AWS 보안!

시작하는 엔지니어를위한..(텅장을 지키는 보안)

2022년 7월 19일(화) 19:00

장소 구트아카데미 (구로소모임)

발표 Linuxer - 정태환

CONTENTS

부동산도 배우고 주식도
배우는데 AWS 계정 지키
는 법은 왜 안 배우나요?

01 망한 텅장들...

"해킹당한 사례를 가져와 봤어요."

주제 1

AWS 해킹 당해서 사용료 3억이 넘게 나왔습니다.

URL - https://www.clien.net/service/board/park/17225662 (원글은 삭제되어 펌글만 남음)

주제 2

저에겐 2174만원이 없습니다.

URL - https://velog.io/@gmtmoney2357/aws-저에겐-2174만원이-없습니다.-해킹과금

주제 3

AWS 해킹 당한 경험담과 과금 대처 가이드 라인

https://m.blog.naver.com/awesomedev/220716804533

01 해킹시 대처 방안

발단

국제 전화 혹은 등록된 이메일로 연락이 오게됨

사실 확인

청구서에 적힌 금액을보고 현실을 부정함

서비스 삭제

이미 메일로는 이상 감지에 대한 내용과 리소스에 대한 삭제를 요구함

일단비세요

고객센터는 친절하고 번역기 지원하고 정안되면 한글로라도

보안조치

몇가지 보안조치를 진행하고 사례 검토를 받는다

살려주세요

1회성으로는 가끔봐주는데 금액이 너무 크면 그또한 어려워질수 있음

이런 번거로운 일을 겪지 않으려면?

02 MFA 부터 AWS CONFIG까지

NO.1	Root Account 에서 MFA 사용하기
NO.2	IAM User 사용하기 With MFA
NO.3	Role Change and Policy
NO.4	Budget 생성
NO.5	AWS Trusted Advisor
NO.6	AWS Config

"처음엔 어렵지만,
이것만 알아도 텅장을 지
킬수 있다구!"

03 IAM Identity and Access Management

서비스

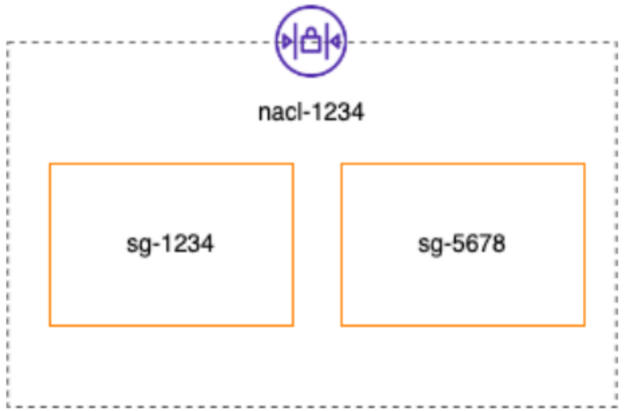
AWS 의 인증 서비스
디렉토리 구조

역할

AWS Identity and Access Management(IAM)은 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
IAM을 사용하여 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)된 대상을 제어

03 SG & NACL Identity and Access Management

구성도



용도

NACL은 서브넷 기반의 Stateless 포트 방화벽
SG는 ENI기반의 Stateful 포트 방화벽

Stateless 와 Stateful 그리고 적용대상의 차이로 응용과 사용 범위가 제한됨

sgr-0ffbb1e6b607a...	–	SSH	TCP	22	sg-09637670b85d847...	20220719_test
sgr-092deb103ca1...	IPv4	HTTP	TCP	80	0.0.0.0/0	–

