




# AWS EC2 클라우드의 보안



## 대형 클라우드 사건 분석했더니, 클라우드 보안의 핵심은 '넓은 영역'과 '빠르게'

“ 2020년부터 2022년 사이에 발생한 클라우드 관련 사이버 공격들에는 몇 가지 공통점이 존재한다. 그 중 가장 중요한 건 '충분히 막을 수 있던 사건'이라는 것이다. 순전히 사용자 편에서의 실수 때문에 발생한 클라우드 사건들이 전체 사고에서 큰 비중을 차지하고 있으며, 심지어 그 실수들이라는 것도 대단히 사소하고 허무한 것들이 대부분이다.”

[https://m.boannews.com/html/detail.html?tab\\_type=1&idx=123662](https://m.boannews.com/html/detail.html?tab_type=1&idx=123662)



1) 파이토치(PyTorch) : 2022년 12월, 한 공격자가 PyPI 코드 리포지토리를 활용해 악성 파이토치 디펜던시가 피해자의 시스템의 다운로드 되도록 유도했다. 이 악성 디펜던시에는 시스템 데이터를 훔치는 멀웨어가 포함되어 있었다.

2) 메디뱅크(MediBank) : 2022년 11월 미리 확보한 정상 로그인 크리덴셜을 가지고 공격자들이 메디뱅크라는 의료 기관의 내부 시스템에 불법적으로 접근하는 데 성공했다. VPN 접근과 관련된 데이터를 훔쳤을 가능성도 제기됐다. 공격자들은 약 한 달 동안 표적의 시스템에 조용히 머무르며 공격의 피해를 최소화 했다. 하지만 은행 측은 공격자들과의 협상에 응하지 않았다. 공격자들은 병원의 데이터를 다크웹에 공개했다.

3) 알리바바와 상하이 공안 : 2022년 7월, 알리바바 클라우드 서버가 잘못 설정된 채로 인터넷에 고스란히 공개되는 일이 발생했다. 이미 1년 넘게 그 상태로 서버가 유지된 상황이었다.

4) 오누스(ONUS) : 2021년 12월 베트남 최대 암호화폐 거래 기업에 있었던 로그4j(Log4j)의 취약한 버전을 공격자들이 발견해 익스플로잇 하는 데 성공했다. 이 사건으로 공격자들은 200만이 넘는 고객 개인정보를 가져가는 데 성공했다. 고객의 이름과 이메일 주소, 전화번호, 비밀번호, 거래 내역 등이 여기에 포함됐다.

5) 펠로톤(Peloton) : 2021년 5월, 승인 과정을 거치지 않은 펠로톤 사용자가 다른 펠로톤 사용자들의 민감한 정보와 개인 식별 정보를 열람할 수 있다는 사실이 발견됐다. 펠로톤 장비를 통해 저장되는 각종 기록과 통계 자료들도 포함된 얘기였다. 사용자가 계정을 비밀 모드로 전환을 한다 해도 이 공격을 막을 수 없었다.

6) 에퀴닉스(Equinix) : 2020년 9월 데이터센터 전문 업체인 에퀴닉스에서 랜섬웨어 공격이 발생했다. 공격자들은 에퀴닉스의 내부 시스템들에도 침입하는 데 성공했고, 이를 통해 여러 정보를 가져간 뒤 회사 측에 450만 달러를 요구했다.



## AWS EC2란

- AWS의 컴퓨터를 빌려서 쓰는 것
- Elastic Compute Cloud의 약자
- IaaS



## 다른 종류의 클라우드 컴퓨팅

- 컴퓨터에 소프트웨어를 설치하고 대신 운영해주는 방향으로 확장
- 서버 컴퓨터에 소프트웨어를 구성하고 운영하는 것은 어렵고 위험하기 때문
- SaaS ...



