위협항목 리스트

소 속	BoB 9 기 디지털포렌식트랙
팀 명	Cloud?Kloud!
작성 일자	2020.12.18

목 차

1. 위협항목 리스트

- CK에서 선정한 서비스 별 위협항목 및 위험도 목록입니다.

서비스	항목 번호	항목명	위험도
IAM	1	침투 테스트 시스템(Kali, Pentoo, Parrot)에서 API 호출	Medium
	2	네트워크 액세스 권한 변경 (보안그룹, 라우트, ACL)	Medium
	3	CloudTrail 로깅 중단, 기존 로그 삭제	Medium
	4	IAM 사용자, 그룹 정책 등 추가/변경/삭제	Medium
	5	리소스 보안 액세스 정책 변경	Medium
	6	루트 계정으로 API 호출	Low
	7	컴퓨팅 리소스 시작	Low
S3	8	버킷 목록 검색	Low
	9	S3 데이터 생성	Low
	10	S3 데이터 삭제	Medium
	11	권한이 없는 IAM 개체의 S3 API 호출	Medium
	12	서버 액세스 로깅 비활성화	Medium
	13	버킷 또는 객체 권한 변경	Medium
	14	버킷 정책 변경	Medium
	15	침투 테스트 시스템(Kali, Pentoo, Parrot)에서 API 호출	Medium
RDS	16	DB 목록 검색	Low
	17	DB 내의 데이터 삭제	Medium
	18	DB 사용자 추가	Medium
	19	DB 사용자 권한 변경	Medium
	20	권한이 없는 IAM 개체의 RDS API 호출	Medium
	21	RDS 로깅 비활성화(파라미터 그룹 수정)	Medium
	22	RDS 로깅 비활성화(파라미터 그룹 삭제)	Medium
	23	DB 중지	Medium
	24	DB 삭제	Medium
	25	침투 테스트 시스템(Kali, Pentoo, Parrot)에서 API 호출	Medium
	26	RDS 로깅 비활성화(CloudWatch 로깅 수정)	Medium
	27	DB 연결 실패	Medium
EC2	28	쉘 명령어 사용(yum)	Low
	29	쉘 명령어 사용(sudo)	Low
	30	쉘 명령어 사용(service)	Medium
	31	쉘 명령어 사용(cron)	Medium
	32	인스턴스 생성, 실행	Low
	33	인스턴스 중지, 삭제	Medium

	34	보안그룹 수정	Medium
	35	침투 테스트 시스템(Kali, Pentoo, Parrot)에서 API 호출	Medium

2. 서비스 별 위협항목 설명

2.1. IAM

1] 침투 테스트 시스템(Kali, Pentoo, Parrot)에서 API 호출

- 선정 이유 : 악의적인 목적을 가진 경우, 침투 테스트 도구를 사용하여 AWS 환경에 대한 무단 액세스 권한을 얻기도 함
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "iam.amazonaws.com"으로 IAM 서비스에서 발생한 로그임을 알 수 있고, userAgent에 "kali"/"parrot"/"pentoo" 문자열이 보이면 해당 시스템에서 접근한 것으로 판단할 수 있다.

2] 네트워크 액세스 권한 변경 (보안그룹, 라우트, ACL)

- 선정 이유 : 공격자가 공격을 위해 다양한 포트에서 특정 인바운드 트래픽을 허용하도록 보안 그룹을 변경하여 EC2 인스턴스에 대한 액세스 능력을 개선하도록 시도하는 경우가 많음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "iam.amazonaws.com"으로 IAM 서비스에서 발생한 로그임을 알 수 있고, eventName에 "CreateSecurityGroup", "DescribeInstances" API가 보이면 해당 위협항목이라 판단할 수 있다.

3] CloudTrail 로깅 중단, 기존 로그 삭제

- 선정 이유 : 공격자가 추후 공격 수행 사실을 들키지 않기 위해 로깅을 중단하거나 기존 로그를 삭제했을 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "iam.amazonaws.com"으로 IAM 서비스에서 발생한 로그임을 알 수 있고,

eventName에 "StopLogging" API가 보이면 해당 위협항목이라 판단할 수 있다.

4] IAM 사용자, 그룹 정책 등 추가/변경/삭제

- 선정 이유 : 액세스 포인트가 닫혀 있어도 공격자는 도난된 자격 증명을 사용하여 공격을 위해 사용자 생성, 그룹 정책 추가, 권한 변경 등의 행위를 할 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "iam.amazonaws.com"으로 IAM 서비스에서 발생한 로그임을 알 수 있고,

eventName에 "CreateSecurityGroup", "DescribeInstances" API가 보이면 해당 위협항목이라 판단할 수 있다.

