AWS WAF 실전 도입 101

AWS SUMMIT SEOUL RECAP

이지영
Security Engineer
Backpackr

Agenda

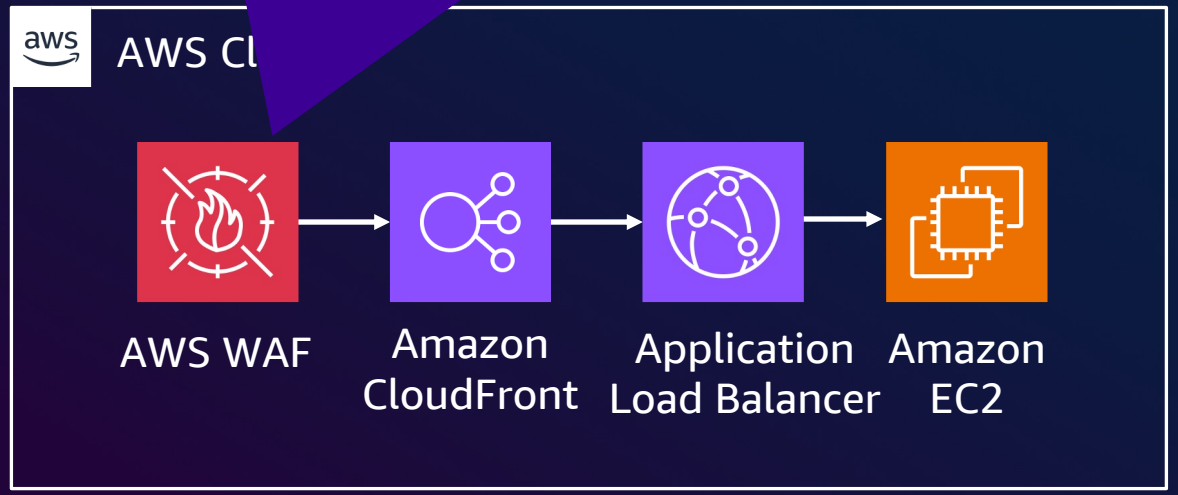
- Application LoadBalancer VS CloudFront 연결 지점 정하기
- 정규식으로 룰 용량 절약하기
- 효과적인 관리형 규칙 예외 처리
- 로그 필터링 팁
- AWS WAF 모니터링 쉽게하기
- Terraform으로 WAF 변경 히스토리 관리
- AWS WAF IP set 업데이트 간편하게 하기

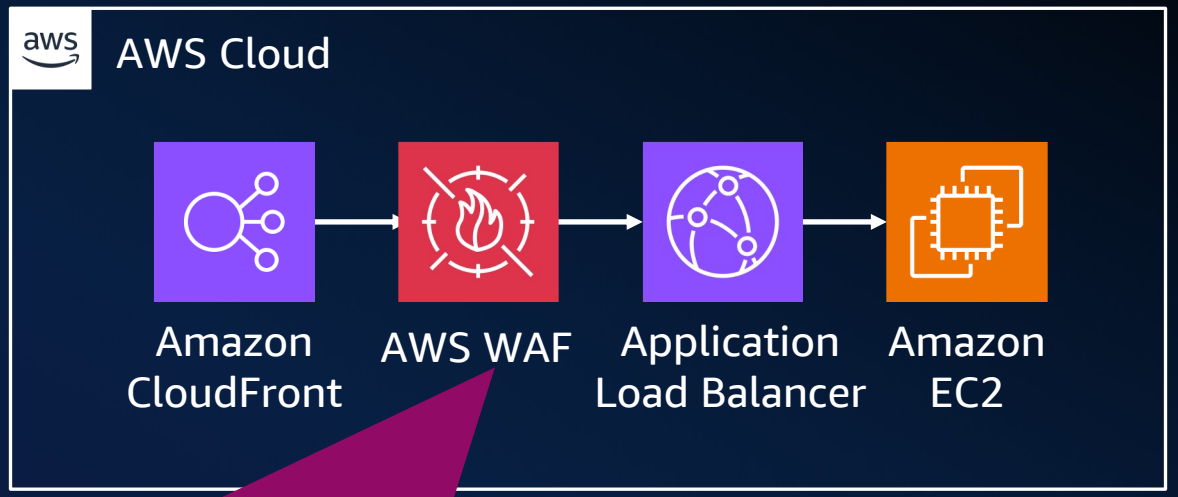
Application Load Balancer VS CloudFront 연결 지점 정하기

