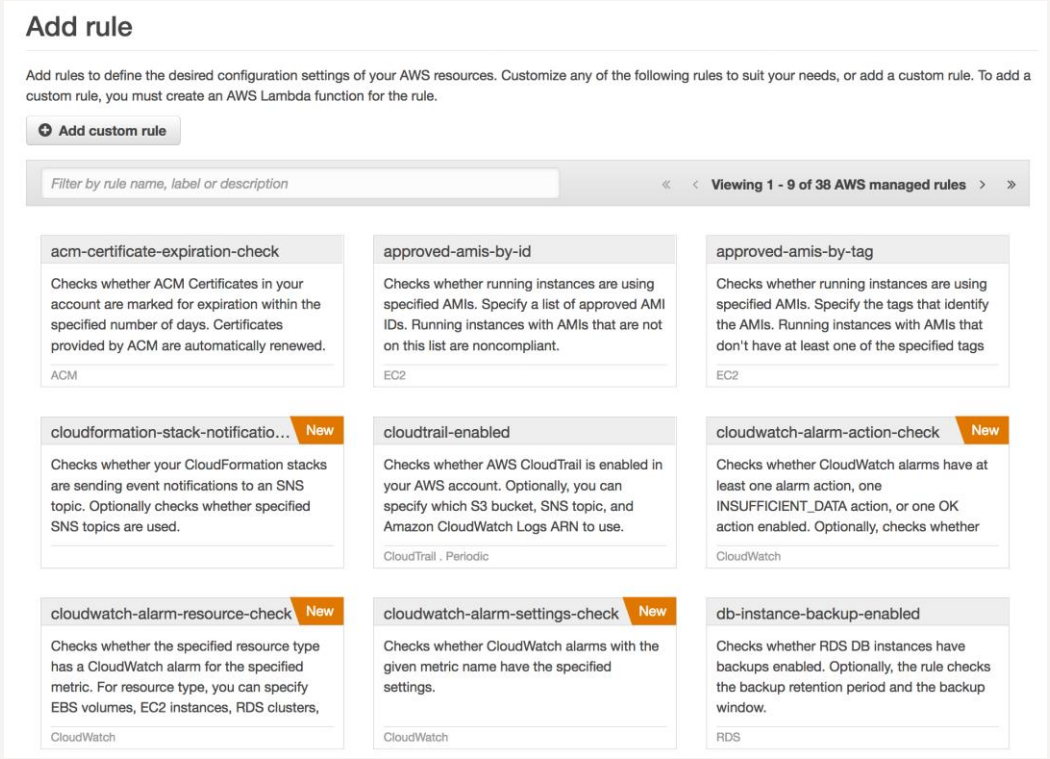


AWS Config

- 구성 **변경 추적**
- 구성 변경 이력 관리
- 리소스 관계 변경 추적

Config Rules

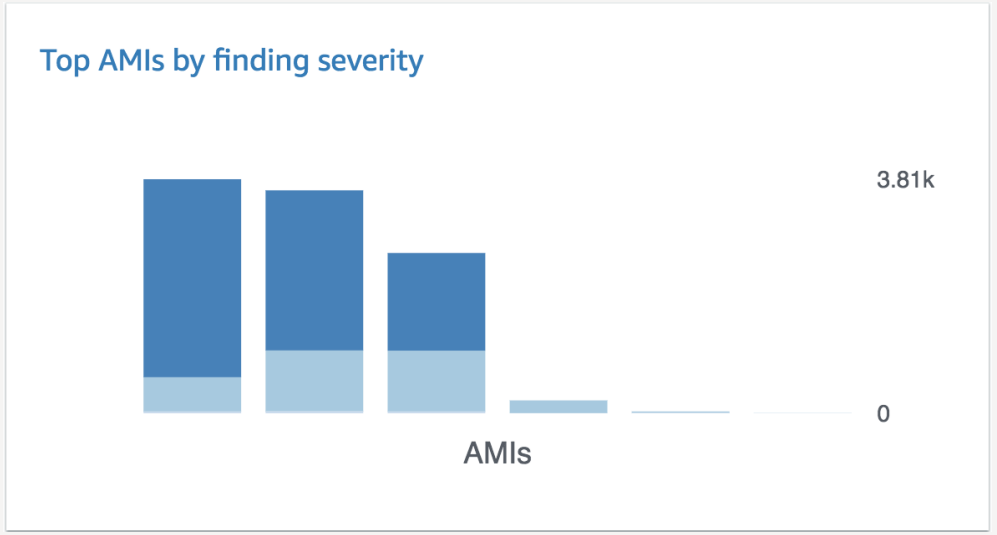
- AWS 제공 : Managed Rule
- 고객이 직접 Custom Rule 작성
- New RDK: https://amzn.to/2Wp3GkT
- Config Rules Git hub 저장소: https://github.com/awslabs/aws-config-rules



Security Hub Insights

연관관계, 필터, 우선순위 등을 주어 **Correlation**시킨 Finding들의 집합

- AWS 및 파트너들이 20여개 빌트인 Insight 제공
- **Custom Insight 정의** 지원
- Top 탐지 내역을 한번에 보여주는 대시보드 제공



Insight: 5. AMIs that are generating the most findings

Actions ▼ | Create insight

Insight results show an aggregated view of findings, typically by resource ID. To view the underlying findings of an insight result, click on the linked text below, or select a result(s) to take an action. You can also modify and save the insight definition

Record state *EQUALS* ACTIVE ⊗ | Group By: ResourceAwsEc2InstanceImageId ⊗ | *Add filter* ✕

EC2 instance image ID	Count
ami-f2d3638a	4051
ami-d1c5d1e1	3729
ami-5d967725	2640
ami-f6f16b9f	753
ami-2a8f2f43	502
ami-31814f58	502

SEC 5. 계속되는 보안 위협에 어떻게 대처하고 있는가?

모범사례

1. 법규, 규제, 회사 내규를 시의적절하게 **현행화**하여 관리하기.
2. AWS가 제언하는 권장 보안 모범사례의 최신버전을 준용하기.
3. 최신 공격 유형/기법/트렌드를 숙지하기.
4. AWS 또는 파트너에서 출시되는 신규 보안 기능/서비스에 대해 적극적으로 인지하고, 필요시, 적용하기.
5. 예상되는 **위협모델**을 수립하고, 리스크 별로 **우선순위와 대응방안**을 준비하기.

위협 모델

- 위협 모델을 세우셨나요?
- 모든 종류의 위협은 **MOM**을 가집니다:
    - **Method** : 공격을 수행할 스킬, 지식, 도구
    - **Opportunity** : 공격을 시도할 시간과 기회
    - **Motive** : 공격을 통해 의도한 것
- 탐지 및 대응 통제 절차를 주기적으로 점검하나요?

무엇을 주목해야 할까요?

준비

- 위협 모델
- 공격 **판단 기준** 수립
- **자동 대응** 절차 준비
- **상세 점검** 절차

내부자

- 훼손된 **가시성**
- 데이터 이동
- **미사용 자원**
- 소셜 관계

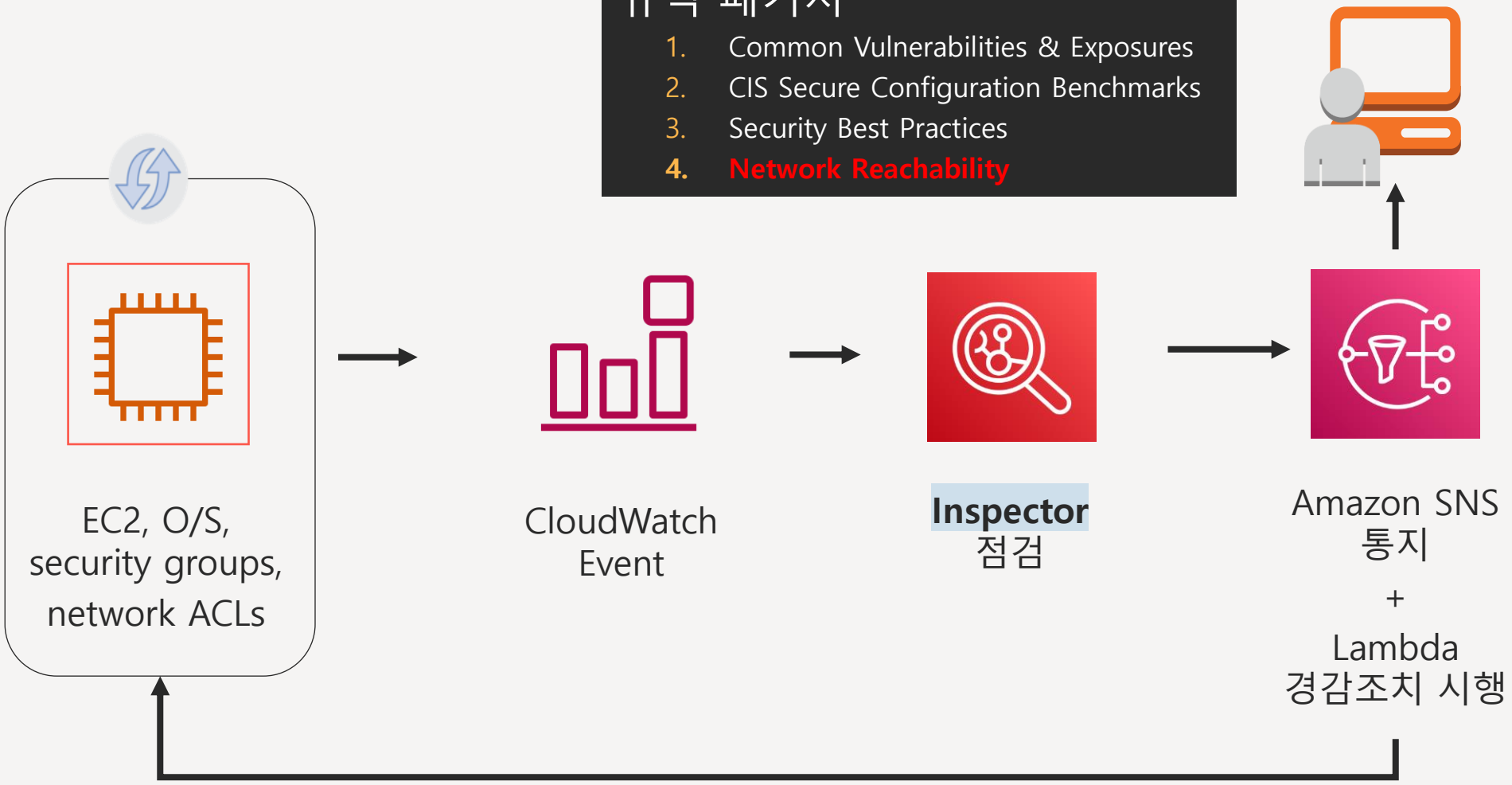
정황정보

- DNS 쿼리
- **거부/거절 로그**
- **404** Not found
- 로그인 / 시간대

상시 보안 평가

규칙 패키지

1. Common Vulnerabilities & Exposures
2. CIS Secure Configuration Benchmarks
3. Security Best Practices
4. **Network Reachability**



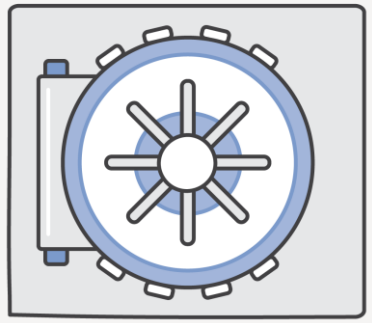
aws partner network | service delivery 솔트웨어(주) saltware

인프라 보호

인프라 보호

SEC 6. **네트워크**를 어떻게 보호하고 있는가?

SEC 7. **컴퓨팅 자원**을 어떻게 보호하고 있는가?

