K-CTI 2022

2022 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

OSINT를 활용한 Attack Surface Threat 모니터링

ΣxWareLab KISEC

I am...

윤 영 수석 연구원

- 현 ㈜한국정보보호교육센터(KISEC) 교수연구부 수석연구원
- 현 ㈜시큐리티허브 수석컨설턴트
- 현 ExWareLabs 페이스북 운영자
- 전 ㈜에이쓰리시큐리티 모의해킹 수행팀장

하는 또는 했던 일

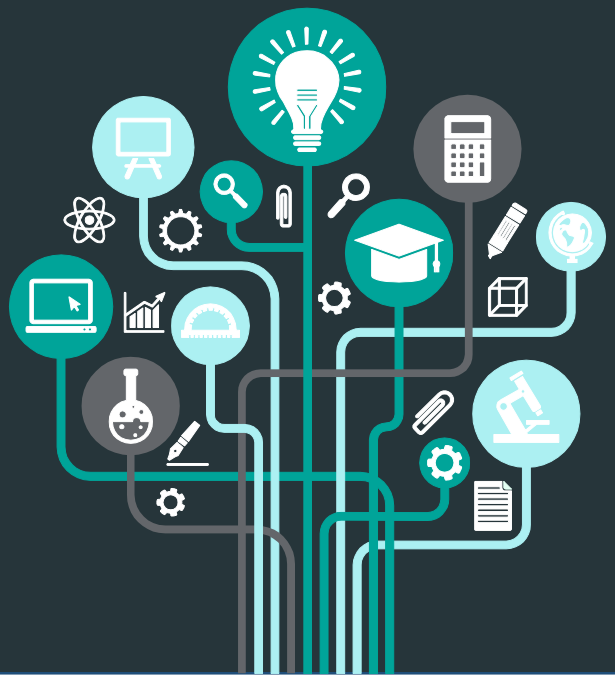
- 관련분야 경력 : 20년
- 강의분야: 사이버 해킹, Penetration Test, OSINT, Cyber Threat Intelligence
- 보안교육: 경찰청 사이버수사대 대상 정보보호 강의 다수
- 보안컨설팅: 금융회사 外 기업 모의해킹 다수
- Email : coderant@fngs.kr, coderant@nate.com
- ExploitWareLabs 운영자
  https://www.facebook.com/ExWareLabs/

목차

[Cyber Reacon - OSINT]

- **OSINT 란 무엇인가?**
- **OSINT로 무엇을 할 수 있을까?**
- **OSINT를 활용한 Attack Surface 위협정보 사례**

Cyber Reacon
- OSINT -



소목차

→ OSINT 란 무엇인가?

OSINT 란 무엇인가?

OSINT는 Open Source Intelligence 약자로서 공개된 출처에서 수집・분석한 지능정보를 의미한다.

OSINT 개념 및 소개

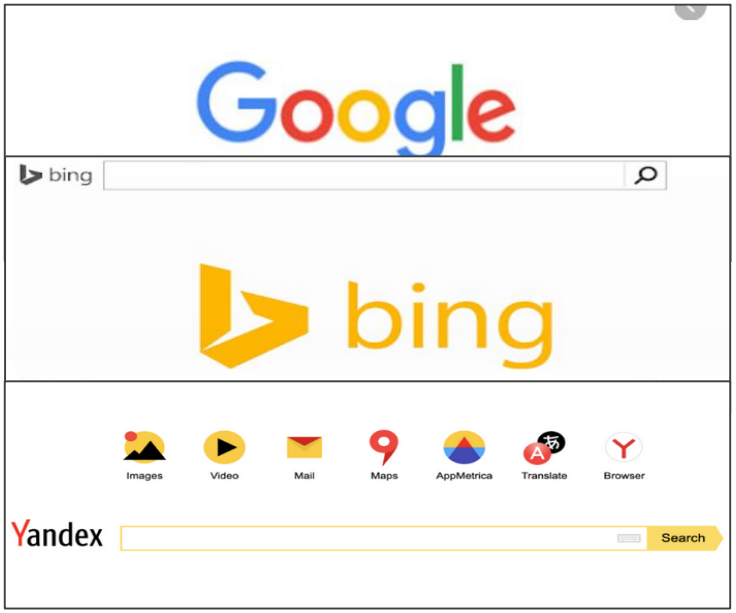
- **공개된 출처의 정보로 인텔리전스 지능정보를 만들어 내는 보안영역**
  - **인터넷 자체가 거대한 빅데이터 플랫폼 + 집단지성**
  - **공개출처란 언론미디어, 구글검색, 블로그/SNS 등 누구에게나 공개되어 있는 것을 의미함**
  - **OSINT를 활용하여 국가 안보, 기업 기밀자료, 개인정보 등 민감정보의 유출 모니터링 활동**
  - **OSINT로 수집되는 정보 유형은 TXT 파일, 전자 문서파일(Office, HWP), 이미지 등**

OSINT 란 무엇인가?

공개출처지능정보(OSINT)는 검색엔진, 소셜 네트워크 서비스, 이미지 공유, 익명공유 사이트, 다크웹 해킹포럼 등 다양한 출처에서 정보를 수집함

OSINT 지능정보 출처

- **검색 엔진 / SNS / 익명 공유사이트 / 해킹포럼**
  - ▶ 검색엔진 / SNS : Google, Bing, Yandex, Shodan/Censys, 트위터, 페이스북, 인스타그램
  - ▶ 익명 공유사이트/해킹 포럼 : RaidForums, Pastebin, MegaSync, Anonfile



SHODAN

Censys

twitter

Instagram

Telegram

GitHub

Jira Software

Trello

anonfile
anonymous file upload

PASTEBIN

RAID FORUMS

CRACKED.IO

OSINT로 무엇을 할 수 있을까?