Recommended

CloudFront로 연결할 경우

- 트래픽 검사 사이즈가 기본 16KB ~ 최대 64KB
- DDOS 패턴의 큰 트래픽 방어에도 더욱 효과적

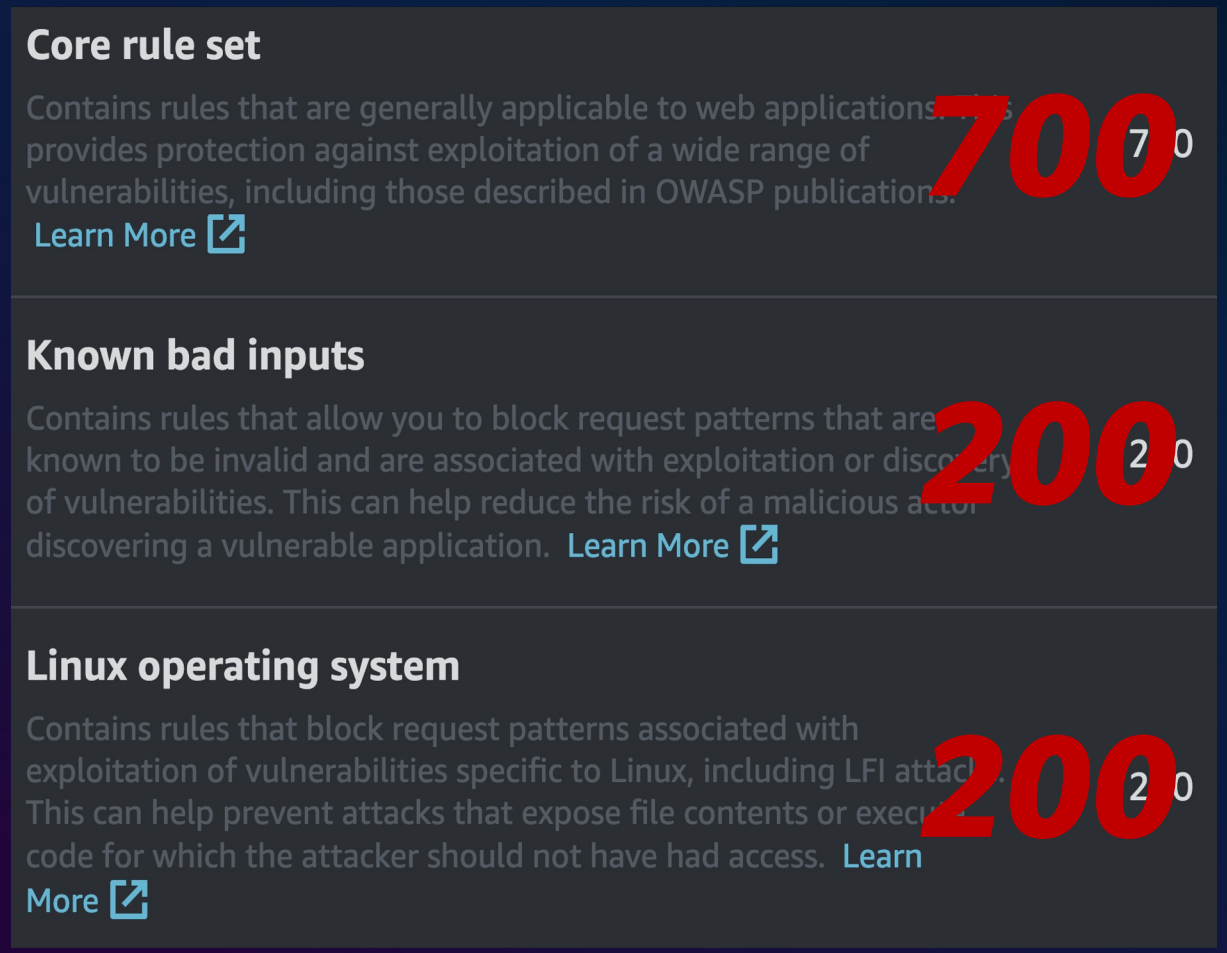




Application Load Balancer로 연결할 경우

- 트래픽 검사 사이즈가 8KB로 제한됨
- IP 기반 정책에서 CloudFront의 IP로 인식됨

정규식으로 룰 용량 절약하기



WCU(Web ACL Capacity Unit)는
1500 이상 사용시
500 구간 단위로 WAF 검사비용 증가

필수 매니지드 룰 몇개면
대부분 사라지는 1500 WCU

원하는대로 쓰려면
정규식을 통한 WCU 절약이 필수

정규식으로 룰 용량 절약하기

```
1. HeadlessChrome
2. HTTPie
3. Wget
4. Go-http-client
5. go-resty
6. Python
7. BLEXBot
8. Petalbot
11. sqlmap
12. Fuzz
13. WordPress
```

```
1. .*(?i)(HeadlessChrome|HTTPie|Wget|Go-http-client|go-resty|python|BLEXBot|petalbot|dataforseo|SemrushBot|sqlmap|fuzz|WordPress).*
```

단 1건의 정책으로 OK

정규식으로 차단해야 할 모든 User Agent를 한줄로

3 WCU의 사용만으로 정책 완성

대소문자 무시까지도 정규식 안에서 해결 가능

차단해야 할 User Agent마다 정책 필요

급속도로 소진되어가는 WCU

각 정책 별로 대소문자만 무시해도 정책마다 WCU 10 추가 소진

효과적인 관리형 규칙 예외 처리

효과적인 관리형 규칙 예외 처리

Name	Rule action
SQLi_BODY_RC_COUNT	Use action defined in the rule
SQLi_QUERYARGUMENTS_RC_COUNT	Use action defined in the rule
SQLiExtendedPatterns_QUERYARGUMENTS_RC_COUNT	Use action defined in the rule
SQLiExtendedPatterns_QUERYARGUMENTS	
SQLi_QUERYARGUMENTS	
SQLi_BODY	*Rule action : Count*
SQLi_COOKIE	
SQLi_URIPATH	