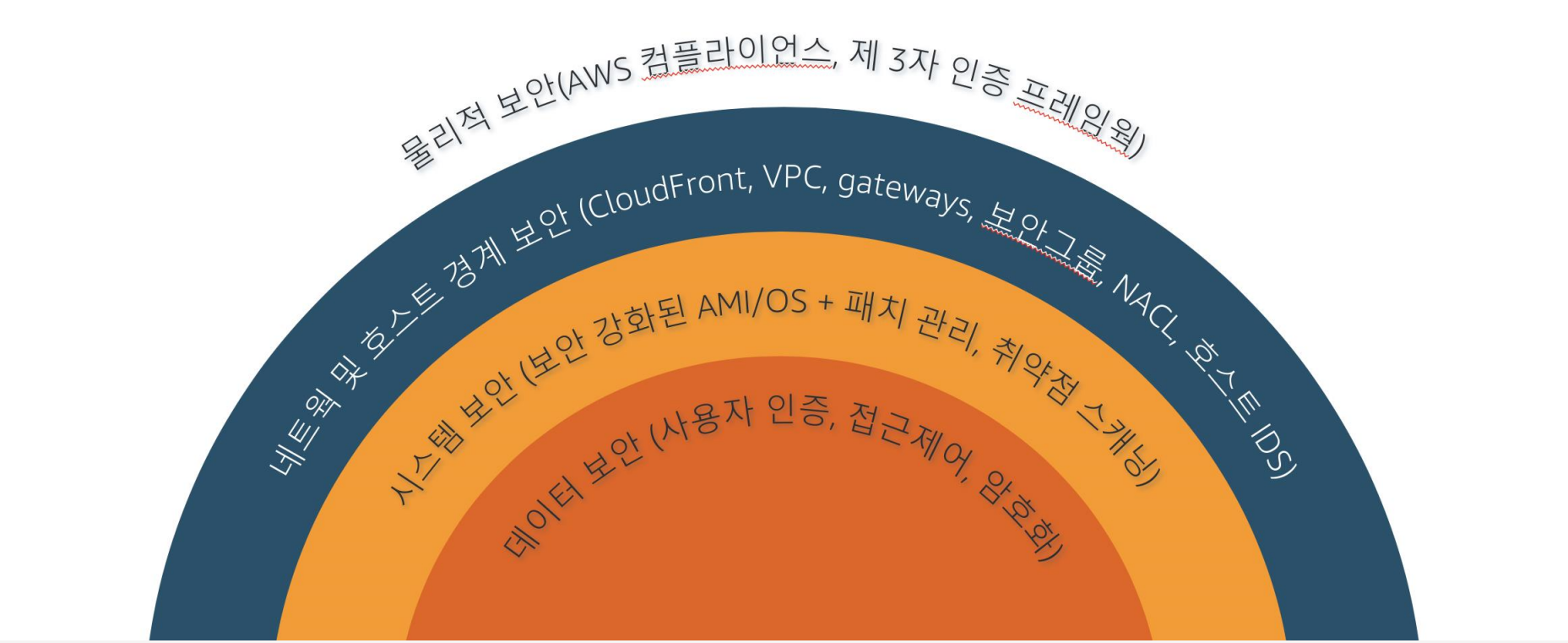


SEC 6. 네트워크를 어떻게 보호하고 있는가?

모범사례

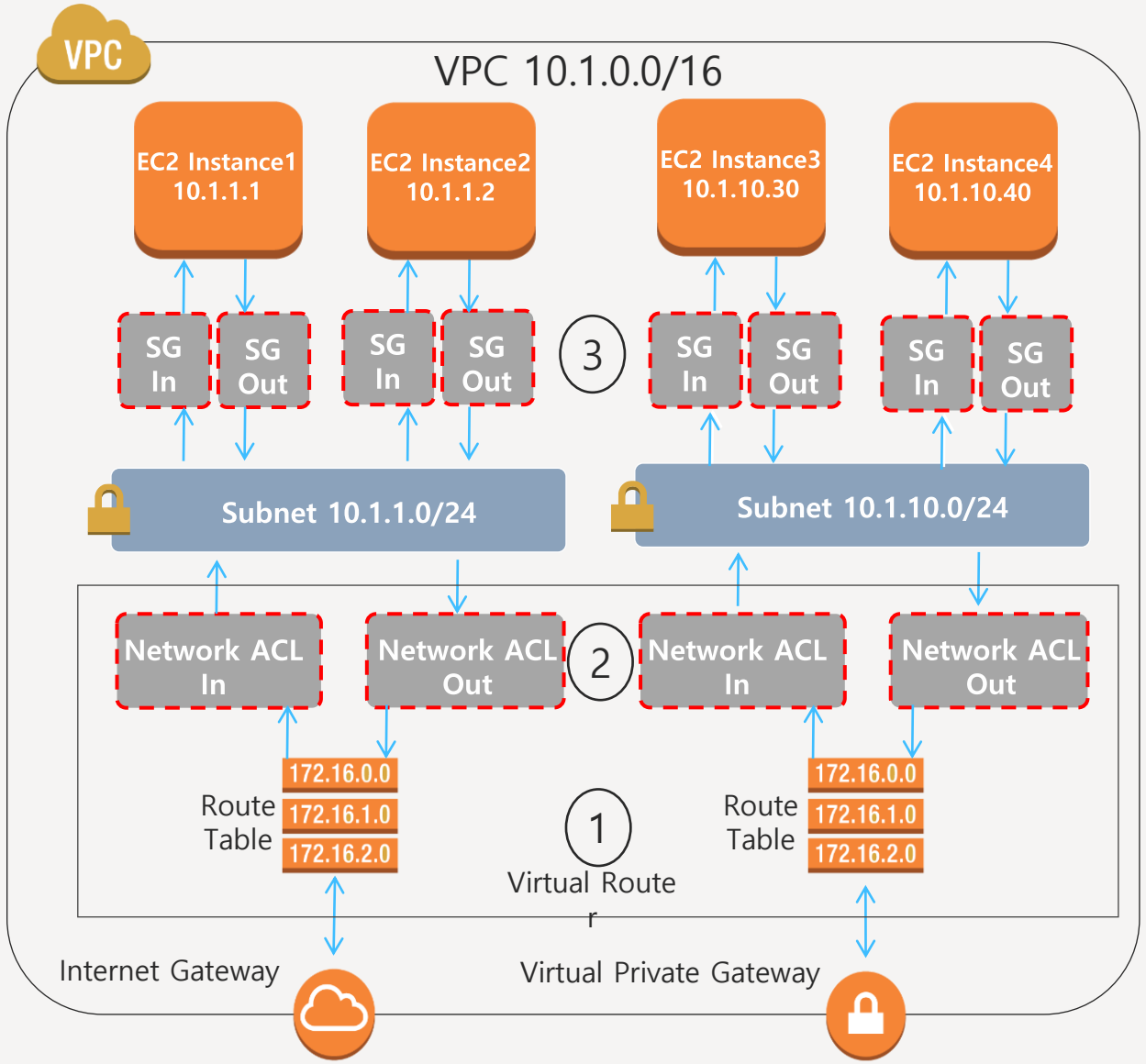
1. 법규, 규정, 회사내규 등에 맞는 **네트워크 보안 요건** 정의.
2. 꼭 **필요한 접근만 허용**하도록 하여, 워크로드를 인터넷 또는 다른 네트웍으로부터 접근하는 지점을 최소화 하기.
3. 관리자 실수를 예방하기 위하여, **구성/변경 관리툴을 통한 자동화**.
4. 지능형 위협 정보와 아노말리 탐지 기능을 기반으로 네트웍 환경 보호를 자동화.
5. 외부로부터의 위협을 방어하기 위해 웹 방화벽 같은 애플리케이션 환경을 보호해 주는 **방어 레이어**를 구성하기
6. VPC, 보안그룹, NACL, 서브넷, 라우팅, DNS 같이 모든 네트웍 레이어에 필요한 접근 통제 기능 활용하기

AWS의 심층적 보안 레이어

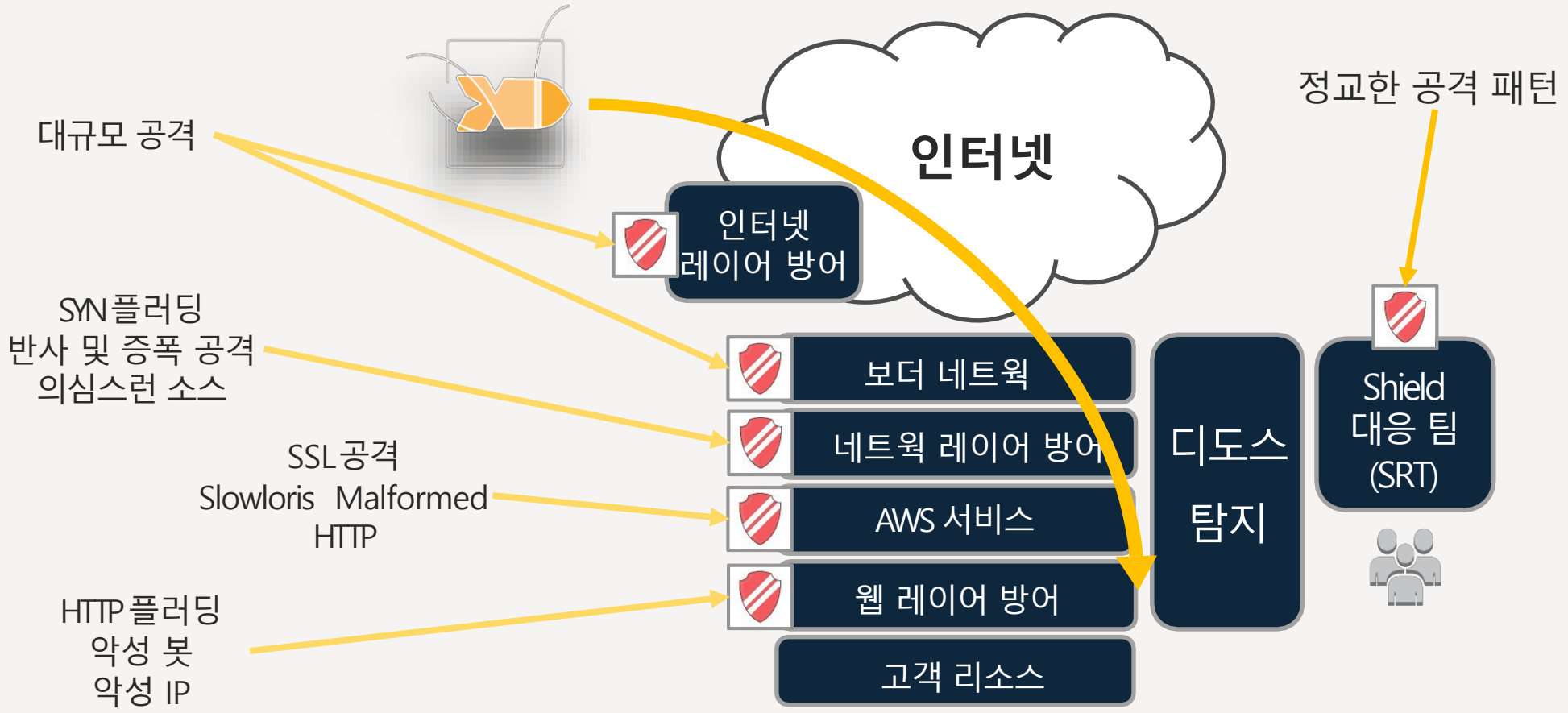


Amazon VPC

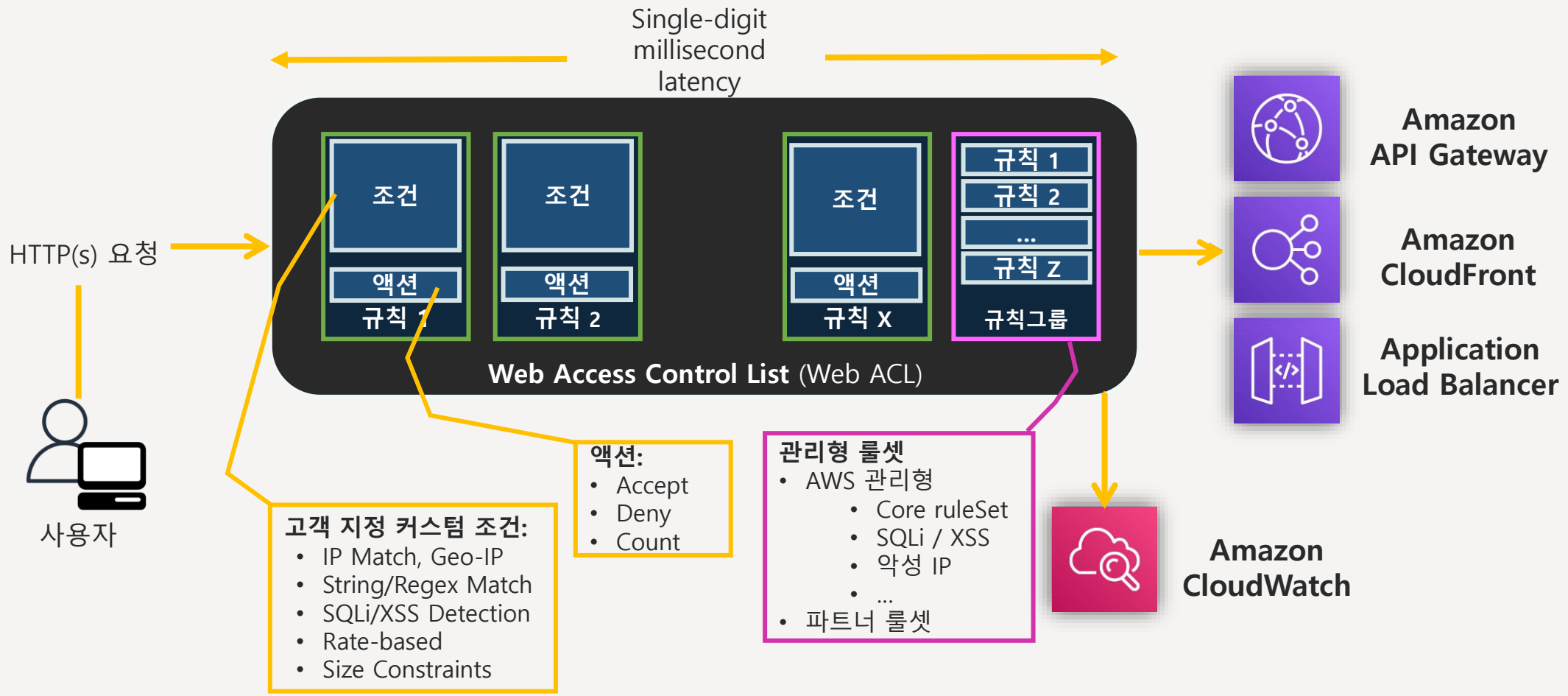
1. Route Table
   - Subnet 단위
2. Network ACL
   - Subnet 단위
   - Stateless
   - Allow/Deny
   - Rule # ordering
3. Security Group
   - 인스턴스 단위 Attach
   - Stateful
   - Allow only