5] 리소스 보안 액세스 정책 변경

- 선정 이유 : 자격 증명이 도난된 경우 공격자가 리소스 정책을 변경하여 해당 리소스에 대한 액세스 권한을 얻을 수 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "iam.amazonaws.com"으로 IAM 서비스에서 발생한 로그임을 알 수 있고,

eventName에 "PutBucketPolicy" API가 보이면 해당 위협항목이라 판단할 수 있다.

6] 루트 계정으로 API 호출

- 선정 이유 : AWS 루트 계정은 AWS의 모든 리소스에 제한없이 접근이 가능하며 사용 권한을 제한할 방법이 존재하지 않음. 그러므로 루트 계정에 대한 액세스 키를 생성하지 않는 것이 좋으며, 루트 계정의 사용을 자제하여야 함
- 위험도 : Low
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "iam.amazonaws.com"으로 IAM 서비스에서 발생한 로그임을 알 수 있고,

userIdentity.type이 "Root"면 해당 위협항목이라 판단할 수 있다.

7] 컴퓨팅 리소스 시작

- 선정 이유 : 공격자가 도난된 자격 증명을 사용하여 컴퓨팅 리소스를 시작하여 채굴 또는 암호 크래킹을 할 가능성이 있고, 또한 공격자가 EC2 인스턴스와 그 자격증명을 사용하여 계정 액세스를 유지하는 신호일 수 있음
- 위험도 : Low
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "iam.amazonaws.com"으로 IAM 서비스에서 발생한 로그임을 알 수 있고,

eventName에 "RunInstances" API가 보이면 해당 위협항목이라 판단할 수 있다.

2.2. S3

8] 버킷 목록 검색

- 선정 이유 : 공격자가 정보를 수집하여 AWS 환경이 더 광범위한 공격에 취약해졌는지 확인하는 공격의 검색 단계와 관련되어 있음
- 위험도 : Low
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "s3.amazonaws.com"으로 S3 서비스에서 발생한 로그임을 알 수 있고, eventName에 "ListObjects" API가 보이면 해당 위협항목이라 판단할 수 있다.

9] S3 데이터 생성

- 선정 이유 : 악의적인 목적을 가진 공격자의 경우, 공격을 위한 파일이나 과금을 위한 대용량의 데이터를 업로드했을 가능성이 있음
- 위험도 : Low
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "s3.amazonaws.com"으로 S3 서비스에서 발생한 로그임을 알 수 있고, eventName에 "PutObject" API가 보이면 해당 위협항목이라 판단할 수 있다.

10] S3 데이터 삭제

- 선정 이유 : 악의적인 목적을 가진 공격자가 중요한 데이터를 임의로 삭제했을 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "s3.amazonaws.com"으로 S3 서비스에서 발생한 로그임을 알 수 있고, eventName에 "DeleteObjects" API가 보이면 해당 위협항목이라 판단할 수 있다.

11] 권한이 없는 IAM 개체의 S3 API 호출

- 선정 이유 : 이미 공격자가 공격에 성공하여 데이터 유출 단계일 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "s3.amazonaws.com"으로 S3 서비스에서 발생한 로그임을 알 수 있고, eventName에 "ListObjects" API가 보이고, 로그에 "errorCode":"AccessDenied"가 보이면 해당 위협항목이라 판단할 수 있다.

12] 서버 액세스 로깅 비활성화

- 선정 이유 : 공격자가 추후 공격 수행 사실을 들키지 않기 위해 로깅을 비활성화했을 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "s3.amazonaws.com"으로 S3 서비스에서 발생한 로그임을 알 수 있고, eventName에 "GetBucketPublicAccessBlock" API가 보이면 해당 위협항목이라 판단할 수 있다.

13] 버킷 또는 객체 권한 변경

- 선정 이유 : 공격자가 계정 외부에서 정보를 공유할 수 있도록 하기 위해 수행했을 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "s3.amazonaws.com"으로 S3 서비스에서 발생한 로그임을 알 수 있고, eventName에 "PutBucketAcl" API가 보이면 해당 위협항목이라 판단할 수 있다.

14] 버킷 정책 변경

- 선정 이유 : 권한이 없는 사용자들에게 버킷을 공개적으로 액세스 가능하게 할 수 있음

- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "s3.amazonaws.com"으로 S3 서비스에서 발생한 로그임을 알 수 있고, eventName에 "PutBucketPolicy" API가 보이면 해당 위협항목이라 판단할 수 있다.

