보안 관련 서비스

AWS를 시작하기 위한 첫 걸음

1. 정보 보안 3대 요소
    - 정보 보안: 저장한 정보를 안전하게 보호하는 것
    - 정보 보안의 3대 요소
        - **기밀성:** 정보가 유출되지 않도록 관리
        - **무결성:** 정보가 손상되거나 손실되지 않고 최신의 상태인 것
        - 가용성: 정보를 언제나 사용할 수 있게 하는 것
    - **관리하는 정보를 인가된 사람만이(기밀성) 손상되지 않은 상태에서(무결성) 필요할 때(가용성) 사용할 수 있어야 한다는 것**

2. 다양한 서비스를 결합해 정보를 보호하는 AWS
    - 온프레미스 환경
        - 데이터 센터와 계약한 뒤 할당받은 랙(Rack)에 자신의 서버를 설치
        - 서버의 취약점을 이용하는 것이 아니라면 서버 탈취, 문제 발생 가능성 0에 수렴
    - **클라우드 서비스(AWS)**
        - 전체 권한을 가진 root 계정이 노출되면 악의를 가진 사용자로 인해 악용 가능
        - 따라서 root 계정은 처음 설정때만 사용하고 2FA를 설정해 보안 강화 필요
        - 별도 계정 생성해 사용자별로 권한을 나누고 각 사용자도 반드시 2FA를 이용하도록 정책을 만들어야 함
        - AWS에서는 IAM이라는 서비스에서 이러한 설정 관리 가능
    - AWS가 보안상 더 위험하다고 생각할 수 있지만 AWS의 보안 서비스를 이용해 관리하면 온프레미스와 동등하거나 그 이상으로 안전하게 관리 가능

AWS를 안전하게 사용하기 위한 IAM

1. AWS Identity and Access Management란
    - AWS를 사용하는 계정 권한 관리 서비스
    - AWS 서비스의 조작 제어는 모두 IAM으로 관리

2. IAM 사용자, IAM 그룹
    - IAM 사용자
        - 사용자가 AWS 조작을 위해 사용하는 것
        - 비밀 번호 등의 인증 정보를 사용해 로그인 시 IAM 사용자에게 할당된 권한 사용 가능
        - 관리 콘솔에서 여러 조작 가능, 액세스 키라는 인증 정보 발행해 권한 사용 가능
    - IAM 그룹
        - IAM 사용자는 해당 그룹에 설정된 권한 사용 가능
        - 여러 사용자가 동일한 권한을 갖도록 관리해야 할 때 유용하게 사용 가능

3. IAM 정책
    - 어떤 서비스의 기능에 어떤 조작을 할 수 있는 지와 같은 권한 설정
    - 동일한 권한 설정해야 하는 경우 재 사용 가능
    - 단일 IAM 사용자, IAM 그룹이나 IAM 역할에 여러 IAM 정책 연결 가능
    - **AWS 관리형 정책:** 서비스나 기능 추가 시 자동으로 관련 권한 추가

      고객 관리형 정책: 사용자가 만든 IAM 정책

4. IAM 역할
    - 사용자 생성 시 액세스 키 생성 가능
    - **액세스 키**
        - CLI로 AWS 자원 조작, 프로그램 제어 시 사용하는 인증 정보
        - 고정 문자열, AWS 계정과 동일한 권한 → 유출 시 보안 위협 노출 가능
    - 따라서 AWS 서비스에 권한 부여 시 IAM 역할 사용 권장

- 서비스에 해당 서비스를 사용할 수 있는 사용자를 지정하는 것 → 권한 부여X → 더 안전
- **Role Switch:** IAM 역할만 생성하고 사용자가 필요할 때만 역할을 부여해 적절한 권한으로 작업할 수 있게 설정

계정 내 작업 이력 기록

1. AWS CloudTrail이란
   - AWS 계정을 만들 때부터 자동으로 모든 작업을 기록하는 서비스
   - 관리 콘솔, 프로그램, AWS 서비스에서 수행한 모든 작업 기록
   - 사용자의 악의적인 조작, 프로그램 문제로 발생한 설정 변경 등 조사 가능
   - **Trail(트레일)**
     - S3에 별도로 저장하는 로그 파일
     - 암호화되어 보관
     - 문제 발생 시 당시 조작 기록 증명을 위한 중요 기록

2. 기록되는 내용
   - 관리 콘솔과 API를 통한 조작 이력 저장, 이 외는 기록되지 않음
   - 관리 이벤트
   - 데이터 이벤트
   - 인사이트 이벤트