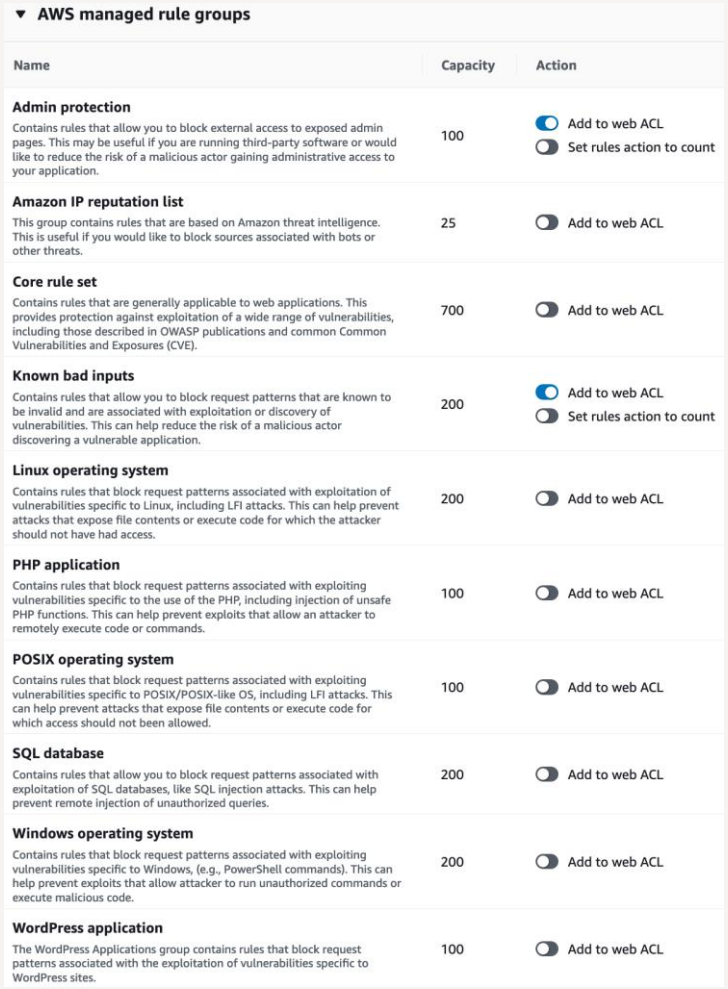
AWS Shield : 디도스 방어



AWS WAF + Managed Rulesets

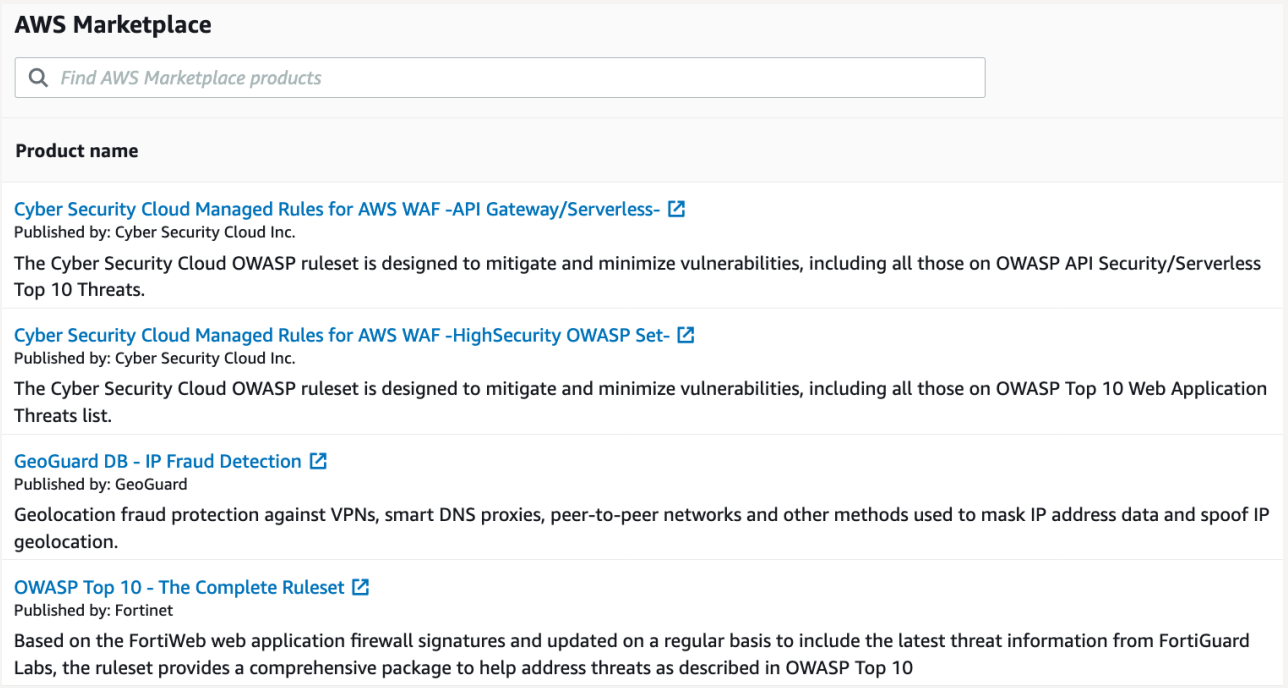


AWS WAF : 관리형 규칙 그룹



▼ AWS managed rule groups

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.	100	Add to web ACL Set rules action to count
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.	25	Add to web ACL
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications and common Common Vulnerabilities and Exposures (CVE).	700	Add to web ACL
Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.	200	Add to web ACL Set rules action to count
Linux operating system Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.	200	Add to web ACL
PHP application Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands.	100	Add to web ACL
POSIX operating system Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not been allowed.	100	Add to web ACL
SQL database Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries.	200	Add to web ACL
Windows operating system Contains rules that block request patterns associated with exploiting vulnerabilities specific to Windows, (e.g., PowerShell commands). This can help prevent exploits that allow attacker to run unauthorized commands or execute malicious code.	200	Add to web ACL
WordPress application The WordPress Applications group contains rules that block request patterns associated with the exploitation of vulnerabilities specific to WordPress sites.	100	Add to web ACL



AWS Marketplace

Find AWS Marketplace products

Product name

Cyber Security Cloud Managed Rules for AWS WAF -API Gateway/Serverless-
Published by: Cyber Security Cloud Inc.
The Cyber Security Cloud OWASP ruleset is designed to mitigate and minimize vulnerabilities, including all those on OWASP API Security/Serverless Top 10 Threats.

Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-
Published by: Cyber Security Cloud Inc.
The Cyber Security Cloud OWASP ruleset is designed to mitigate and minimize vulnerabilities, including all those on OWASP Top 10 Web Application Threats list.

GeoGuard DB - IP Fraud Detection
Published by: GeoGuard
Geolocation fraud protection against VPNs, smart DNS proxies, peer-to-peer networks and other methods used to mask IP address data and spoof IP geolocation.

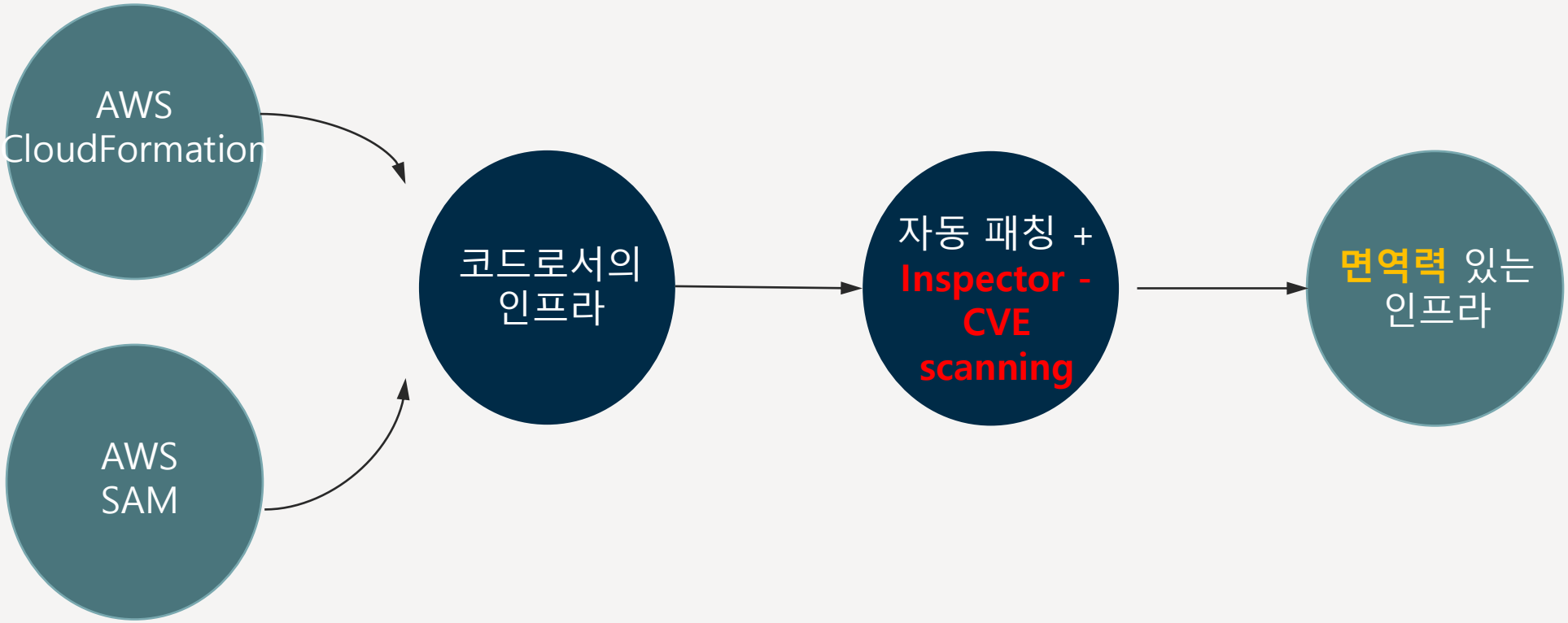
OWASP Top 10 - The Complete Ruleset
Published by: Fortinet
Based on the FortiWeb web application firewall signatures and updated on a regular basis to include the latest threat information from FortiGuard Labs, the ruleset provides a comprehensive package to help address threats as described in OWASP Top 10

SEC 7. 컴퓨팅 자원을 어떻게 보호하고 있는가?

모범사례

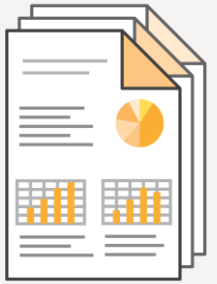
1. 법규, 규정, 회사내규 등에 맞는 컴퓨팅 리소스 보안 요건 정의.
2. 코드 레벨이나 O/S, 플랫폼 레벨의 **취약점**들을 상시 스캔하여 신규 위협에 대처
3. 관리자 실수를 예방하기 위하여, 구성/변경 관리툴을 통한 **자동화**.
4. **버추얼 패칭** 같이 알려지지 않은 위협에 대처하기 위한 자동화된 침입 방어 레이어를 구성하기.
5. **외부에 노출된 지점을 최소화**하여 공격 가능성을 줄이고, 서버보안이나 컨테이너/서버리스 보안 레이어를 구성하기.
6. 패치 관리 부담을 줄이기 위해 AWS가 제공하는 RDS, 람다, ECS 같은 관리형 서비스들을 이용하기.