03 WAF Web Application Firewall

서비스

AWS 관리형 WAF
AWS CloudFront / ALB
AWS 리소스 레벨에서 동작

역할

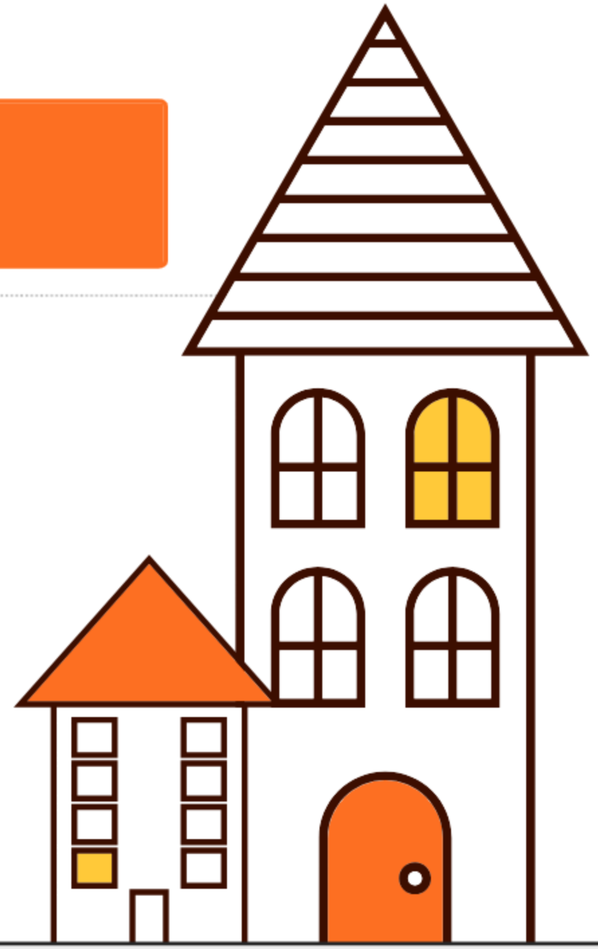
AWS WAF는 굉장히 범용적인 룰을 관리형 룰로 생성하여 제공
가격이 매우 저렴한 편이며 널리 알려진 공격형태를 차단하기에 적합.
서드파티 룰도 사용가능하며, 서드파티 룰은 별도의 비용발생.

04 제로트러스트 현대적 보안 - 안드로메다 토끼

https://andromedarabbit.net/현대적-보안

현대적 보안이 아닌것

1. 다양한 데이터스토어를 무시하고 RDBMS만 중요 자산으로 취급한다
2. 전통적인 솔루션 IPsecVPN 등과 같은 기술만 신뢰하고 새로운 기술은 불신한다.
3. 망의 경계를 기준으로 사고한다. 망 분리의 목적보다 수단에 집착한다.
4. 폐쇄망이 개방망보다 안전하다고 믿는다
5. 보안 조직이 감사 권한을 권력이라 착각하고 이를 행사하는데 심취한다.
6. 개발 조직이 보안 조직을 경멸하고 백도어를 확보하려 한다.



04 제로트러스트 현대적 보안 - 안드로메다 토끼

https://andromedarabbit.net/현대적-보안

현대적 보안 이란?

1. 누구도 믿지 말라 - IAM,MFA,IP제한은 시작점. 시스템과 개인 모두를 검증하라
2. 동기화 된 실패를 피하라 - 무조건 신뢰보다는 상호검증이 필요,무조건 통합관리하는 편의주의 탈피
3. SaaS를 활용하라 - Okta 와같은 IDP를 보안체인안에 넣으면 서드파티 서비스부터 뚫어야 한다.
4. 물은 거꾸로 흐르지 않는다 - 빌드 서비스가 운영환경으로 직접 배포하지 않아야 한다. push -> pull
5. 권한보다 합의와 시스템이다. - 결제를 통한 권한부터 시스템에서 합의로 승인하는 구조로.
6. 상상력과 영감을 믿자 - 과거의 보안방식을 탈피하고 원인을 제거 방식으로 변경
7. 상부상조하자 - devops 개념이 나온이유는? 그리고 Devsecops

04 제로트러스트

현대적 보안은 잘 정리 된 이론은 아니다.

“질 문”

!!!!!주세요!!!!!

INFRASTRUCTURE ENGINEER

“MILLIE”

Login