QUAXAR

AI 기반 사이버 위협 인텔리전스 플랫폼

S2W

QUAXAR

AI 비서가 탑재된 조직 맞춤형 CTI 플랫폼

QUAXAR(퀘이사)는 기업 맞춤형 AI 기반 사이버 위협 인텔리전스(CTI) 플랫폼입니다. QUAXAR AI 비서가 실시간으로 기업의 주요 사이버 위협 인텔리전스를 선별해서 알려줍니다. 기업의 정보 유출 현황, 자산 취약점 정보를 맞춤형으로 생성해서 보여줄 뿐 아니라, 사이버 보안 측면으로 주목할 만한 위협 관련 주요 키워드, 동향 등을 알려줍니다.

또한, QUAXAR는 디지털 리스크 프로텍션(DRP), 공격 표면 관리(ASM), 그리고 위협 인텔리전스(TI)를 하나의 플랫폼에서 관리할 수 있어 전방위적으로 기업의 주요 자산을 보호할 수 있습니다. QUAXAR는 다수의 국제 고객사를 보유하고 있으며 조직별, 산업별 맞춤형 위협 탐지와 대응을 위한 풍부한 데이터와 노하우를 제공합니다.

실시간 사이버 위협 AI 비서

QUAXAR ASSISTANT

2024년 9월 10일 **우리 회사가 속해있는 산업 관련 TI 주요 이슈**입니다.
- 국내 IT 기업 대상 악성 LNK 유포 공격자: KONNI (상세보고서↗)

오늘 우리 회사 시스템과 관련된 **신규 취약점 2건**이 탐지되었습니다.
- CVE-2021-34473: Microsoft Exchange 서버의 ProxyShell 취약점 (대응책↗)
- CVE-2021-26855: Microsoft Exchange 서버의 ProxyLogon 취약점 (대응책↗)

조직 맞춤 전방위적 사이버 위협 인텔리전스

디지털 리스크 프로텍션
(Digital Risk Protection)

디지털 리스크 프로텍션은 조직이 디지털 환경에서 직면하는 직/간접적인 정보 유출과 브랜드 위협 대응을 지원합니다.

- ✓ 계정 탈취 모니터링(ATOM)
- ✓ 랜섬웨어 분석 및 모니터링
- ✓ 브랜드 위협 대응 액션 도구
- ✓ 다크웹/텔레그램에 올라오는 기업 및 산업 정보 제공

공격 표면 관리
(Attack Surface Management)

조직의 공격 표면을 식별하고 가시화하여 비공식 IT 자산을 제공하고 영향도를 평가하여 공격 표면을 최소화합니다.

- ✓ 자체 스캐너를 통한 전체 포트 스캔
- ✓ 자산의 취약점 측정과 위험도 평가
- ✓ 인증서 기간 모니터링 시스템
- ✓ 유출 계정과 연계된 취약점 정보 제공

위협 인텔리전스
(Threat Intelligence)

각종 채널에서 사이버 위협 정보를 수집/분석하고, 잠재적 위협에 선제 대응을 할 수 있는 인텔리전스를 제공합니다.

- ✓ 침해사고지표(IoCs)
- ✓ 탐지룰 (Yara, Snort)
- ✓ OSINT (구글, GitHub)
- ✓ 주요 랜섬웨어 그룹 등의 공격자 정보 및 분석

S2W

AI 기반 사이버 위협 인텔리전스 플랫폼, QUAXAR

QUAXAR 주요 기능

기업 맞춤 AI 어시스턴트

기업 맞춤 사이버 위협 현황을 알려주고, 사이버 보안 정보 및 동향을 제공합니다.

- 데일리브리핑
- 기업 자산 공격 표면 현황 (ASM)
- 기업 데이터/계정 유출 현황 (DRP)
- 사이버 보안 주요 키워드 및 동향

AI 기반 자동화 보고서

AI 보고서 생성 기능으로, 기업의 사이버 위협 현황과 보안 관련 기술 정보 보고서를 손쉽게 생성할 수 있습니다.

- 기업 특화 보고서 (Brand Security Digest)
- 기술 정보 보고서 (Trend Security Digest)

기업 계정/데이터 유출 관리

기업 계정과 기밀 자산 등의 유출 현황을 모니터링 하고 위협에 대응할 수 있습니다.

- 딥/다크웹, 텔레그램 모니터링
- 유출된 계정 정보 모니터링 및 탐지
- 랜섬웨어 그룹 모니터링
- 위협 출처 등 상세 내용 제공

기업 브랜드 위협 관리

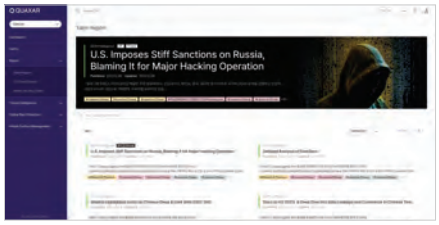
기업 브랜드 사칭, 피싱 등 브랜드 가치를 위협하는 요소들을 모니터링하고 보안 대응을 위한 인텔리전스를 제공합니다.