Statement 1

Inspect

Has a label

Match scope

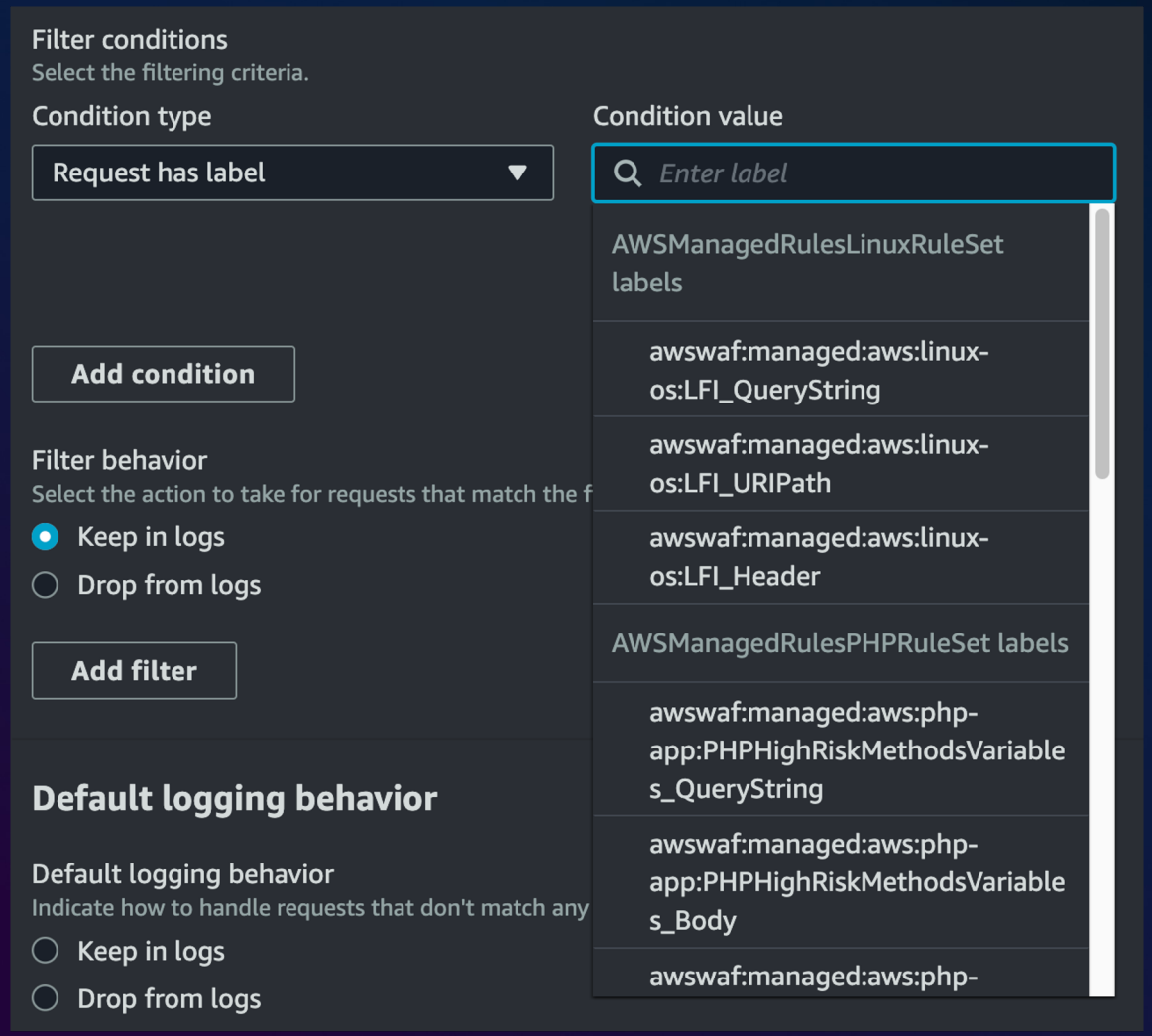
LABEL

Match key

awswaf:managed:aws:sql-database:SQLi_Body

관리형 규칙에서 지정한 레이블 기반 차단 정책 추가 생성

로그 필터링 팁

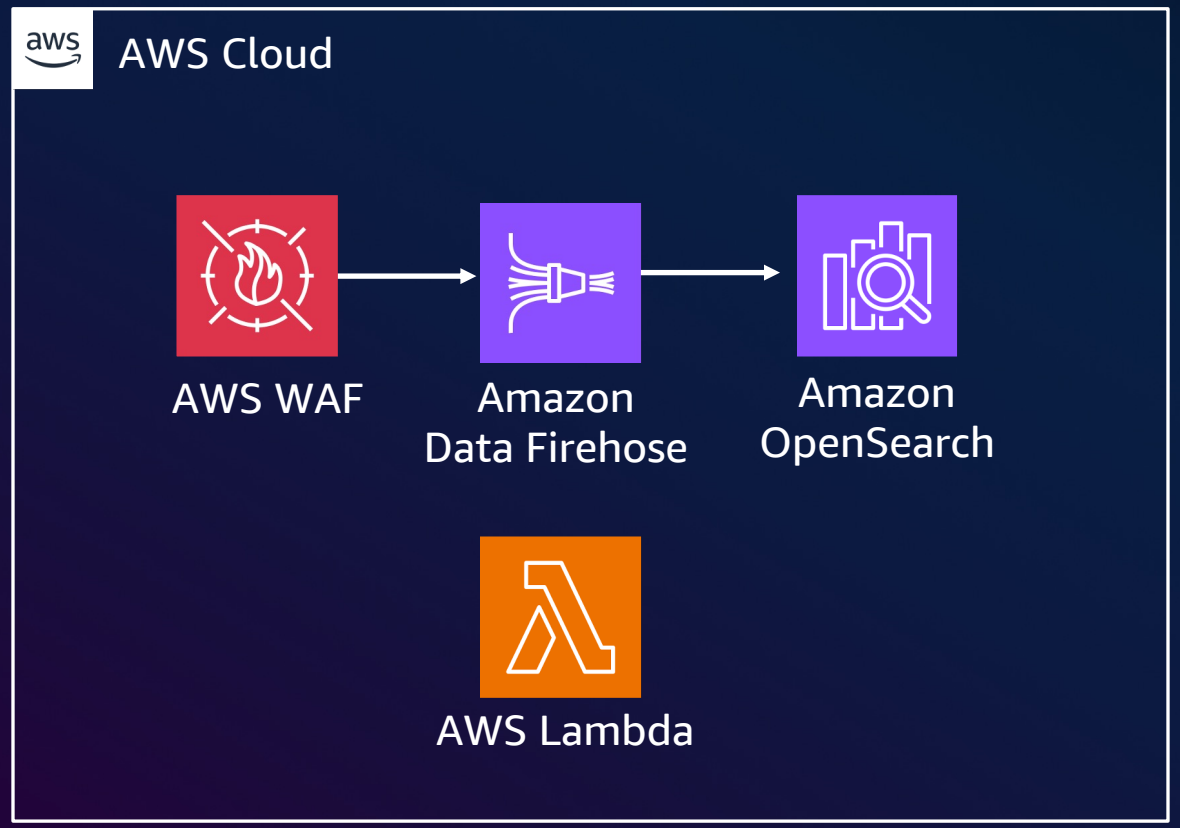


레이블만 잘 활용해도
필터링은 성공한다

Action 기반으로만 로그를 남기면
로그 최적화가 쉽지 않음

로그 필터링 최적화는
로그 모니터링 비용과 성능과 직결

