MANDIANT

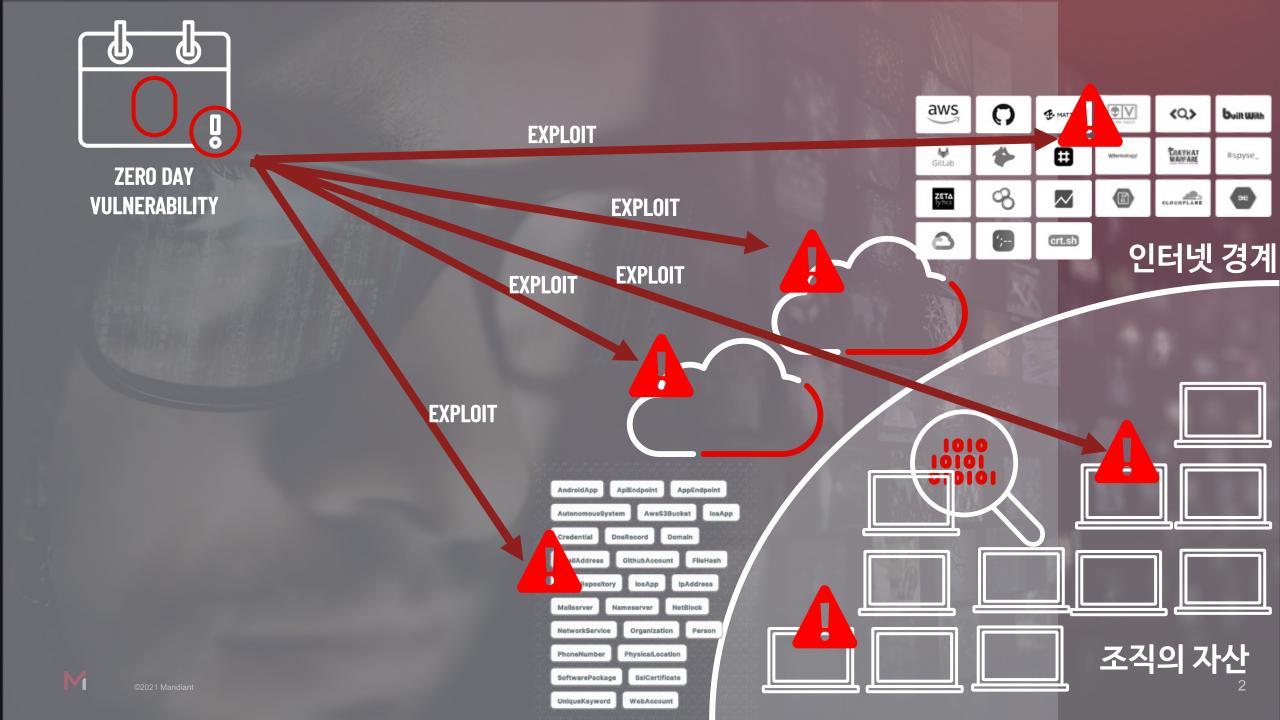
MANDIANT ADVANTAGE

Attack Surface Management

멘디언트 ASM의 주요 특징과 필요성

오진석 기술총괄 상무

Mandiant Senior SE Manager Korea



"We don't know, what we don't know..."



제가 다 알고 있습니다.

아 그거는 잠깐 쓰고 지운다고 했어요

통제가 가능하죠

라떼는 말이야.. 서버는

클라우드 관리 툴 있어요

개인이 쓰겠다는데 그걸 어떻게 확인해요

취약점 컨설팅 정기적으로 받죠

우리 회사는 어플리케이션 종류 많지 않아요

Gartner

ASM은 취약점이 존재하며 인터넷에 노출되어 있는 기업의 자산과 시스템을 발견하고 관리하기 위한 전문적 프로세스와 기술 서비스를 의미합니다.

Forrester

ASM은 최초 검색을 통해서 보안팀과 IT팀이 알고 관리하고 있는 조직의 자산 내용보다 평균 30%가 넘는 클라우드 자산을 발견 했습니다.