- 브랜드 사칭/피싱 모니터링
- 위협그룹 프로파일링 정보
- 침해지표(IoC), 탐지룰(Yara/Snort 등)
- 취약점 정보

기업 자산 관리

공격 표면 전체 포트 스캔을 통해 IT자산을 관리할 수 있고, 취약한 자산을 대상으로 즉시 활용 가능한 인텔리전스를 제공합니다.

- 자산에 존재하는 취약점 정보
- 자산과 연계된 계정 정보
- 주의가 필요한 자산 알림 및 로그 관리
- 인증서 관리



전문 분석가 지원 (TALON)

위협 분석 전문가가 침해사고 대응, 위협 대응 교육, 분석 보고서 등을 지원합니다.

- 침해사고 조사 · 대응
- 전문가 분석 보고서
- 스킬업 세미나
- 테이크다운 (Takedown) 서비스

S2W

QUAXAR 활용 사례

[A 고객사]
실시간 대응 사례 - 공격 타겟 선포

S2W는 2023년 모니터링을 수행 중 Breach Forums에 제조사 데이터를 찾는 글을 포착하였으며 게시자와 접촉하여 타겟 정보를 획득하여 각 사별로 안내.

01 Breach Forums 게시글 내 제조사 데이터를 찾는 글 포착

02 해당 게시글을 올린 유저와의 대화를 통해 어떤 자료를 원하는지와 타겟에 대한 정보가 확인되었으며 8개 제조사에 대한 타겟 정보가 도메인을 통해 확인됨

03 각 업체별로 해당 정보에 대한 공유 및 공격에 대한 대비를 할 수 있도록 개별 안내

[B 고객사]
선 대응 사례 – 소스코드 유출

S2W는 2023년 모니터링을 수행 중 Github 내 B사 관련 키워드가 포함된 자산 정보가 노출되어 있음을 확인 후 고객사에 즉시 알림 및 조치를 권고함.

01 B 고객사의 내부 자산이 포함된, 혹은 자산으로 추정되는 서비스 일부가 Github에 노출됨을 탐지

02 노출된 민감항목 내에는 내부서버 접속 정보(username, password, access-key 등)가 포함됨을 확인

03 내부망에서 사용중인 자산임을 확인. 해당 정보로 외부에서 접근 시 민감정보 유출피해 발생 가능성이 높기 때문에 외부 서비스 노출 차단 권장

[C 고객사]
실시간 대응 사례 – 취약점 공개

한국을 타겟으로 하는 중국 텔레그램에 파일이 업로드 됨. 파일 내용은 국내 1금융권 웹 페이지에 SQL 인젝션 취약점이 존재한다는 내용이고, 취약점 스캔 팁을 공유함.

01 해커들은 SQL 인젝션에 사용한 공격 구문을 공유

02 공격자는 불특정 다수의 웹 사이트에 무작위 취약점을 스캔해 취약한 사이트 수집 목록을 중국 텔레그램방에 공유

03 한국 웹 사이트 취약점 스캔시 유용한 팁을 공유하고 있음

04 국내 1금융권 이외에도 다양한 웹사이트 약 100건을 공유

05 고객사에 해당 내용을 안내하고 공격시도를 식별하여 공격 벡터를 제거하도록 가이드

[D 고객사]
실시간 대응 사례 – 중요 정보 유출

바이러스 검증 사이트 모니터링 중 S2W 고객사 납품 장비로 추정되는 D사 솔루션의 압축파일이 업로드된 것을 탐지, 파일 분석 결과 솔루션 서버/설정 정보가 포함된 파일임을 확인.

