위협 인텔리전스

발표자 조대인

위협 인텔리전스란?

- CTI(CyberThreat Intelligence)
- 사이버 보안 위협에 대한 분석된 정보
- 사이버 공격 사전 방지 및 진행중인 공격에 대한 대응책

위협 인텔리전스의 특징

- 조직에 대해 특화된 위협 인텔리전스를 구축 가능
- 공격을 수행할 수 있는 대상과 사이버 공격의 신호까지 예측
- 원시데이터를 가공(분석)하고 시각화, 또는 별도의 처리를 한 '인텔리전스'

위협 인텔리전스와 위협 정보의 차이

사이버 위협 정보	사이버 위협 인텔리전스
필터링 되지 않은 원시 정보 평가를 거치지 않은 데이터 거의 모든 데이터 원천에서 수집 제대로 된 정보일 수도 있으나 잘못된 정보일 수도 있음 보안 운영 측면에서 실행 가능한 정보가 아님	잘 분류된 정보 숙련된 분석가의 평가와 해석이 담긴 데이터 신뢰할 수 있는 출처에서 수집 정확하고, 적절한 정보 보안 운영 측면에서 탐지와 대응에 있어 실행 가능한 정보

위협 인텔리전스의 라이프 사이클

1. 계획수립
2. 위협 데이터 수집
3. 처리
4. 분석
5. 배포
6. 피드백

계획 수립

- 보안팀과 조직의 CSIO 등이 협력, 계획 수립
- 의사 결정권자와의 협의를 통해 인텔리전스 요구사항 설정

위협 데이터 수집

- 요구사항에 따른 원시 위협 데이터 수집

처리

- 보안 분석 팀에서 수집한 원시 데이터를 집계, 표준화

분석

- 원시 위협 데이터를 토대로 추세, 패턴을 분석
- 공격자가 동종 업계를 대상으로 삼았을 때, 이용된 취약점 및 공격기법을 파악하는 것을 예시로 들 수 있음.

배포

- 보안팀이 의사 결정권이 있는 관계자들에게 인사이트 공유, 이를 토대로 의심스러운 IP를 블랙리스트화하고 위험 점수 등을 부여할 수 있음.

피드백

- 처음에 제시한 요구사항을 토대로 이를 충족했는지 검토
- 새로 제시된 질문 등을 다음 라이프사이클에 활용 가능.

전술적 위협 인텔리전스

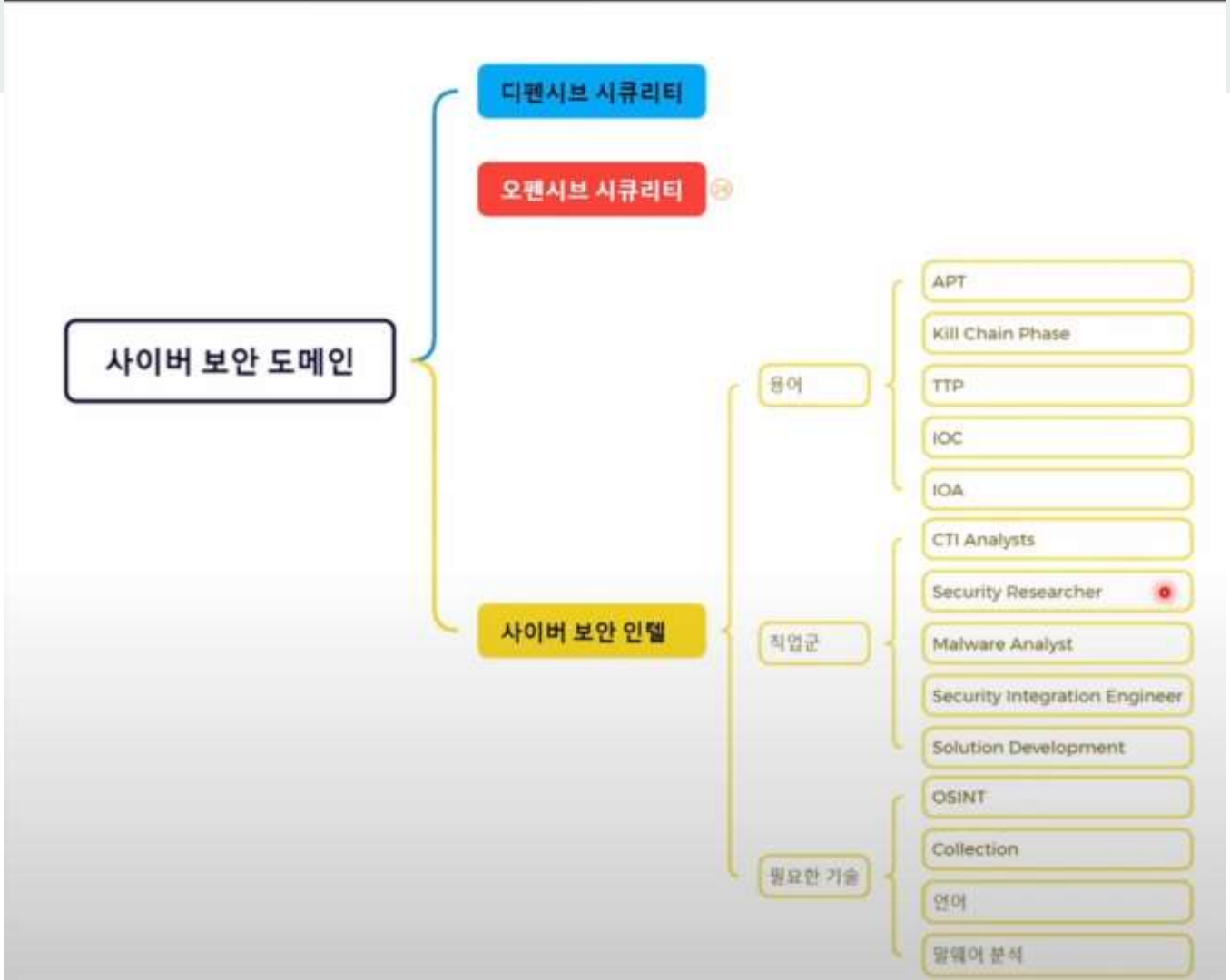
- 가장 기본적인 형태로 조직이 어떻게 공격을 받을 수 있는지에 대한 공격자의 전술에 대해 방어책을 제공
- 알려진 악성코드, 피싱 공격 이메일이나 C&C서버의 주소 등이 이에 해당함
- 보안 업체와 기업 내 사이버 보안 컨설턴트의 보고서가 주요 출처임