## EC2에 환경을 구축하는 것이 어려운 이유

- 데이터 베이스 등은 정지, 해킹 등에 위험하기 때문
- IDS/IPS와 웹 WAF 등을 사용하는 환경을 빌리는 것이 효율적

## AWS에서 제공하는 보안기능



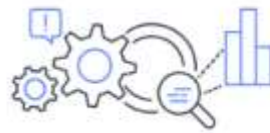
ID



방지



탐지

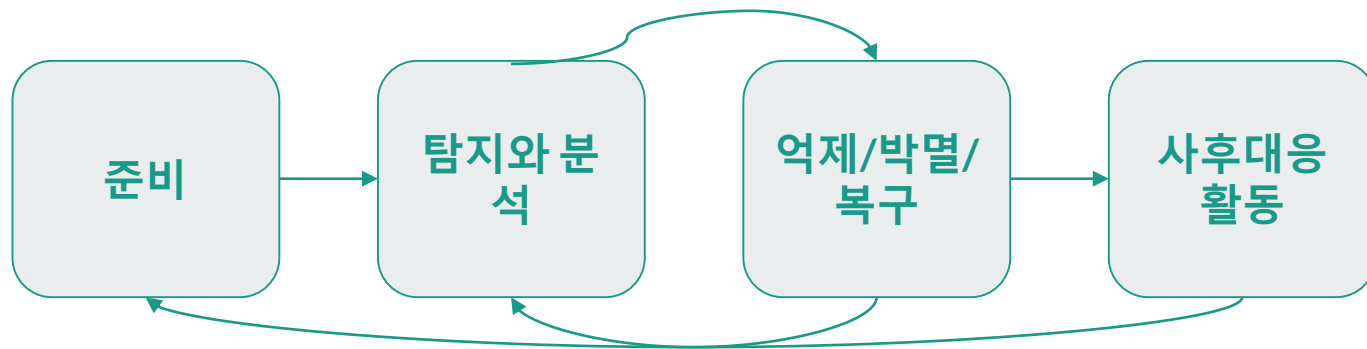


대처



해결

## 침해사고 대응 NIST 모델(참조)







## AWS의 NIST 프레임워크 5가지 요소

식별

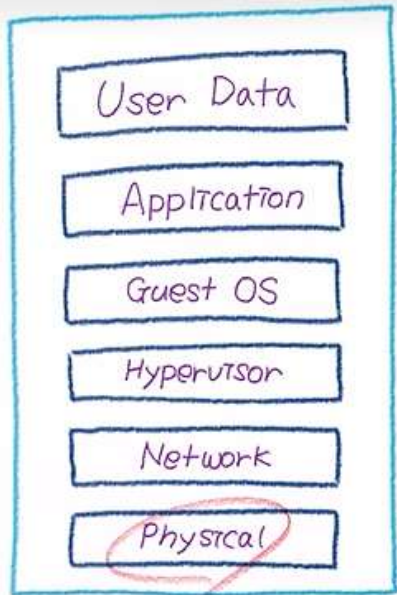
보호

탐지

대응

피드백

## AWS에서의 보안 책임

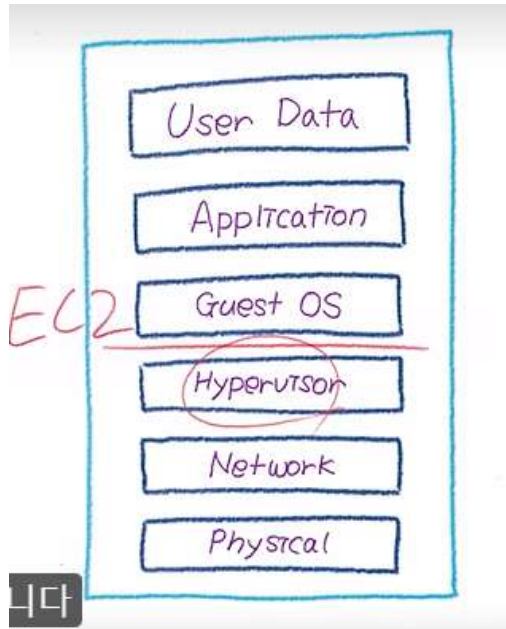


AWS에서는 보안을 AWS와 고객의 공동책임이라고 명시하고 있음.

따라서 스택 구조에 따라, 특정 부분은 AWS의 책임, 특정 부분에 대해서는 고객의 책임으로 정의하고 있다.

AWS에서는 보안이 어떻게 구성되어 있는지 밝히지 않는다. 대신 어떠한 인증을 받았는지 공개되어 있다.

## AWS에서의 보안 책임



해당 스택 구조에서 Hypervisor와 Guest OS를 구분하는 선이 있다. 이 선상 위에서는 AWS는 어떤 일이 일어나는지 알아낼 방법이 없다.

이 구분선 아래에서는 AWS는 모든 책임이 있고 구분선 위에서는 고객이 모든 책임이 있다.



## AWS에서 AWS의 보안 책임

- 규정상 공개 불가
- 알려진 방안 중 하나로는 인스턴스를 삭제 시 데이터를 모두 0으로 스크러빙 하는 방법을 사용



## EC2 환경에서의 사용자의 보안 조치

- 인스턴스에 연결되는 자격 증명 관리
- 네트워크 액세스 제어
- 업데이트 및 보안 조치
- IAM의 역할 및 역할 권한 구성



## IAM이란

- Identity and Access Management(IAM)
- AWS 리소스에 안전하게 접근할 수 있는 웹 서비스이다.
- IAM을 통해 인증 및 권한이 부여된 대상을 중앙에서 제어할 수 있다.



## EC2와 함께 사용 가능한 서비스

- S3 스토리지
- Dynamo DB
- EC2 인스턴스를 생성하고 위 서비스를 연동하는 방식으로 작동한다.



## IAM을 통한 관리

- IAM을 통해 사용자를 생성하고 사용자에게 S3, DB 등에 권한을 부여할 수 있다.
- 부여된 권한 이외의 작업은 할 수 없고, 특정 시간만 이용 가능하게하는 등의 보안조치가 가능하다.





# AWS CloudTrail

- AWS계정에서 일어난 활동들이 AWS CloudTrail에 기록된다.
- 이를 통해 데이터 이벤트를 로깅할 수 있다(기본적으로 AWS는 데이터와 Insight를 로깅하지 않는다)



## 데이터 이벤트와 인사이트 이벤트

- 데이터 이벤트는 리소스 내에서 발생하는 이벤트를 의미한다
- 인사이트 이벤트는 비정상 API호출, 비정상 활동 등을 파악한다.



## 보안 설정

- 데이터 이벤트와 인사이트 이벤트는 기본적으로 로깅되지 않기 때문에 로깅하도록 해야한다.
- 이는 CloudTrail에서 가능하다.



## 오픈소스 취약점 진단 프레임워크

- 오픈소스 취약점 진단 프레임워크를 EC2 상에 올려서 서비스한다.
- SECaaS의 일종으로 활용할 수 있다.