01 D사 솔루션 서버 동작에 필요한 각종 소스코드, IP, 설정 파일이 원본으로 올라와 있는 것을 확인

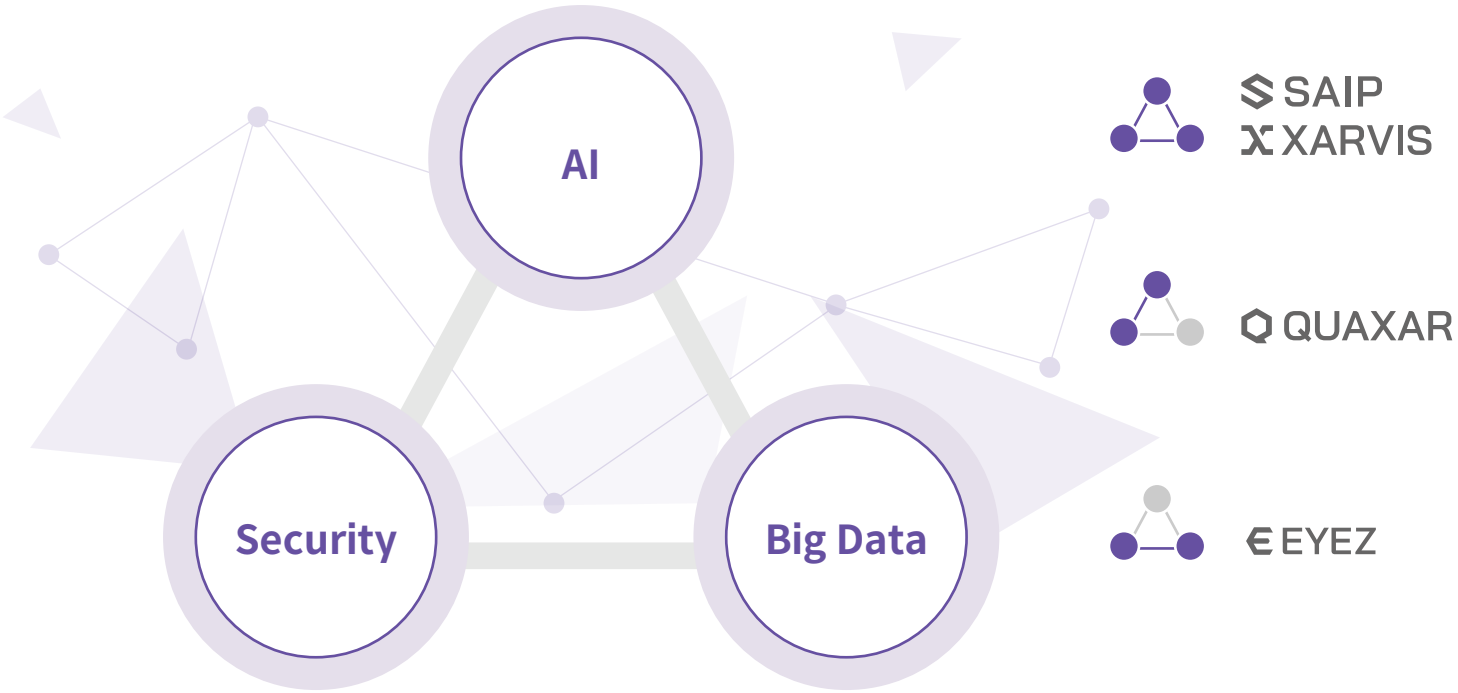
02 설정 파일 내 주석을 통해 해당 솔루션 우회 방식 등을 파악

03 바이러스 검증 사이트에 컨택하여 해당 파일에 대한 삭제 요청

04 추후 동일한 사고가 발생하지 않도록, 해당 파일이 업로드 된 경위를 분석하여 조치 권고

WHY S2W?

S2W는 멀티도메인 교차 분석 기술을 활용해 사용자 맞춤형 데이터 운용 플랫폼을 제공합니다. 이는 조직이 축적하고 있는 정형, 비정형 데이터를 수집·처리하는 시스템, 그리고 주어진 데이터를 가장 잘 이해하는 도메인 특화 언어 모델, 마지막으로 축적된 지식들을 하나의 그래프 형태로 통합 연결해 교차 분석하는 기술로 이루어집니다. S2W의 데이터 운용 시스템은 효과적인 데이터 활용을 돕습니다. 뿐만 아니라, 예기치 못하게 발생하는 데이터 유출, AI의 신뢰성 등의 문제까지 대응할 수 있는 시큐리티 가드레일을 탑재하여 안정적인 데이터 활용 시스템을 구축합니다.



국제 논문

NAACL 2024
Ignore Me But Don't Replace Me: Utilizing Non-Linguistic Elements for Pretraining on the Cybersecurity Domain

61회 ACL 2023
DarkBERT: A Language Model for the Dark Side of the Internet

NDSS 2019
Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web

NDSS 2024
DRAINCLoG: Detecting Rogue Accounts with Illegally-obtained NFTs using Classifiers Learned on Graphs

NAACL 2022
Shedding New Light on the Language of the Dark Web

THE WEB CONFERENCE 2019
Doppelgänger on the Dark Web: A Large-scale Assessment on Phishing Hidden Web Services

수상 이력

KBS 사이버보안 자문 기업 선정 (2024)

World Economic Forum
100대 기술선도 스타트업 선정 (2023)

Mircosoft Copilot
국내 유일 마이크로소프트 시큐리티 코파일럿 (Copilot for Security) 파트너

NCSC National Cyber Security Center
국가정보원 사이버 안보센터 참여기업 (2022)

S2W

sales@s2w.inc | +82 70 5066 5277 | www.s2w.inc