운영 위협 인텔리전스

- 기술적 위협 인텔리전스라고도 하여 위협 행위자를 식별하고 각종 조치로 공격을 막아내는 데에 초점이 맞춰져 있음
- 알려진 공격자들에 있어 공격 벡터, 공격 행위, 익스플로잇 취약점 및 주로 표적으로 삼는 자산을 설명하는 인텔리전스로 가장 적극적임
- 출처로는 포렌식 위협 인텔리전스 보고서, 위협 데이터 피드, 보안 이벤트 등이 있음

전략적 위협 인텔리전스

- 광범위하거나 장기적인 이슈를 다루며, 위협에 대한 트랜드를 분석하는 인텔리전스
- 자료의 출처는 보통 뉴스나 보안 연구 보고서 등이 있음


사이버 보안 도메인
디펜시브 시큐리티
오펜시브 시큐리티
사이버 보안 인텔
용어
APT
Kill Chain Phase
TTP
IOC
IOA
직업군
CTI Analysts
Security Researcher
Malware Analyst
Security Integration Engineer
Solution Development
필요한 기술
OSINT
Collection
언어
맬웨어 분석

위협 인텔리전스 관련 솔루션(CTI 솔루션)

안랩 TIP

KISA의 C-TAS

쿤텍 사이버 호크아이

마이크로 소프트 Defender 등

위협 인텔리전스 요약

- 위협 인텔리전스는 미리 위험 징조를 파악하여 침해사고를 예방하거나 이미 발생한 상황에 대한 대처 능력을 높이는데 의미가 있음.

- 위협 인텔리전스는 조직마다 필요한 정보의 차이가 있음
- 위협 인텔리전스의 출처는 크롤러, OSINT, SNS, 다크웹 등 다방면에 걸쳐있음

위협 인텔리전스의 제공 형태 예시

- 침해 자원에 대한 데이터 베이스
- 다크웹 포럼에서 가져온 정보 보고서
- 오픈소스 인텔리전스에서 추출한 정보 시각화
- 사이버 위협 정보 분석 및 공유 시스템(json이나 xml로 제공) 및 시각화 인터페이스를 통한 데이터 출력

앞으로 할 일

- 위협 데이터 피드를 분석하는 법
- 공개출처 정보를 위협 인텔리전스로 추출하는 법
- 위협 인텔리전스에 대해 배울 수 있는 포럼 및 커뮤니티 참여

참고자료

https://www.ibm.com/kr-ko/topics/threat-intelligence
https://nordvpn.com/ko/features/threat-protection/threat-intelligence/
https://www.ahnlab.com/ko/product/threat-intelligence?utm_source=google&utm_medium=cpc&utm_campaign=google_b2b&utm_content=AhnLab%20TIP&utm_term=%EC%9C%84%ED%98%91%EC%9D%B8%ED%85%94%EB%A6%AC%EC%A0%84%EC%8A%A4&gad_source=1&gclid=CjwKCAjwtqmwBhBVEiwAL-WAYRYsRGolhNxKrBEPyu_3bNeX6gCgYTYLpupjZgfwv9EcGpAY2BliFxoCFNMQAvD_BwE