인프라 면역 체계

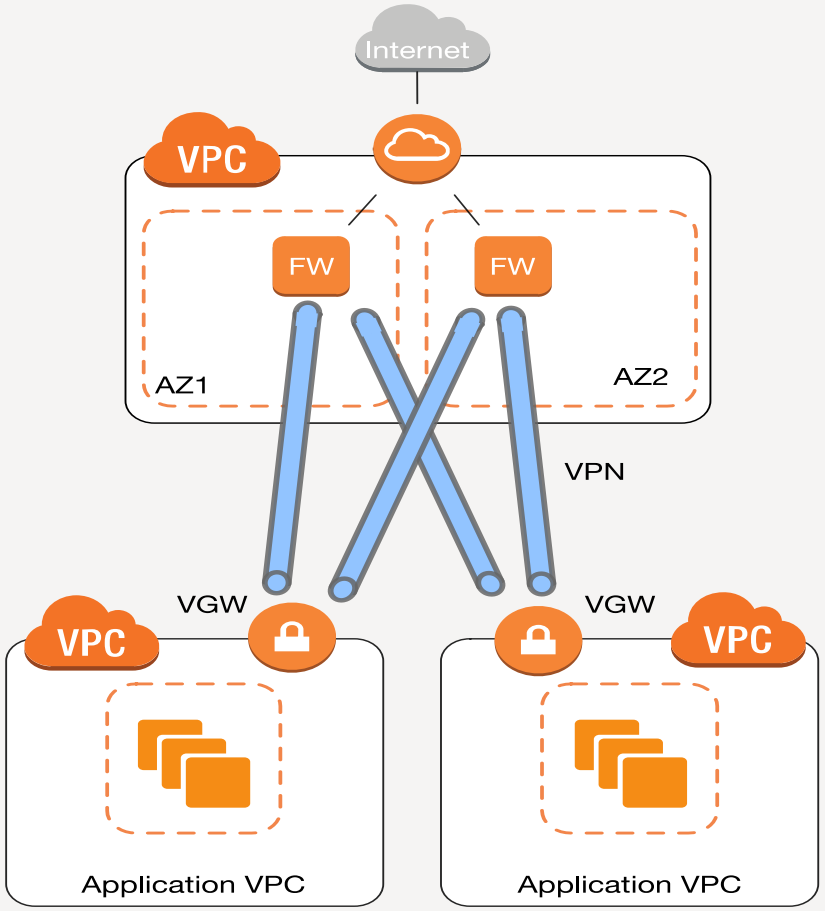


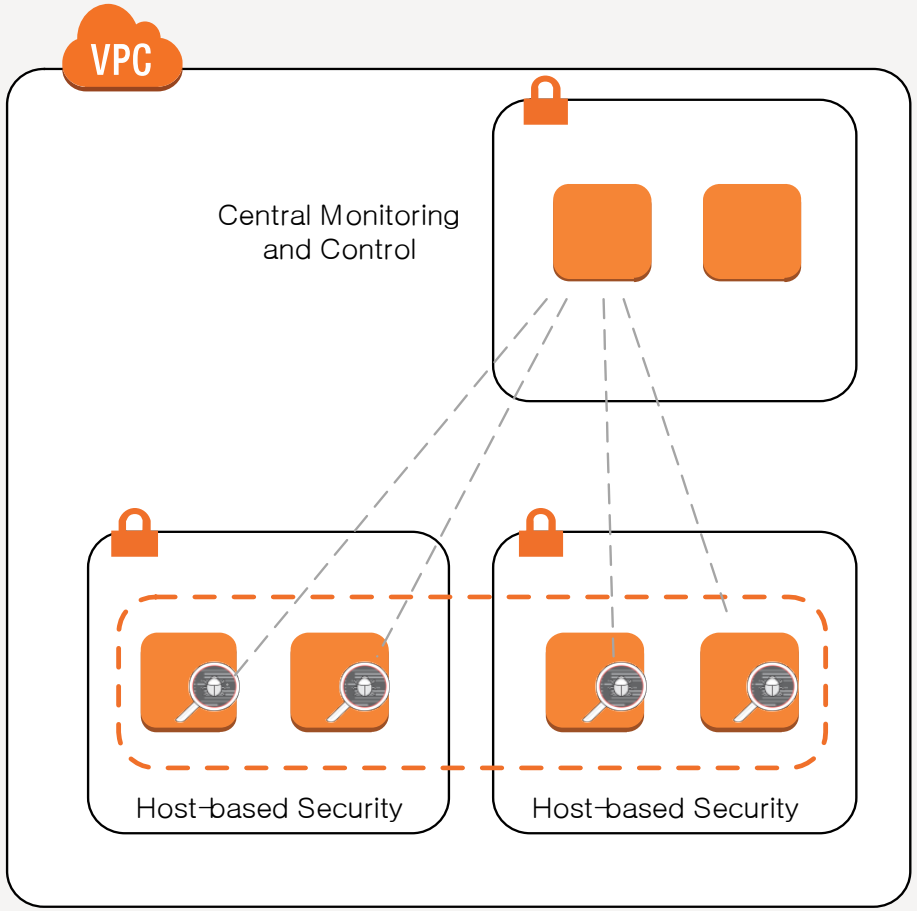
AWS Config Rules

- 구성 변경에 대한 **규정 위반** 체크
- AWS 제공 규칙 활용
- 람다를 이용하여 **커스텀 점검** 규칙 제작/적용
- 상시 점검 수행
- 규정 위반 건에 대한 가시성을 제공하는 대쉬보드



파트너 : In-line vs. Host





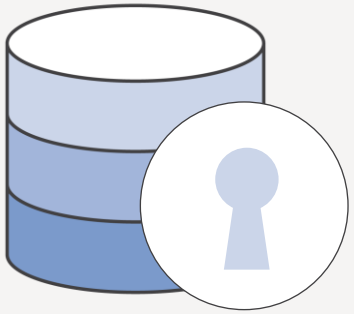
데이터 보호

데이터 보호

SEC 8. 데이터를 어떻게 **분류**하는가?

SEC 9. **저장**된 데이터를 어떻게 보호하는가?

SEC 10. **전송** 중 데이터를 어떻게 보호하는가?



SEC 8. 데이터를 어떻게 분류하는가?

모범사례

1. 법규, 규정, 회사 내규 등에 맞는 데이터 **분류 요건** 정의.
2. 민감한 데이터에 대한 추가 보호 조치 등 분류 레벨 별로 적절하게 **데이터 보호** 기능 구현하기.
3. 리소스 **태깅** 기능 등을 이용하여 적절하게 데이터 식별자를 부여하고 분류하기.
4. 관리자의 실수를 방지하기 위해 **자동 식별 및 분류** 프로세스 구현하기.
5. 워크로드 상에 법규, 규정, 회사내규 등에 맞는 데이터 유형들만 처리/보관 되고 있는 지를 통제할 수 있는 기능 구현하기.

데이터 분류

민감도를 기반으로 데이터 분류 시작하기:

- 퍼블릭 데이터 = 민감하지 않고 공개 가능한 데이터
- 프라이빗 데이터 = 엄격한 통제가 필요한 공개 불가능 데이터

리소스 태깅 기능을 이용하여 접근제어 정책과 적절하게 연계하기:

- “DataClassification=Private”
- IAM 정책과 연계하여 통제

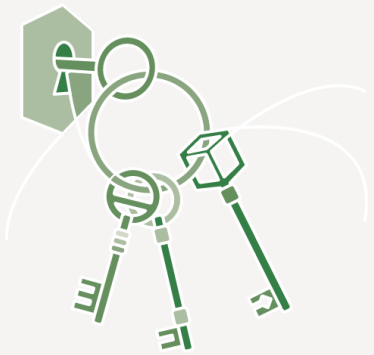
SEC 9. 저장된 데이터를 어떻게 보호하는가?

모범사례

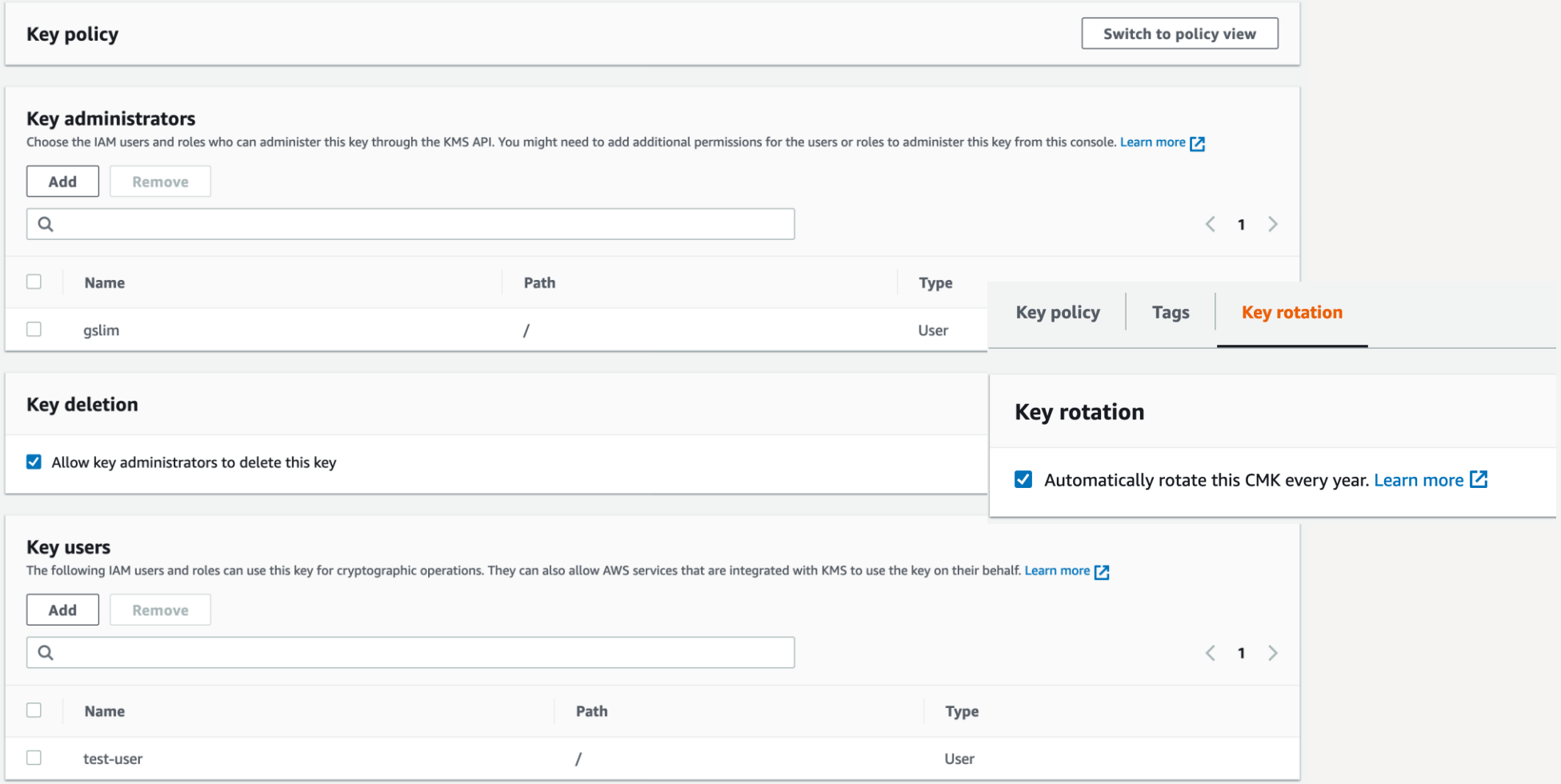
1. 암호화, 데이터 보존 연한 등 법규, 규정, 회사내규 등에 맞는 데이터 **관리 및 보호 요건** 정의하기
2. AWS KMS를 활용하여 암호화 키를 안전하게 보관하고 주기적으로 교체하고 엄격한 접근제어 적용
3. 다양한 분류 레벨과 보존 정책 별로 **서로 다른 암호화 키**를 사용하도록 통제하기.
4. 정의된 암호화 요건을 최신 기준/기술을 반영하여 현행관리하고, 이에 따라 엄격하게 통제하기.
5. 백업, 격리, 버전관리 등을 포함하여 최소 권한 부여 기준에 따라 암호화 키에 대한 엄격한 접근 통제를 구현
6. **퍼블릭 공개되는 데이터**들에 대해 상시 모니터링 체계 적용하기.
7. 대쉬보드, 간접 관리 도구를 활용하여 민감한 데이터에 직접 접근하는 경우를 최소화하여 데이터로부터 사용자를 최대한 격리하기.

AWS KMS

- 50여개 이상의 AWS 서비스에 대해 원클릭으로 암호화 적용
- 암호화 키의 중앙 관리
- 고객 생성 키 Import
- 자동화된 키 교체 적용
- 키에 대한 엄격한 접근 정책
- AWS CloudTrail상에 로깅

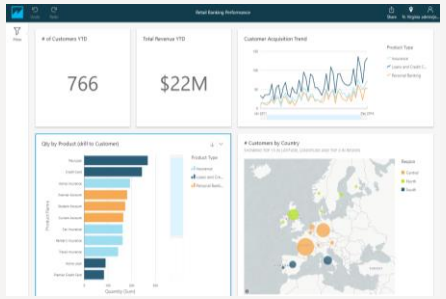


KMS Key policy + Rotation



데이터로부터 사용자 이격

대쉬보드 사용



암호화

마스킹

토큰화

기타 격리

자동화를 통해

직접 접근

최소화

+

접근통제

데이터

프로세스에 대한

버전 관리

SEC 10. 전송 중 데이터를 어떻게 보호하는가?

모범사례

1. 법규, 규정, 회사내규 등에 맞는 전송 중 데이터 보호 요건 정의하기.
2. 채널 암호화 용 인증서 및 키에 대한 관리를 **AWS Certificate Manager** 서비스를 이용하여 안전하게 보관, 교체, 접근 통제를 구현하기.
3. 최신 보안 모범사례, 기술을 반영하여 암호화 규정을 현행 관리하기.
4. 자동화된 데이터 유출 탐지 도구를 통해 외부로의 유출을 상시 감시하기.
5. 사칭이나 가로채기 등을 방지하기 위해, TLS, IPSec과 같은 프로토콜을 이용하여 통신 양자간 신원 확인을 정확히 하기.