ATTACK SURFACE MANAGEMENT (ASM)

Mandiant Advantage - Attack Surface Management 동작 특성

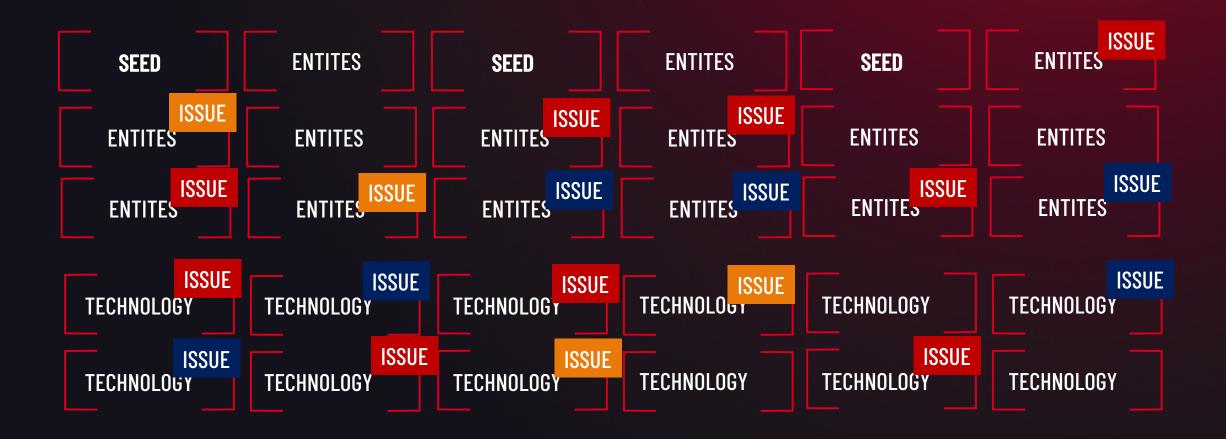
① 자산 확인 (Asset Discover)

MA-ASM 인터넷 접점의 조직 자산 및 개별 구성요소에 대한 식별 확인을 통해 내/외부에 구성되어 외부로 노출된 자산을 정확하게 구분합니다.

② 이슈 분석(Issue Analysis)

자산이 수집되고 발견되면 MA-ASM은 네트워크를 모니터링하여 각 엔티티에 대해 존재하는 이슈를 확인 검증합니다. 이슈에는 CVE, 잘못된 구성, 데이터 유출 또는 위험을 초래하는 모든 문제를 포함 합니다.

COLLECTION



ENTITY & SEED ENTITY

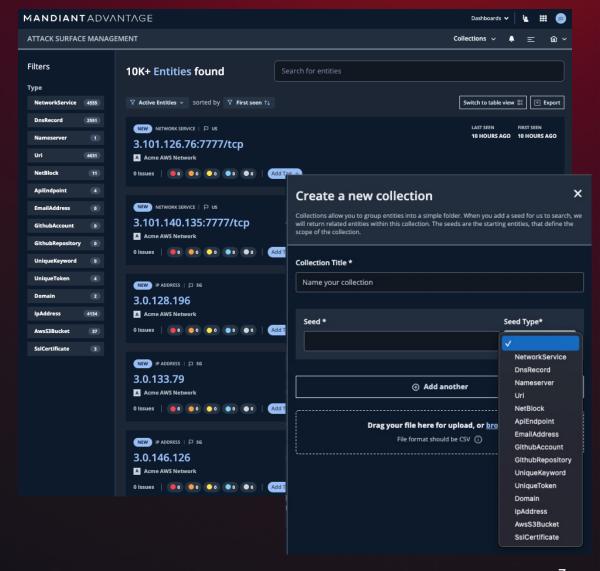
Digital Assets Discovered By MA-ASM

- AWSS3Bucket
- APIEndpoint
- DnsRecord a subdomain or hostname (e.g., example.company.com)
- Domain a top level domain (e.g., company.com)
- EmailAddress
- IpAddress an IPv4 or IPv6 IP address (e.g., 1.1.1.1)
- GithubAccount- a string specifying the name of a public GitHub account
- GithubRepository

(e.g., bobbyjoe)

- NameServer a hostname (e.g., ns1.company.com)
- NetBlock a network block in CIDR format (1.1.1.0/24)

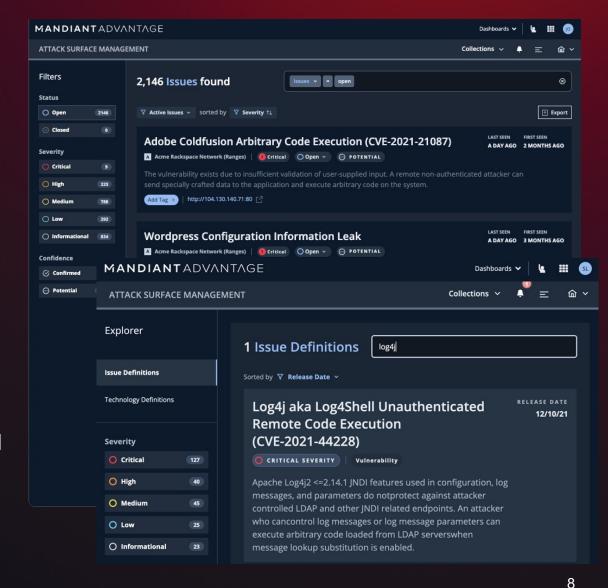
- NetworkService
- SSLCertificate
- UniqueKeywork
- UniqueToken
- URI