3. 트레일 출력
   - **로그를 트레일해 S3나 CloudWatch Logs로 출력 가능 → 저장 비용 발생, 무기한 저장 가능**
   - S3
     - 파일 형태 저장
     - 저장한 파일의 무결성 검사 파일(다이제스트 파일) 출력 가능
   - CloudWatch Logs

- 스트림 형식 저장
  - 스트림: 로그의 내용이 순차적으로 저장되는 것
- 로그 내용을 확인하고 특정 문자열을 찾을 때 이벤트를 발생시키는 기능 존재

  → 특정 조작 발생 시 사용자에게 알림

설정 내역 및 설정 내용 자동 관리

1. 설정 이력을 저장하는 AWS Config
   - AWS 자원에 대한 구성 정보와 변경 이력 기록 서비스
   - 활성화 시 자동으로 구성 정보 수집, 이력 관리 가능
   - AWS 자원의 설정 내용 기반으로 이력 저장
   - **고급 쿼리:** 특정 자원 수 확인 가능

2. 설정을 확인하는 AWS Config 규칙
   - 규칙 4가지
     - EBS가 암호화되어 있는가
     - CloudTrail이 사용 설정되어 있는가
     - S3 버킷이 공개적으로 읽고 쓸 수 없는가
     - 보안 그룹에 SSH 포트(22번)가 공개적으로 게시되지 않았는가
   - **AWS 관리형 규칙:** AWS에서 제공하는 규칙

     사용자 지정 규칙: 사용자가 만드는 자신만의 규칙
   - Amazon EventBridge, Amazon SNS와 결합해 규칙 미준수 자원 발견 시 알림 가능
   - 미준수 리소스 자동 수정 기능 존재

     → AWS Systems Manager라고 하는 서비스의 Automation 이용

AWS 작업 내용 감시

1. 지능형 위협 탐지 서비스 Amazon GuardDuty

- AWS 계정 내 모든 활동을 감시하는 위협 탐지 서비스
- 탐지 내용 예시
  - 루트 사용자 사용
  - IAM 액세스 키가 대량 사용됨
  - EC2가 DDoS 공격을 위한 좀비 PC가 됐을 가능성
- **CloudTrail, VPC 흐름 로그 및 DNS Logs의 세 가지 정보 기반으로 탐지 수행**
- **기계학습**으로 이용 패턴을 학습해 루트 사용자로 로그인하는 행위 탐지, 다른 사용 패턴으로 조작하는 경우도 탐지 가능

웹 응용 프로그램 보안 강화

1. 웹 응용 프로그램을 보안 위협으로부터 보호
   - 방화벽
     - 특정 IP로부터의 접속이나 서버의 특정 포트에 대한 접속을 허가하거나 금지
     - 네트워크나 서버로의 침입 방지 가능
     - 인터넷과 서버 사이에 위치해 인터넷을 통해 서버로 전송되는 통신 제어
   - **웹 방화벽(Web Application Firewall, WAF)**
     - 웹 응용 프로그램의 취약점에 대한 공격 탐지, 방어
     - 요청에 포함된 공격 코드를 탐지해 방어

2. 간단하게 적용 가능한 AWS WAF
   - AWS가 제공하는 관리형 보안 서비스
   - 웹 접근 통제 목록(웹 ACL)이라는 자원으로 요청에 대한 제어 규칙 생성, 적용 → WAF 사용
   - 사용자는 WAF 규칙만 설정하면 됨
   - **WAF 규칙**
     - IP 제한, 정규 표현식 필터링
     - AWS가 제공하는 관리형 규칙 활용 가능

    - 일반적인 공격 기술(SQL 인젝션, 크로스 사이트 스크립팅)에 대한 WAF 규칙도 포함
- AWS가 제공하는 관리형 규칙 그룹에는 기본적인 공격 방어 규칙 준비

  → 더 복잡한 공격에 대한 방어에는 서드파티 도구 도입

시스템 보안을 강화하는 6가지 서비스

1. AWS Network Firewall: VPC를 통한 통신에 대한 방화벽 역할
2. Amazon Inspector: 취약점 관리 서비스, 자동으로 취약점 평가 수행 가능
3. AWS Shield: 별도의 설정 없이 자동 적용, DDoS 공격으로부터 보호
    - DDoS: 분산 서비스 거부 공격
    - EDoS: 경제적 손실을 목적으로 한 DDoS 공격
4. AWS Security Hub: 전체 AWS 계정에 대해 보안 모범 사례 확인
5. AWS Cognito: 웹 응용 프로그램이나 모바일 앱의 사용자 인증 및 권한 부여를 위한 서비스
6. AWS Directory Service: AWS가 제공하는 Active Directory 서비스