15] 침투 테스트 시스템(Kali, Pentoo, Parrot)에서 API 호출

- 선정 이유 : 악의적인 목적을 가진 경우, 침투 테스트 도구를 사용하여 AWS 환경에 대한 무단 액세스 권한을 얻기도 함
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "s3.amazonaws.com"으로 S3 서비스에서 발생한 로그임을 알 수 있고, userAgent에 "kali"/"parrot"/"pentoo" 문자열이 보이면 해당 시스템에서 접속한 것으로 판단할 수 있다.

2.3. RDS

16] DB 목록 검색

- 선정 이유 : 공격자가 정보를 수집하여 AWS 환경이 더 광범위한 공격에 취약해졌는지 확인하는 공격의 검색 단계와 관련되어 있음
- 위험도 : Low
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "rds.amazonaws.com"으로 RDS 서비스에서 발생한 로그임을 알 수 있고, eventName에 "DescribeDBInstances" API가 보이면 해당 위협항목이라 판단할 수 있다.

17] DB 내의 데이터 삭제

- 선정 이유 : 악의적인 목적을 가진 공격자가 중요한 데이터를 임의로 삭제했을 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

general 로그에서 "DELETE"나 "delete", "DROP"이 검출된다면 해당 위협항목이라 판단할 수 있다.

18] DB 사용자 추가

- 선정 이유 : 공격자가 많은 권한을 가진 사용자를 추가하여 모든 DB에 접근하여 정보 유출을 할 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

general 로그에서 "CREATE USER"가 검출된다면 해당 위협항목이라 판단할 수 있다.

19] DB 사용자 권한 변경

- 선정 이유 : 공격자가 DB 사용자의 권한을 임의로 변경하여 정보 유출을 할 가능성이 있음

- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

general 로그에서 "GRANT"가 검출된다면 해당 위협항목이라 판단할 수 있다.

20] 권한이 없는 IAM 개체의 RDS API 호출

- 선정 이유 : 이미 공격자가 공격에 성공하여 데이터 유출 단계일 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "rds.amazonaws.com"으로 RDS 서비스에서 발생한 로그임을 알 수 있고, eventName에 "DescribeDBInstances" API가 보이고, 로그에 "errorCode":"AccessDenied"가 보이면 해당 위협항목이라 판단할 수 있다.

21] RDS 로깅 비활성화(파라미터 그룹 수정)

- 선정 이유 : 공격자가 추후 공격 수행 사실을 들키지 않기 위해 로깅을 비활성화 했을 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "rds.amazonaws.com"으로 RDS 서비스에서 발생한 로그임을 알 수 있고, eventName에 "ModifyDBParameterGroup", "ResetDBParameterGroup" API가 보이면 해당 위협항목이라 판단할 수 있다.

22] RDS 로깅 비활성화(파라미터 그룹 삭제)

- 선정 이유 : 공격자가 추후 공격 수행 사실을 들키지 않기 위해 로깅 파라미터 그룹을 삭제했을 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "rds.amazonaws.com"으로 RDS 서비스에서 발생한 로그임을 알 수 있고,

eventName에 "DeleteDBParameterGroup" API가 보이면 해당 위협항목이라 판단할 수 있다.

23] DB 중지

- 선정 이유 : 공격자가 DB를 중지시켜 사용자가 DB 내 데이터를 사용하지 못하게 할 수 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "rds.amazonaws.com"으로 RDS 서비스에서 발생한 로그임을 알 수 있고,

eventName에 "StopDBInstance" API가 보이면 해당 위협항목이라 판단할 수 있다.

24] DB 삭제

- 선정 이유 : 악의적인 목적을 가진 공격자가 중요한 데이터를 임의로 삭제했을 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "rds.amazonaws.com"으로 RDS 서비스에서 발생한 로그임을 알 수 있고,

eventName에 "DeleteDBInstance" API가 보이면 해당 위협항목이라 판단할 수 있다.

25] 침투 테스트 시스템(Kali, Pentoo, Parrot)에서 API 호출

- 선정 이유 : 악의적인 목적을 가진 경우, 침투 테스트 도구를 사용하여 AWS 환경에 대한 무단 액세스 권한을 얻기도 함
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "rds.amazonaws.com"으로 RDS 서비스에서 발생한 로그임을 알 수 있고,

userAgent에 "kali"/"parrot"/"pentoo" 문자열이 보이면 해당 시스템에서 접속한 것으로 판단할 수 있다.