ISSUE

Cyber Risks Found In Relation To ENTITYS

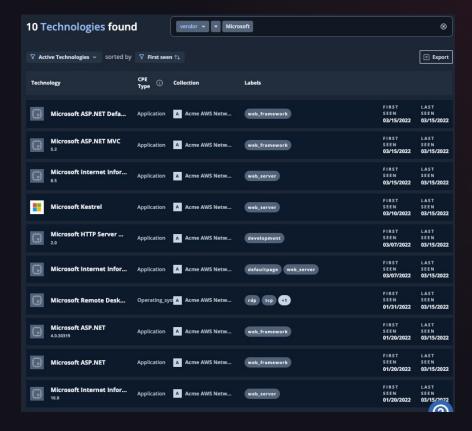
- **Vulnerabilities**
- Misconfigurations
- Indicators of compromise
- Leaks
- **Expired certificates**
- **Exposed development systems**
- Insecure cookies
- Misconfigurations of automated build systems such as Jenkins,
- Microsoft Remote Desktop CVEs
- AWS S3 buckets that are open to writing by the entire world

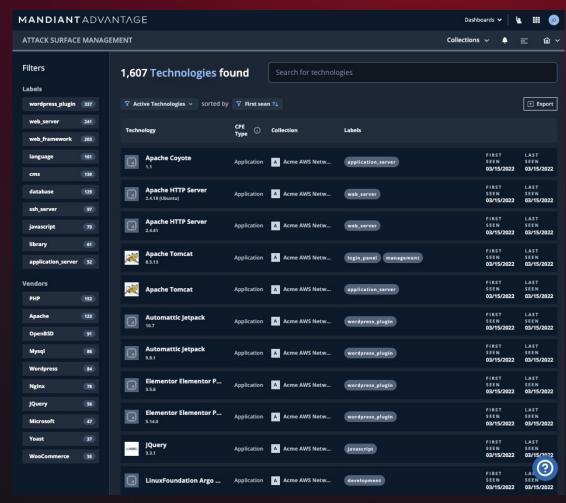


TECHNOLOGY

ENTITYs That Are Software, Services, Appliances, or VMs

- Discovered by Fingerprinting
- > 4300 Technology Fingerprints in MA-ASM database







COLLECTION

ENTITY

TECHNOLOGY

ISSUE

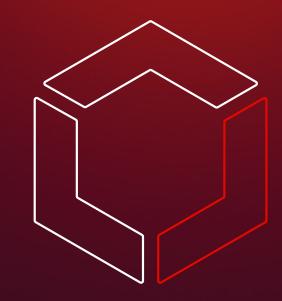
관리대상 버켓

식별 자산

사용 기술

발견된 위험

MA-ASM은 [COLLECTION] 이라는 기본적인 버켓에
[ENTITY]를 통해 식별된 자산을 표현하고 해당 [ENTITY]에



사용되는 [TECHNOLOGY]를 구분하고 이에 대해 잠재적 위험을 식별하여이를 [ISSUE]로 표현하여 정리합니다.

Attack Surface Management



확장된 조직 가시성 확보 및 유지



노출된 위험 식별 및 해결



지속적 위험 모니터링 및 완화

MANDIANT FRONTLINE EXPERIANCE



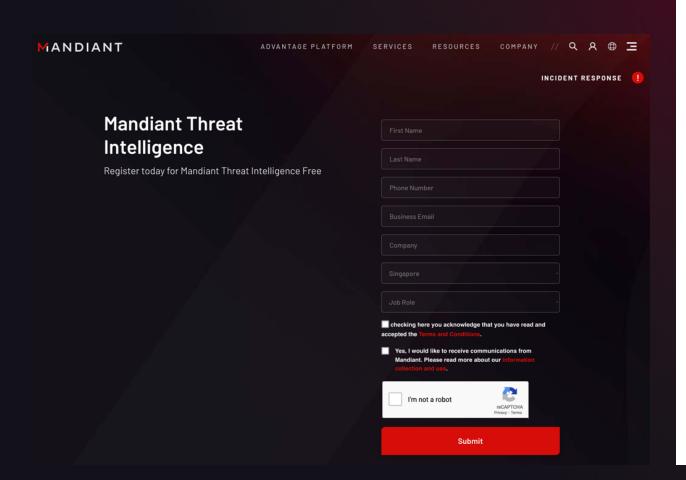






Register @ Mandiant.com

Free Tier Access To MA-TI & MA-ASM





https://mandiant.com/ti-free

MANDIANT

YOUR CYBERSECURITY ADVANTAGE