**1. 가능한 공격 기법**

**1.1. DeleteObject를 이용한 파일 삭제**

* **시나리오**:
  + 공격자가 S3 버킷에 저장된 데이터를 삭제.
  + CloudTrail 로그에 eventName: DeleteObject로 기록됩니다.
* **방법**:
  + 공격자는 S3 API를 통해 DeleteObject 요청을 실행.
  + 이 작업을 위해 AWS Access Key와 Secret Key가 필요하며, 권한(s3:DeleteObject)이 있어야 합니다.
* **결과**:
  + S3 버킷에서 지정된 파일이 삭제되고, 로그에 기록됨.

**1.2. 허가되지 않은 IP 주소에서 접근**

* **시나리오**:
  + 공격자가 AWS 계정의 자격 증명을 획득한 뒤, 허가되지 않은 IP 주소에서 AWS 리소스에 접근.
  + CloudTrail 로그의 sourceIPAddress 필드에 비정상적인 IP가 기록됩니다.
* **방법**:
  + AWS Access Key와 Secret Key를 사용해 허가되지 않은 위치에서 S3 API 호출(GetObject, PutObject, DeleteObject 등).
  + VPN이나 프록시를 사용해 IP 주소를 변조 가능.
* **결과**:
  + 데이터 접근 로그가 기록되며, 공격 시도가 남음.

**1.3. 권한 에스컬레이션**

* **시나리오**:
  + 공격자가 IAM 사용자나 역할의 권한을 변경하거나 추가 권한을 획득.
  + CloudTrail 로그에 eventName: PutUserPolicy, AttachUserPolicy 등으로 기록됩니다.
* **방법**:
  + 기존의 자격 증명으로 IAM 정책을 수정하여 더 높은 권한 획득.
* **결과**:
  + 공격자가 S3 버킷 데이터 삭제, 리소스 생성/삭제 등 높은 권한의 작업 수행.

**2. 방어 전략**

**2.1. DeleteObject 공격 방어**

1. **S3 버킷 정책 강화**:
   * 파일 삭제를 특정 사용자나 역할로 제한:}
2. **버전 관리 활성화**:
   * S3 버킷에서 버전 관리를 활성화하면 삭제된 파일도 복원 가능.
3. **CloudWatch 알림 설정**:
   * DeleteObject 이벤트가 감지되면 알림을 보내거나 자동으로 차단.

**2.2. 허가되지 않은 IP 공격 방어**

1. **VPC 엔드포인트 사용**:
   * S3 버킷을 특정 VPC에서만 접근 가능하도록 설정.
2. **IAM 정책에 IP 주소 조건 추가**:
   * 특정 IP만 접근 가능하도록 제한:

{

**CloudTrail 데이터 이벤트 활성화**:

* + S3 데이터 액세스 이벤트를 모니터링하고 비정상 IP를 탐지.

**2.3. 권한 에스컬레이션 방어**

1. **IAM 최소 권한 원칙 적용**:
   * 사용자나 역할에 필요한 최소한의 권한만 부여.
2. **CloudTrail 로그 모니터링**:
   * AttachUserPolicy, PutUserPolicy와 같은 IAM 정책 변경 이벤트를 감지.
3. **AWS Config 규칙 활용**:
   * IAM 정책 변경 시 알림을 받거나 비정상적인 변경을 자동으로 되돌림.

**3. 모의 공격 기법 구현**

**3.1. Python을 사용한 파일 삭제 모의 공격**

**3.2. 허가되지 않은 IP 접근 모의 공격**

VPN 또는 프록시를 사용해 지정된 IP가 아닌 다른 IP에서 AWS API 호출을 시도.

**3.3. 권한 변경 모의 공격**

IAM 사용자에 권한을 추가하는 시뮬레이션