AWS WAF 모니터링 쉽게 하기

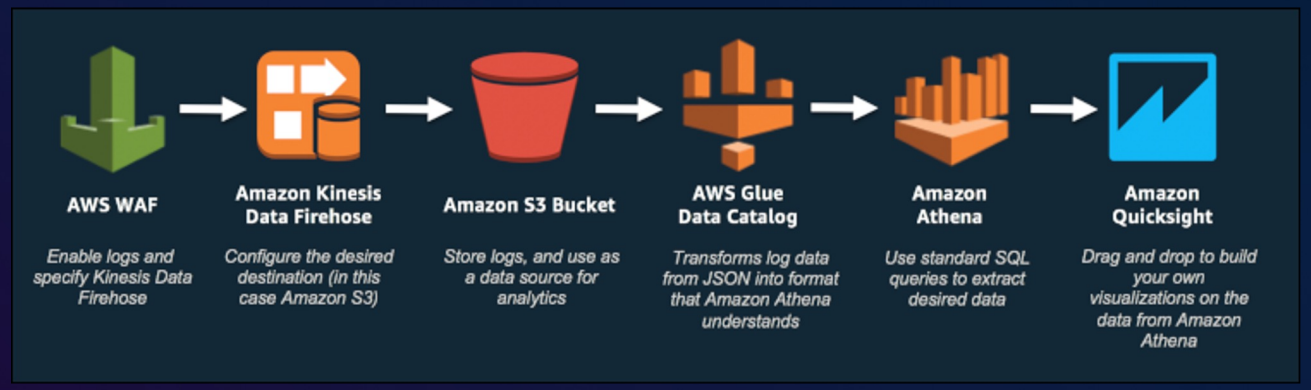


실시간 모니터링 목적으로는
Amazon OpenSearch Service 추천

Cloudwatch logs와 동일 용량의 로그 처리시
Firehose가 약 1/10 수준의 비용 발생

단, 누적 데이터가 많아질수록
인스턴스 + 저장 비용이 높아지므로 주의 필요

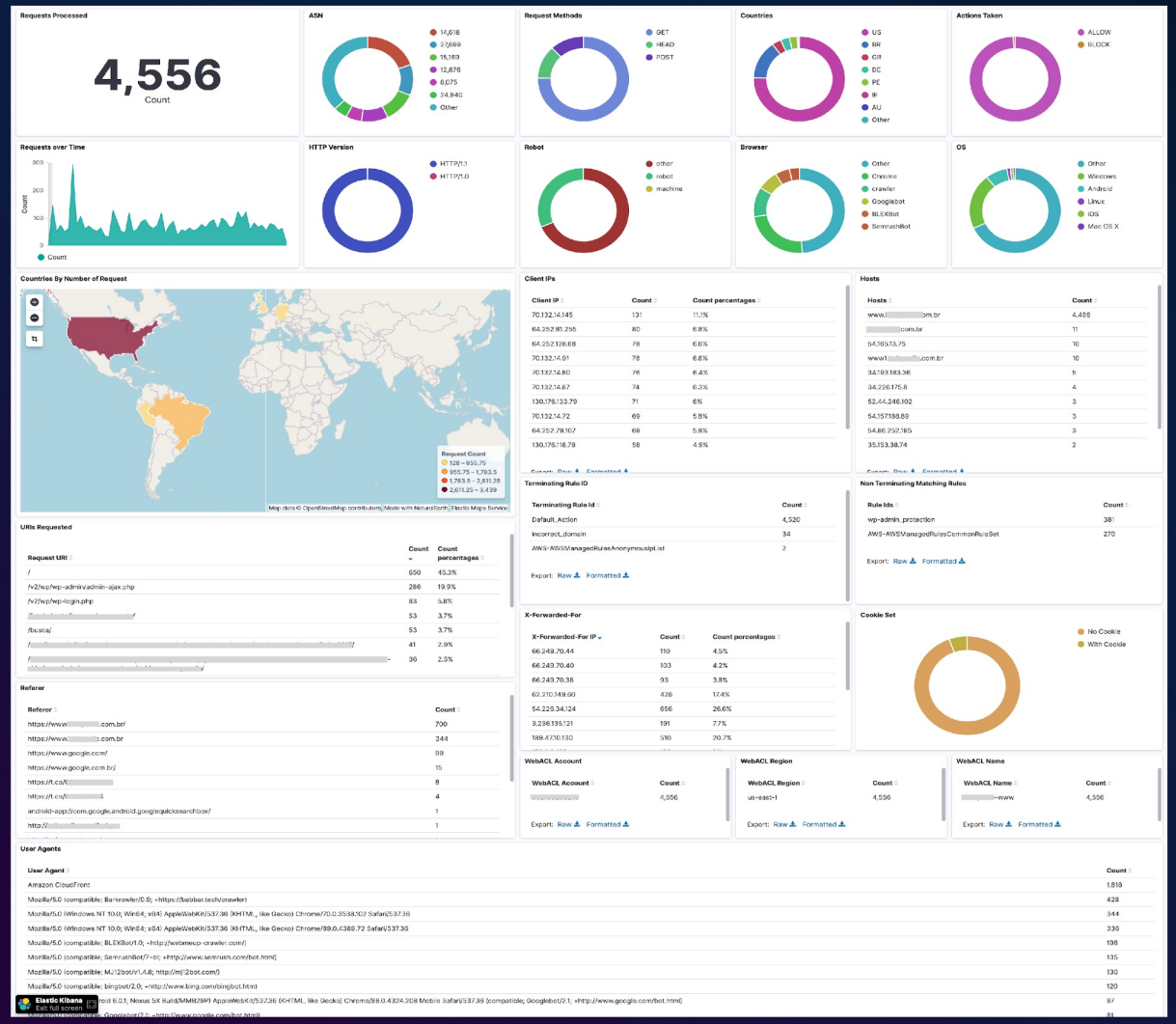
AWS WAF 모니터링 쉽게 하기



준 실시간 모니터링을 하지 않을 경우
S3 + QuickSight + Athena도
가성비 측면에서 효율성이 좋은 조합

단, Firehose 없이
S3로 바로 저장할 경우
5분 단위 저장되므로 갭이 발생하고
로그 사이즈가 커지면
Athena 조회가 상대적으로 느릴 수 있음

AWS WAF 모니터링 쉽게 하기



AWS WAF Operations Dashboards
– Github Repository

Amazon Athena, Amazon QuickSight 를 이용한 AWS WAF Full 로그 분석
– AWS Security Blog

테라폼으로 WAF 변경 히스토리 관리

- 변경 포인트를 한 눈에 인지
- Git과 결합해서 버전관리
- 적용 전에도 변경 포인트 확인 가능

- 알 수 없는 변경 포인트
- 정책 변경 버전관리 어려움
- 적용하기 전에는 알 수 없는 변경점

AWS WAF IP set 업데이트 간편하게 하기

AWS WAF
IP set 업데이트
Lambda Function
코드 (python)

Lambda Function URL을 활용해서
WAF에 정책 추가하는 API 생성 가능

Slack / Grafana 의 ALERT 메시지에서
Lambda Function 호출할 수 있도록
자동화 된 차단 구현 가능

연동으로 WAF에서 응답 기반으로
차단을 구현 가능

Thank you!