26] RDS 로깅 비활성화(CloudWatch 로깅 수정)

- 선정 이유 : 공격자가 추후 공격 수행 사실을 들키지 않기 위해 로깅 비활성화 및 로깅 수정 했을 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "rds.amazonaws.com"으로 RDS 서비스에서 발생한 로그임을 알 수 있고, eventName에 "ModifyDBInstance" API가 보이면 해당 위협항목이라 판단할 수 있다.

27] DB 연결 실패

- 선정 이유 : 권한이 없는 사용자가 접근하여 연결이 실패한 경우, 사용자가 악의적인 목적을 가진 공격자일 가능성이 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

general 로그에서 "Connect Access denied"가 검출된다면 해당 위협항목이라 판단할 수 있다.

2.4. EC2

28] 쉘 명령어 사용(yum)

- 선정 이유 : 패키지 매니저를 사용하여 패키지를 설치/수정/삭제 할 수 있음
- 위험도 : Low
- 해당 위협항목 발생 시 공통적으로 나타나는 것

yum.log 로그 그룹이나, 쉘 명령어 로그 그룹에서 'yum' 문자열이 들어가는 로그가 검출되면 해당 위협항목이라고 판단할 수 있다.

29] 쉘 명령어 사용(sudo)

- 선정 이유 : 루트 권한을 사용하여 명령어를 수행하기에, 시스템 명령 및 권한이 필요한 것을 수행할 수 있음
- 위험도 : Low
- 해당 위협항목 발생 시 공통적으로 나타나는 것

쉘 명령어 로그 그룹에서 'sudo' 문자열이 들어가는 로그가 검출되면 해당 위협항목이라고 판단할 수 있다.

30] 쉘 명령어 사용(service)

- 선정 이유 : 해당 명령을 통해 시스템 및 유저 서비스를 시작 또는 종료할 수 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

쉘 명령어 로그 그룹에서 'service' 문자열이 들어가는 로그가 검출되면 해당 위협항목이라고 판단할 수 있다.

31] 쉘 명령어 사용(cron)

- 선정 이유 : cron 명령어를 통해 시스템에서 주기적으로 실행할 수 있는 명령 및 프로그램을 지정 가능하여, 이를 통해 시스템에 위해를 가할 수 있음

- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

쉘 명령어 로그 그룹에서 'cron' 문자열이 들어가는 로그가 검출되면 해당 위협항목이라고 판단할 수 있다.

32] 인스턴스 생성, 실행

- 선정 이유 : 특정 인스턴스 생성 및 실행은 과금 및 계정 전반에 영향을 미칠 수 있음. 또한, 공격자가 비트코인을 채굴할 때 도난된 사용자 계정을 이용하여 임의로 Spot Instance를 생성하는 경우가 있음.
- 위험도 : Low
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "ec2.amazonaws.com"으로 EC2 서비스에서 발생한 로그임을 알 수 있고, eventName에 "RunInstances", "StartInstances"가 보일 때 해당 항목이 탐지된다.

33] 인스턴스 중지, 삭제

- 선정 이유 : 특정 인스턴스가 중지 또는 삭제되는 것은 사용자가 서비스 및 데이터 운용 시 큰 손해가 발생할 수 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "ec2.amazonaws.com"으로 EC2 서비스에서 발생한 로그임을 알 수 있고, eventName에 "StopInstances", "TermibateInstances"가 보일 때 해당 항목이 탐지된다.

34] 보안그룹 수정

- 선정 이유 : 보안그룹 수정을 통해 네트워크 접근 권한 등을 변조할 수 있음
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "ec2.amazonaws.com"으로 EC2 서비스에서 발생한 로그임을 알 수 있고,

eventName에 "AuthorizeSecurityGroupEgress", "AuthorizeSecurityGroupIngress"가 보일 때 해당 항목이 탐지된다.

35] 침투 테스트 시스템(Kali, Pentoo, Parrot)에서 API 호출

- 선정 이유 : 악의적인 목적을 가진 경우, 침투 테스트 도구를 사용하여 AWS 환경에 대한 무단 액세스 권한을 얻기도 함
- 위험도 : Medium
- 해당 위협항목 발생 시 공통적으로 나타나는 것

eventSource = "ec2.amazonaws.com"으로 EC2 서비스에서 발생한 로그임을 알 수 있고,

userAgent에 "kali"/"parrot"/"pentoo" 문자열이 보이면 해당 시스템에서 접속한 것으로 판단할 수 있다.