전송 중 데이터 보호

필요시, HTTPS AWS 서비스 엔드포인트 이용

- VPC 로의 VPN 연결
- TLS 기반 채널 암호화
- EC2 상의 애플리케이션에 고객이 직접 SSL 인증서 설치
- AWS Certificate Manager (ACM) 인증서를 ELB, CloudFront, API G/W에 적용

AWS 환경의 VPN 옵션

AWS Site-to-Site VPN

AWS VPN CloudHub

AWS Client VPN

파트너 제공
소프트웨어 방식 VPN

From	To	암호화 옵션
고객 데이터 센터	VPC 리소스	• IPSec VPN(Site-to-Site) 적용
인터넷	AWS 서비스 API Public Endpoints	• 서비스 별로 HTTP/HTTPS 엔드포인트를 선별적으로 제공 • IAM 정책을 통해 HTTPS 접근만 허용되도록 통제 가능
인터넷	VPC 리소스	• AWS ClientVPN을 통해 SSL VPN 연결 구성 • 또는 직접 EC2 상에 VPN SW 구성

aws partner network | service delivery 솔트웨어(주) saltware

침해사고 대응(Incident response)

침해사고 대응

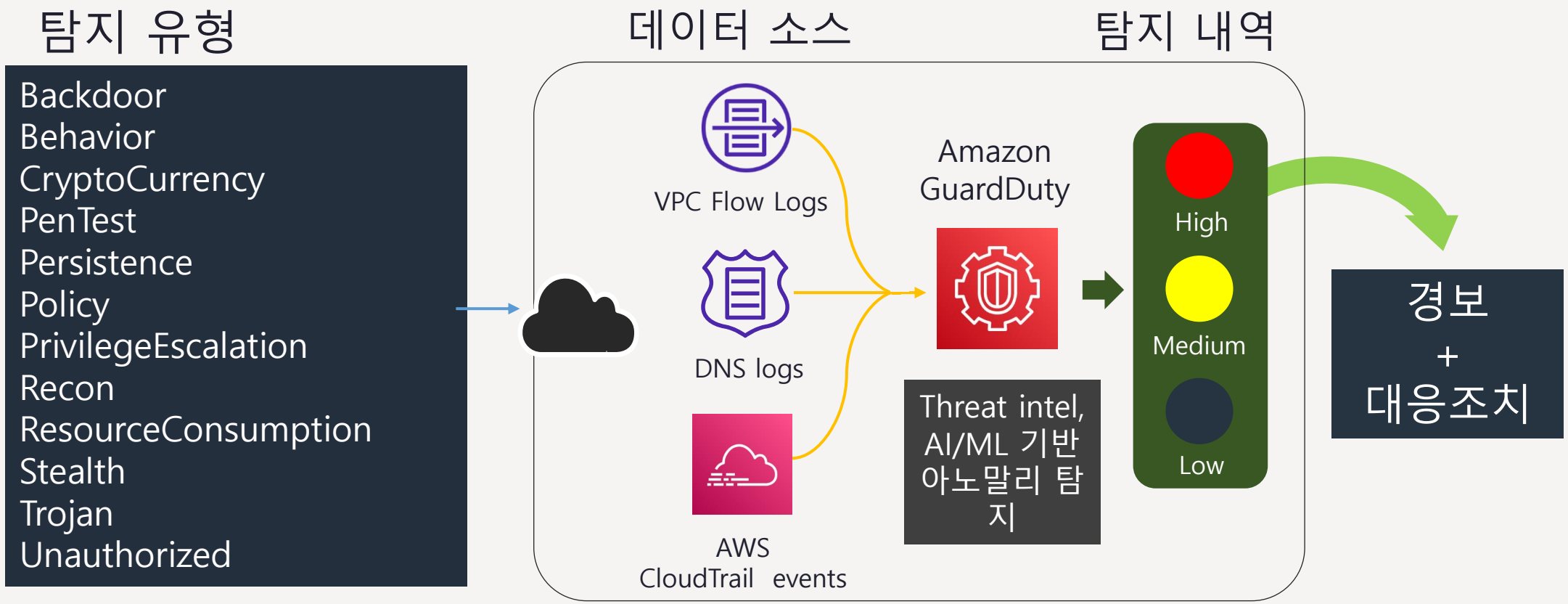
- SEC 11. 침해사고 **대응**을 어떻게 준비하는가?

SEC 11. 침해사고 대응을 어떻게 준비하는가?

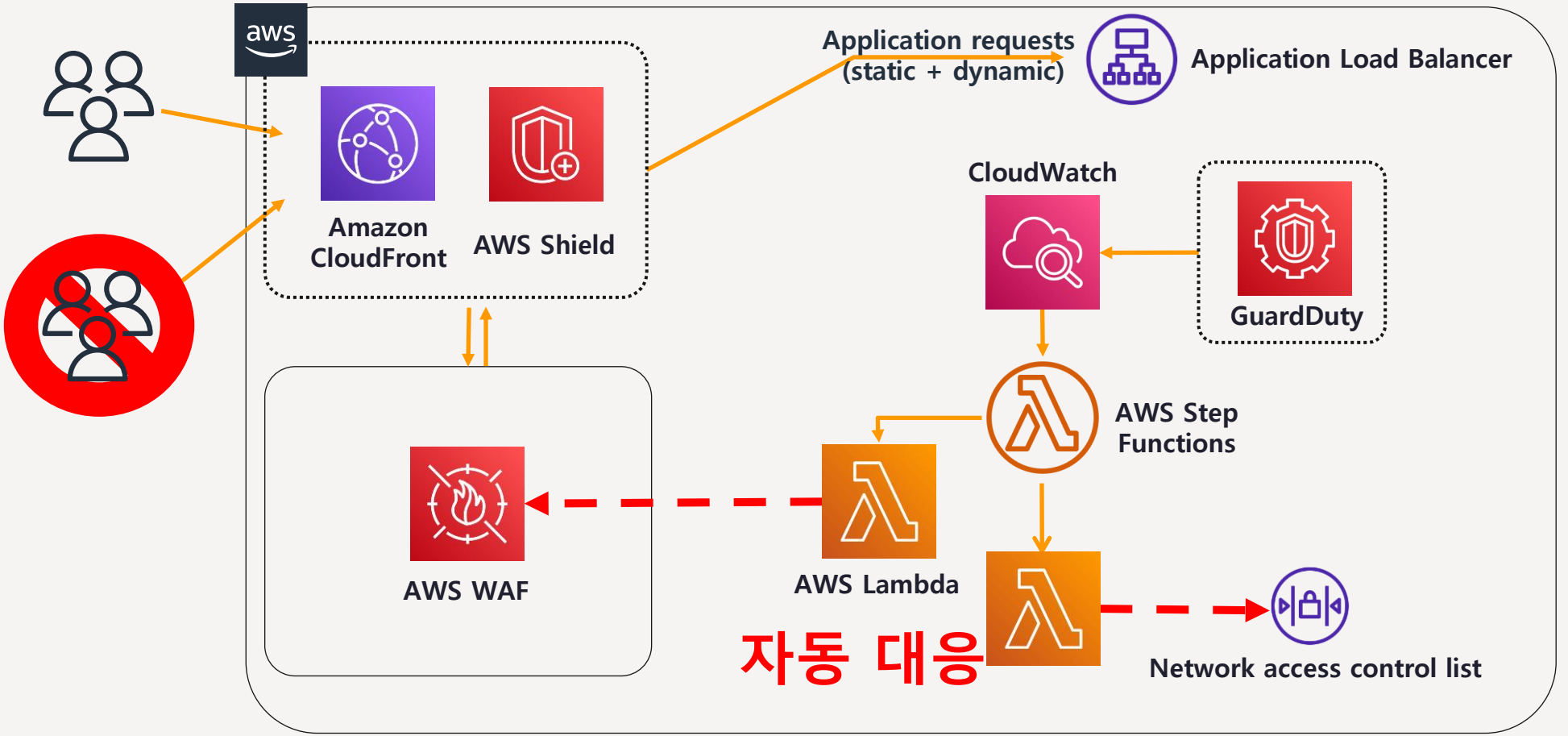
모범사례

1. 침해사고 시, 도움을 줄 수 있는 기관, 외부 전문가 등의 리소스들을 준비하기
2. AWS 제공 기능, 파트너, 오픈소스 툴 등 침해사고에 대처할 수 있는 기능 준비하기.
3. 워크로드, 조직 별로 발생 가능한 시나리오들에 대한 **대응 절차**와 내,외부 에스컬레이션 프로세스를 수립하기.
4. 대응 시간과 피해 범위를 최소화하기 위해 **자동화된 차단**/봉쇄 기능 구현하기.
5. 외부 전문가를 포함하여 유사시 **포렌식** 조사 기능을 준비하기.
6. 유사시, 신속한 대응을 할 수 있도록 대응 인력에 대한 필요 접근 권한을 사전에 부여하기.
7. 유사시, 대응 인력들이 적절하게 대응할 수 있는 충분한 도구/환경을 사전에 준비하기.
8. 대응 절차를 계속해서 개선하고, 시뮬레이션 훈련을 통해 대응 절차를 충분히 **훈련**하기

Amazon GuardDuty를 시작점으로



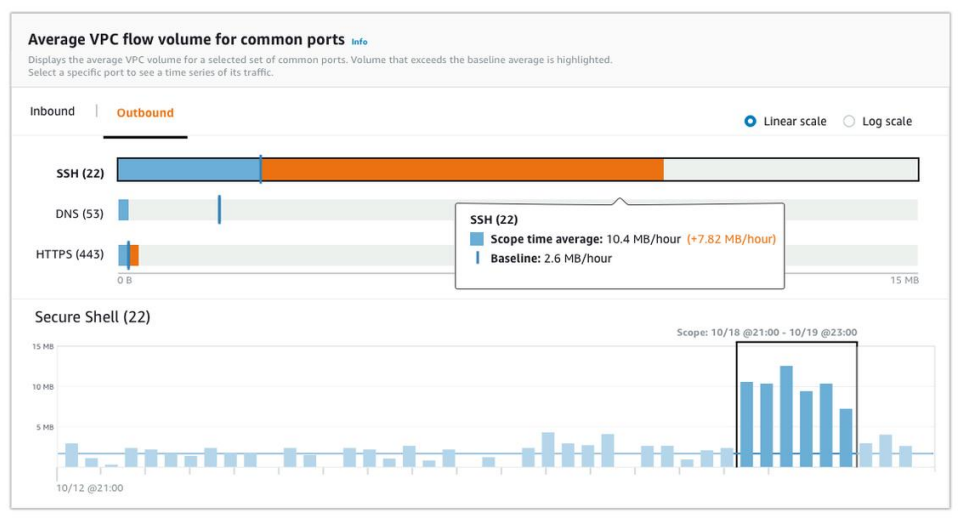
GuardDuty + Network ACL / AWS WAF 규칙



Detective를 이용한 RCA

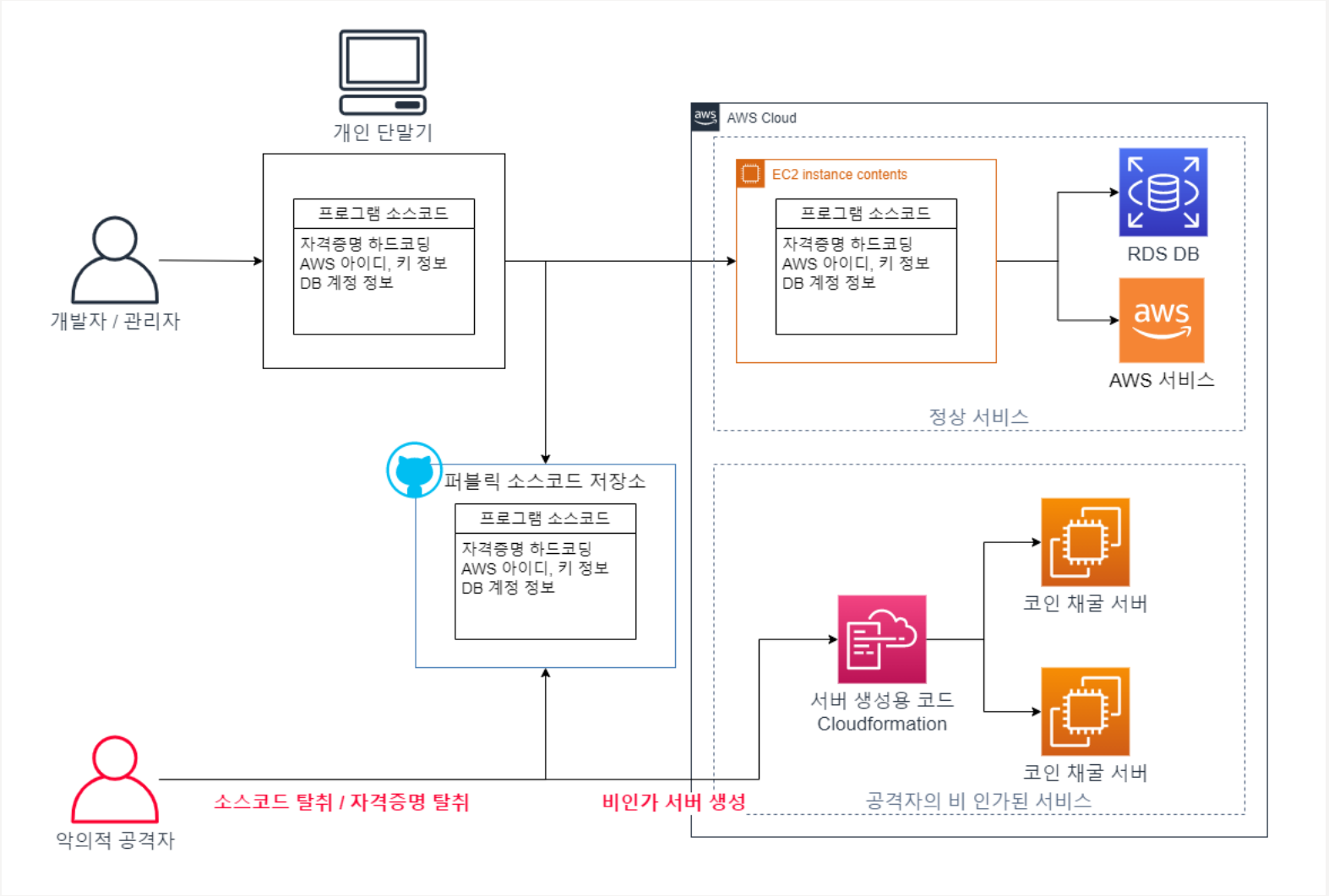
- 조금 전 발생한 일은?
- 이 실패 비율이 정상인가?