OSINT 지능정보를 활용한 사이버 위협정보 모니터링이 필요한 이유

OSINT 활용한 보안위협 정보은 왜 필요한가?

- 첫째, 모든 기업 CISO들의 궁금증 – 우리회사는 정말 해킹으로 부터 안전?
  - 매년 보안진단 수행과 솔루션에 많은 투자를 하는데 과연 충분할까?
  - 정보보호 전담 인력과 보안투자와 충분하지 않다.
- 둘째, 혹시 보안통제를 벗어난 Security Hole은 있지 않을까?
  - Attack Surface 공격 접점은 의외로 많음(보안 담당자도 인지하지 못한 정보자산이 많음)
  - 공급망(Supply Chain) 보안 이슈는 어떻게 점검하지?
- 셋째, 해킹 신기술의 발전속도가 너무 빨라 대응이 쉽지 않다
  - 사이버 공격자들의 해킹기술은 너무 빠른 속도로 발전 – 상대적으로 보안대응 전문인력이 부족
  - 보안 컴플라이언스 대응이 담당자의 제일 중요한 업무
  - 보안 담당자의 잦은 이직 및 부서이동으로 숙련된 보안대응 인력 확보 안됨

OSINT로 무엇을 할 수 있을까?

공격표면 위협(Attack Surface Threat)은 비인가 사용자가 시스템에 액세스하여 데이터를 훔치거나, 해킹공격을 시도할 수 있는 모든 가능한 접점, 공격 벡터를 말함

공격표면 위협(Attack Surface Threat)

- **공격표면 위협(Attack Surface Threat)이란?**
  - **정보 자산, 취약점이나 위협 요소 등 존재하는 모든 잠재적 해킹공격 접점 또는 공격 벡터를 의미**
  - **공개출처지능정보(OSINT)를 활용하여 위협에 대한 검증 및 테스트하기 위한 기능 식별**

- **알려지지 않는 외부 액세스허용으로 해킹 공격에 대상이 될 위험성은?**
  - **인프라 자산 노출 (관리자 페이지, 내부 IP망 정보, 개발/테스트 시스템, 클라우드 정보 노출)**
  - **파일 정보 - 데이터베이스덤프, 전자파일, 도면정보, 개인정보, 기업 영업자료**
  - **APIs - OpenAPI, RestFull API 엔드포인트, Credential(AWS Keys, Oauth Token)**
  - **최신 취약점(CVEs) 영향 받는 장비나 시스템을 존재여부를 사전에 알 수 없을까?**

OSINT로 무엇을 할 수 있을까?

OSINT 활용한 Attack Surface 위협 정보수집에는 다음과 같은 Needs가 있음

기존 보안업무의 미흡한 점을 보완

- **공개출처지능정보(OSINT) 기반의 Attack Surface 위협관리**
  - **기존의 보안 진단에서 미비점 보완**
    - **ISMS 기반의 취약점 진단 대상은 제한된 예산으로 인해 한정된 대상만 진단함(전수 진단 불가)**
    - **주요정보통신기반시설 / ISMS정보보호관리체계 컨설팅의 부족한 부분을 보완**

- **기업 내 사이버 첩보 수집 역량이 필요**
  - **진단영역 외에 존재하는 취약점, 위협을 어떻게 찾아낼 것인가?**
    - **혹시 우리회사의 민감한 정보가 유출된 적은 없는가?**
    - **기업, 기관의 외부자/사이버 공격자 관점에서 위협/위험 요소를 파악해 보자**
    - **외부 액세스 관점에서 취약점 · 위협요소를 찾는 Attack Surface Threat가 주요 핫 트렌드**

OSINT로 무엇을 할 수 있을까?

OSINT 활용한 Attack Surface 위협 정보수집은 보안관제 업무에 많이 활용할 수 있음

OSINT 기반의 Attack Surface 위협 모니터링 활용

- 사이버 첩보 수집 활동 정보 보안관제 업무에서 OSINT 활용
  - ▶ 국가 안보 및 산업기밀 보호
    - 국가 안보와 관련된 사이버 첩보 수집활동
    - 국내외 산업기밀 및 방산정보 유출 정보수집
  - ▶ 사이버 보안 및 범죄 보안관제 및 대응업무 활용
    - 관제서비스 고객의 위협정보 수집(관리자 페이지, 휴면/데모/개발 사이트, Unknown Port 등)
    - 공급망(Supply Chain)에서 발생하는 정보노출 등 다양한 위협 정보
    - 최신 해킹 기법,다크웹/해킹 포럼에 유출 정보 모니터링
  - ▶ 사이버 범죄 첩보 수집 활동
    - 해킹 그룹 추적 및 스미싱, 보이스 피싱에 악용된 웹사이트 모니터링
    - 다크웹 / 랜섬웨어 모니터링

OSINT를 활용한 Attack Surface 위협정보

사이버 위협정보 사례

1. 해외 산업기밀 정보 유출 사례
2. 국내・외 민감정보 유출 사례
3. CVEs 취약점 정보수집
4. 사이버 범죄 관련 정보 사례

- Q & A -