- 데이터 전송량이 얼마인가?
- 이런 상태가 정상인가?



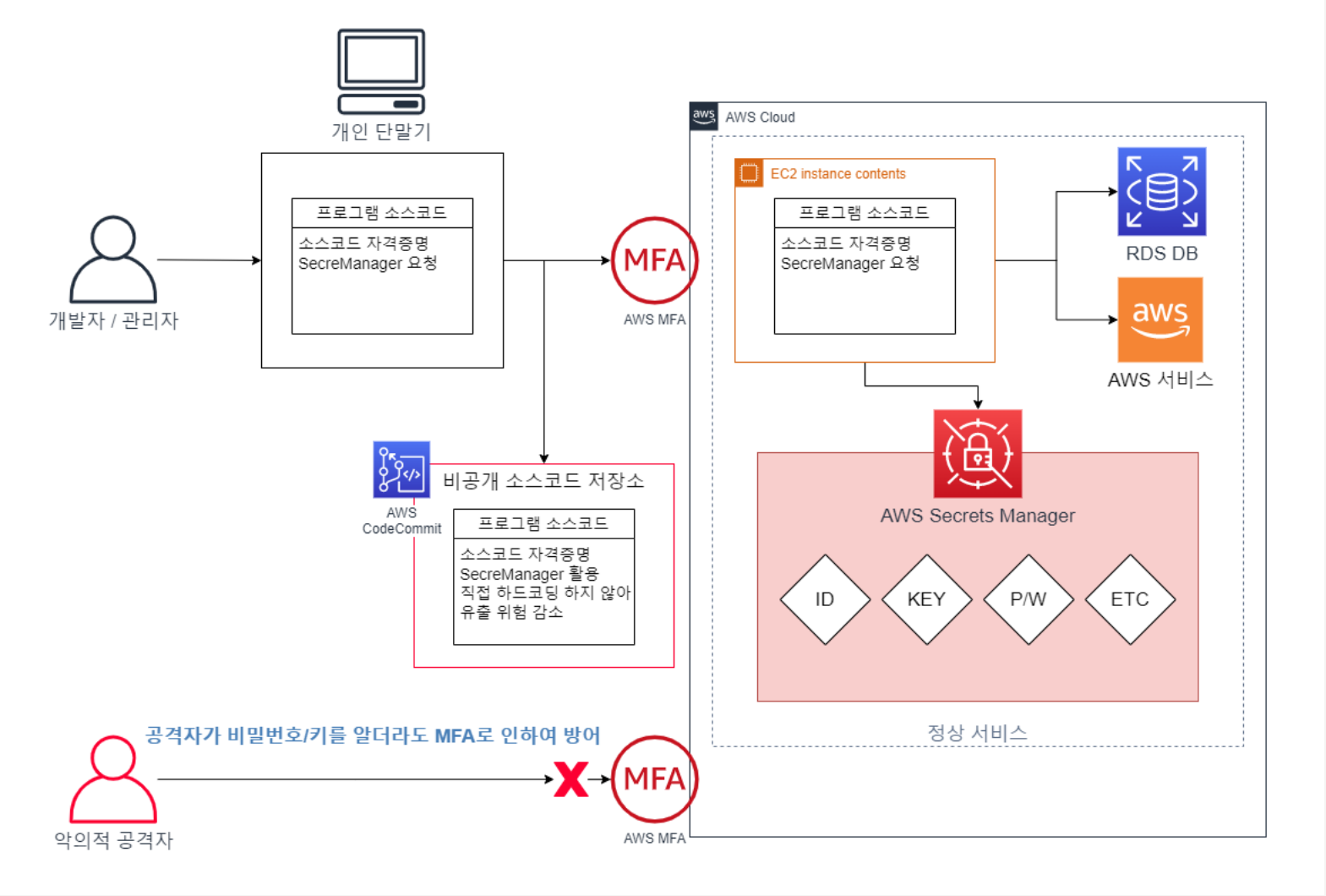
피해 및 보안구성 사례

피해 사례 A사



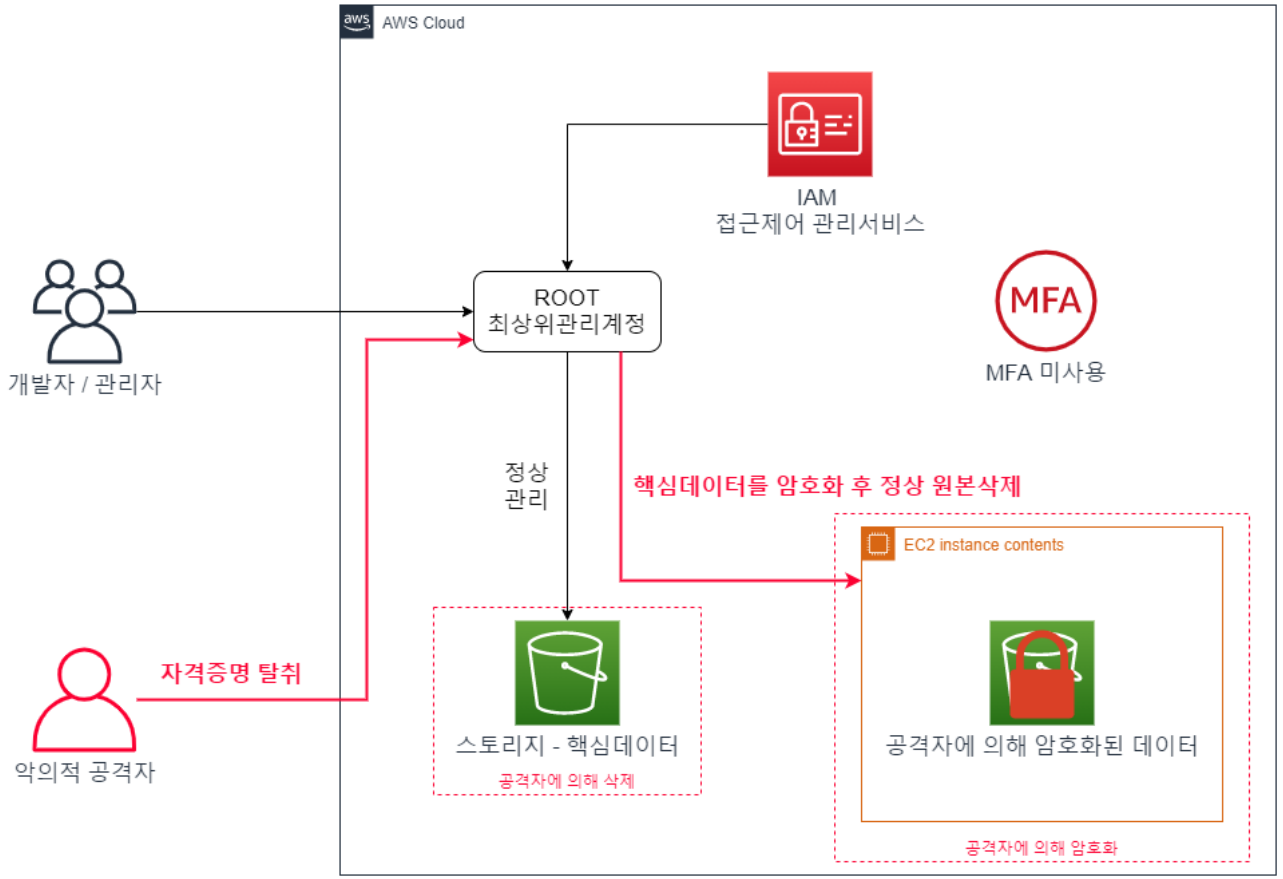
- 자격 증명을 하드코딩한 소스 코드가 유출되어 공격자가 사용자 계정으로 비인가 코인 채굴 활동을 진행 한 사례

피해 사례 A사 보안 조치



- 자격 증명을 하드코딩 하지 않고 AWS Secrets Manager에서 암호화 관리하여 유출 방지
- 소스코드를 외부에 노출하지 않고 사용하여 유출 방지
- MFA옵션을 사용하여 OTP를 모르는 공격자는 접근할 수 없도록 하여 서비스 권한 탈취 방지

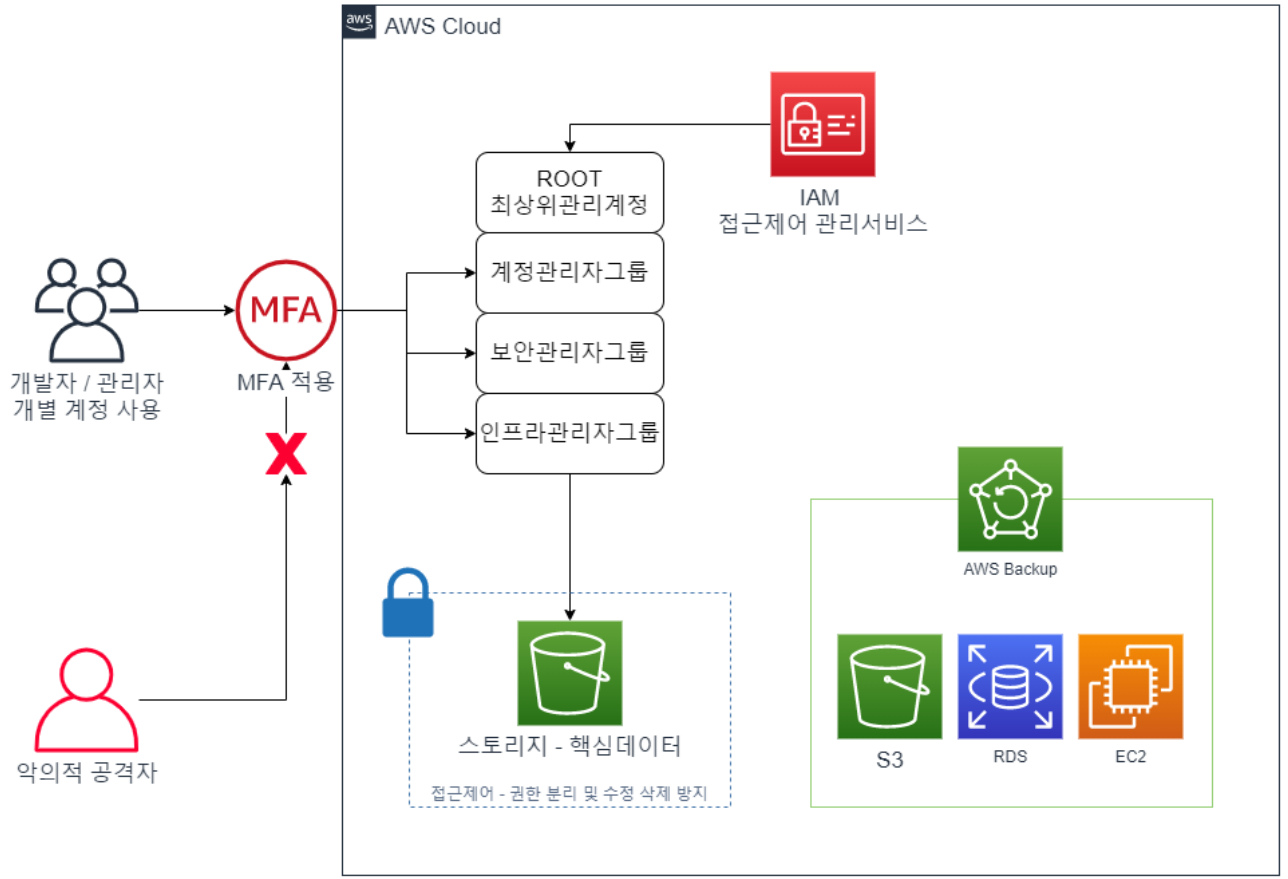
피해 사례 K사



- 단일 최상위 계정을 내부 관리자들이 MFA 없이 사용 중 공격자에 의해 유출
- ROOT를 탈취당하여 해당 계정을 제어할 최상위 계정이 없음
- ROOT가 모든 권한을 가지고 있어 공격자의 활동에 제한이 없음
- 공격자가 중요한 데이터를 암호화 하고 원본을 삭제, 복구에 대한 비용을 요구

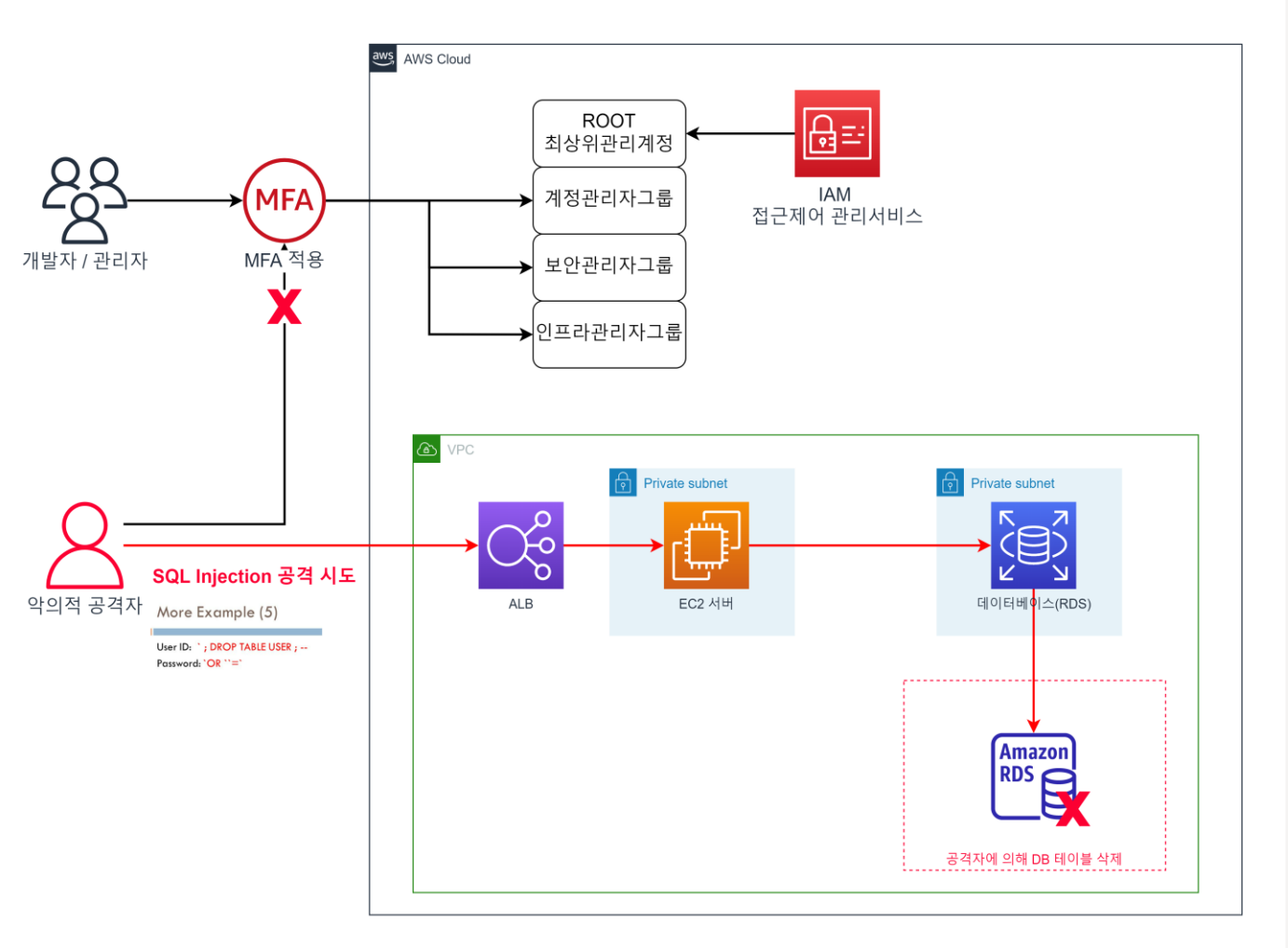
복구 시 까지 영업손실, 엔드고객에 대한 배상 이슈 발생

피해 사례 K사 보안 조치



- MFA를 사용하여 공격자가 일부 자격증명을 알더라도 OTP를 알 수 없어 접근 불가
- 계정을 그룹 권한별로 나누어 개별계정으로 관리하여 각 사용자에게 필요한 권한만 부여
- 핵심 스토리지에 접근제어를 구성하여 임의 접근을 방지하고 수정 및 삭제로부터 보호
- AWS Backup 서비스로 메인 서비스들을 고가용성 환경에 백업, 권한을 관리하여 비상 시 복구할 수 있도록 대비

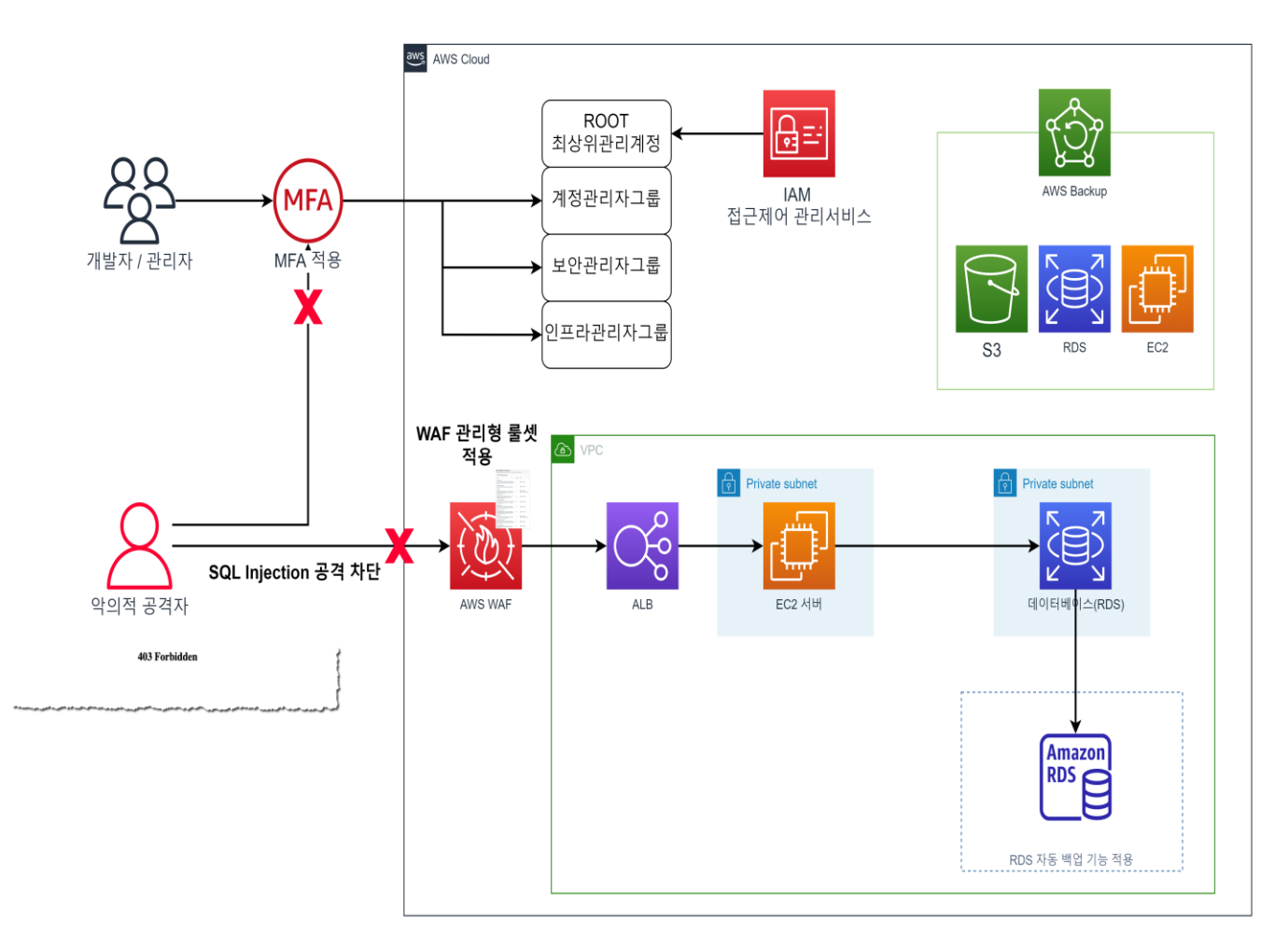
피해 사례 F사



- WEB서버에서 서비스 중인 웹 페이지를 통해 데이터베이스 테이블 삭제 목적의 SQL Injection 공격 시도
- 데이터베이스 테이블 삭제로 인한 서비스 중단 발생
- 백업 미구성으로 인한 데이터 복구 실패
- 자격 증명 탈취 외 다양한 경로를 통한 공격 가능

복구 시 까지 영업손실,
엔드고객에 대한 배상
이슈 발생

피해 사례 F사 보안 조치



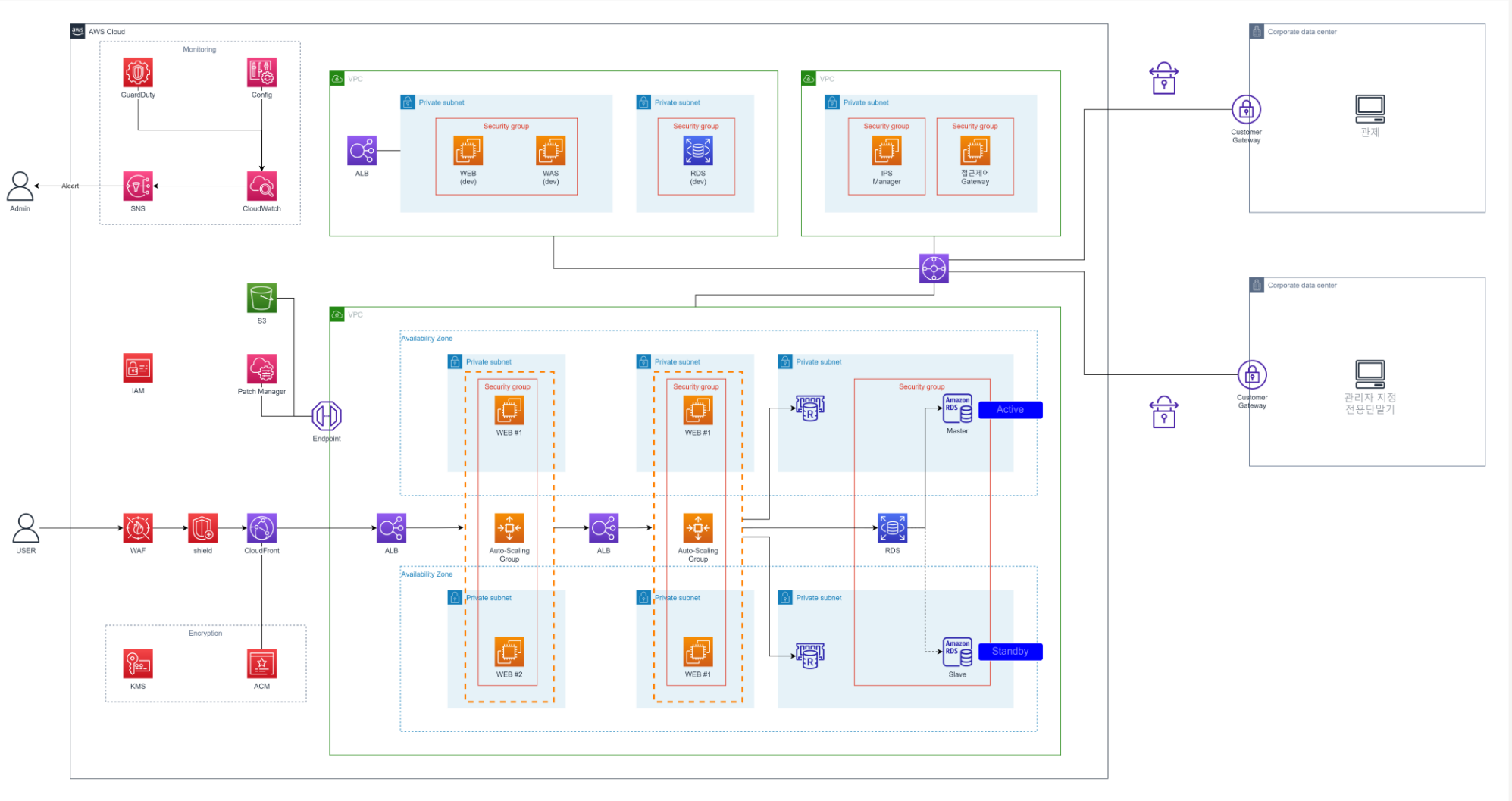
- AWS WAF의 Managed RuleSet 적용하여 SQL Injection 공격 차단
- RDS 자동 백업 기능을 활성화하여 분 단위 시점 백업으로 데이터 보호 조치
- AWS Backup 서비스를 통한 월 단위 백업 구성

aws partner network | service delivery

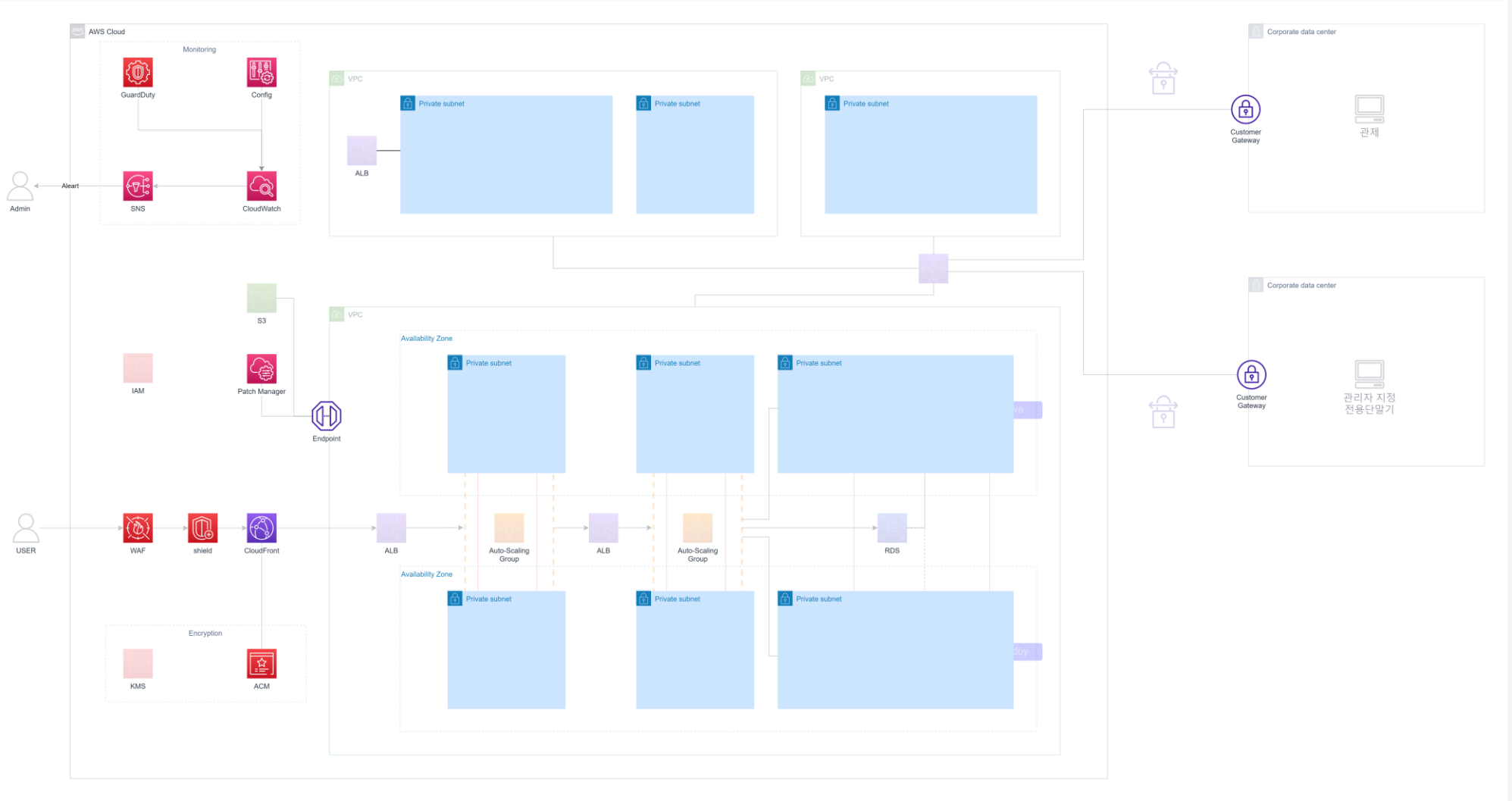
솔트웨어(주) saltware

AWS 보안 아키텍처 설계 소개

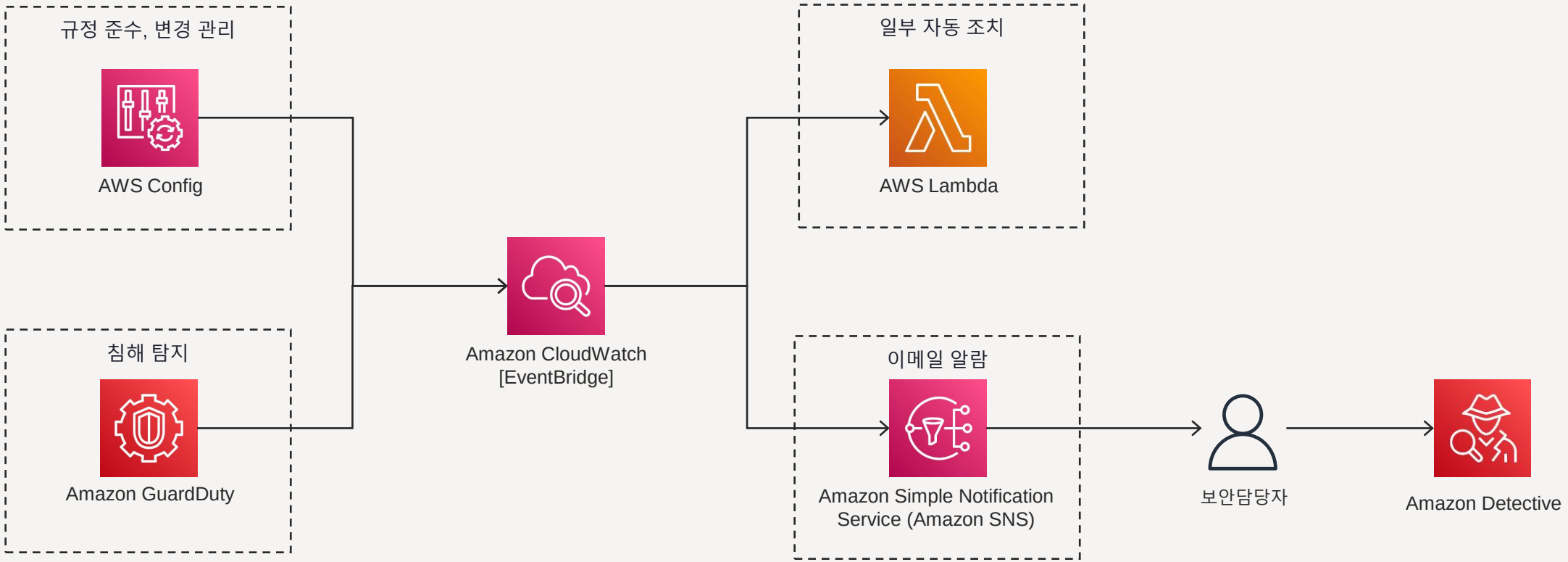
Best Practice 보안 아키텍처 예시



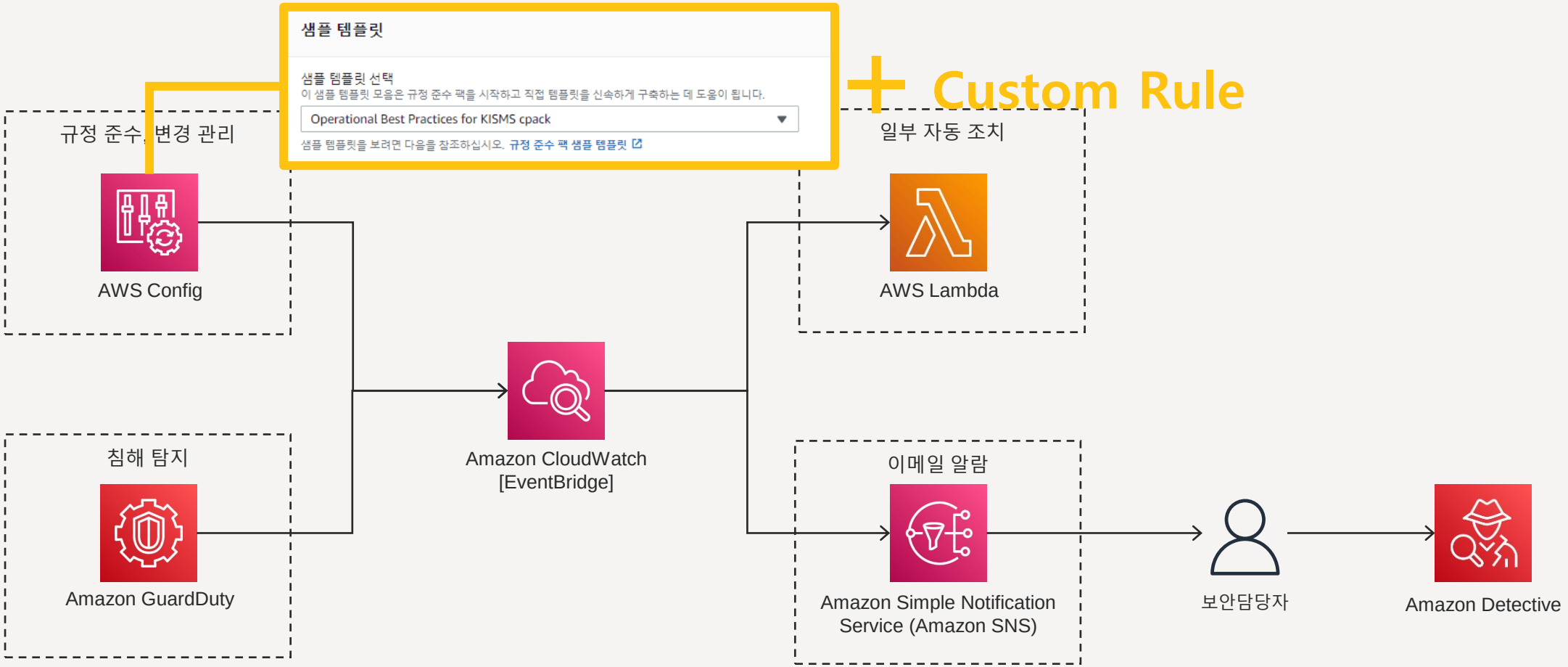
Best Practice 보안 아키텍처 예시



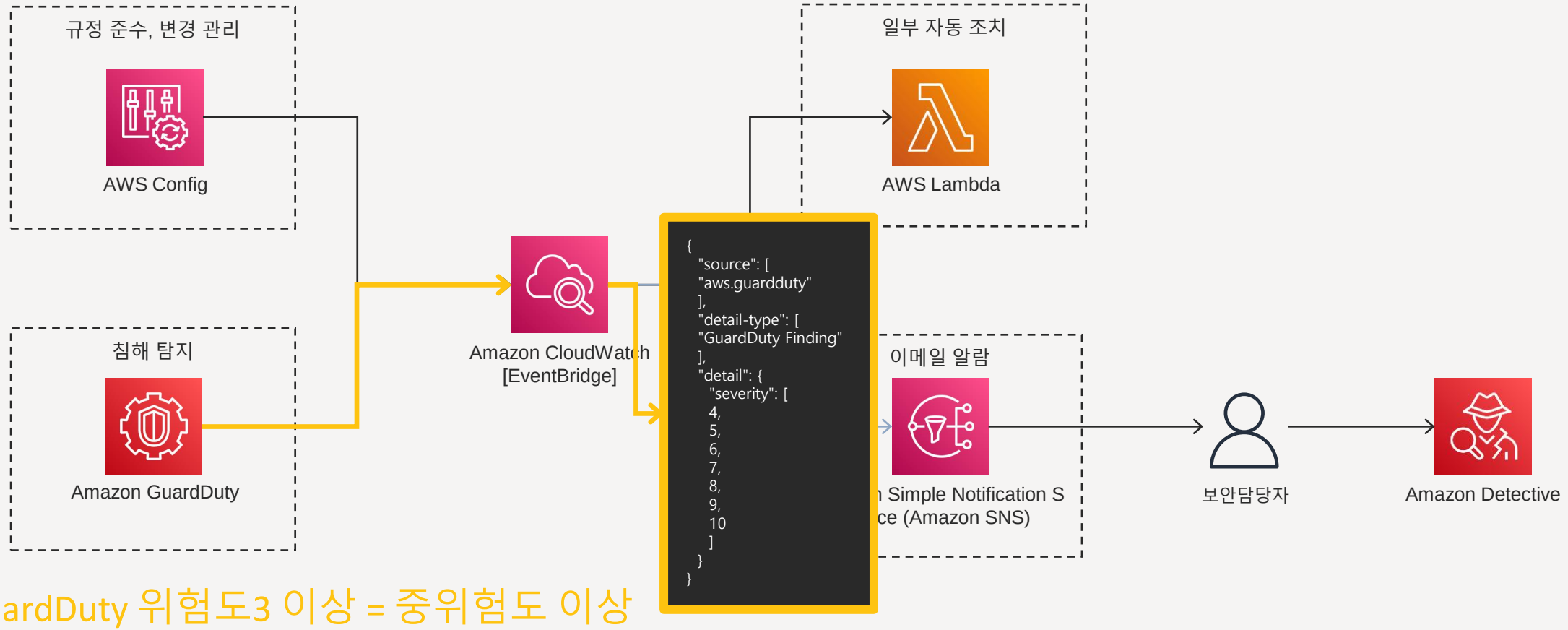
Best Practice 보안 이벤트 처리



Best Practice 보안 이벤트 처리



Best Practice 보안 이벤트 처리



GuardDuty 위험도3 이상 = 중위험도 이상

솔트웨어(주)
saltware

saltware

YOUR CLOUD CONCIERGE

Contact Info

Webpage : www.fitcloud.co.kr
Mail : csm@saltware.co.kr
Call : 02-2025-4942

aws PARTNER

- Public Sector
- Immersion Day
- Solution Provider
- Amazon RDS Delivery
- Amazon CloudFront Delivery
- DevOps Services Competency
- Financial Services Competency
- Well-Architected Partner Program

SALTWARE CO,.LTD.