QUAXAR

AI 기반 사이버 위협 인텔리전스 플랫폼

S2W

QUAXAR

AI 기반 사이버 위협 인텔리전스 플랫폼

QUAXAR는 S2W가 다년간 수집해온 히든채널의 수많은 데이터들을 분류 및 정제하여
기업은 한 개의 플랫폼 내에서 사이버 위협에 대한 전방위적 보안 인사이트를 확인할 수 있습니다.

QUAXAR를 통해 무엇을 할 수 있나요?

- ✔ 국내/외 침해 위협에 대한 신속한 인지 및 대응이 가능합니다.
- ✔ 내부 자산에 존재하는 취약점을 확인하고 외부 위협으로부터 보호합니다.
- ✔ 다크웹, 텔레그램 등에서 유출되는 기업 데이터를 실시간으로 모니터링 합니다.

위협 인텔리전스
(Threat Intelligence)

전문가가 분석한 위협정보를
실시간으로 제공합니다.

- ✔ 위협그룹 정보(TA)
- ✔ 침해사고지표(IoCs)
- ✔ 탐지룰 (Yara, Snort)
- ✔ 취약점 정보 (CVE)

디지털 리스크 프로텍션
(Digital Risk Protection)

기업의 브랜드 가치를 보호하고
고객 신뢰도를 향상합니다.

- ✔ 텔레그램 모니터링
- ✔ 브랜드 피싱 모니터링
- ✔ 랜섬웨어 그룹 모니터링
- ✔ 유출된 계정정보 탐지

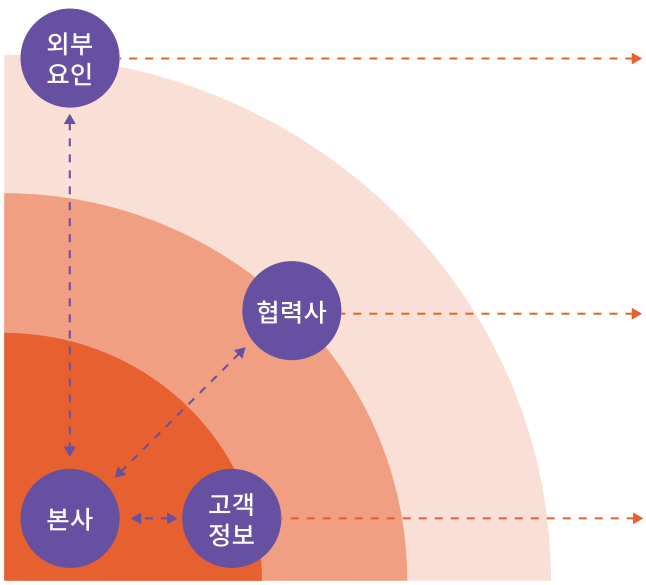
공격 표면 관리
(Attack Surface Management)

다양한 외부 위협 관련 유의미한
인텔리전스를 제공합니다.

- ✔ 외부 접점의 자산 식별
- ✔ 자산의 취약점 정보
- ✔ 자산에 연계된 계정 정보

S2W

전방위적인 CTI



외부 접점에서 내부 침투

외부 접점에 위치한 자산의 취약점을 사용하여
내부망으로 침투가 가능한 자산 모니터링

외부에서 유출된 내부 데이터

협력사/계열사 또는 서드파티 제품을 통해
유출된 내부 데이터에 대한 모니터링

내부 데이터 외부 유출

내부 자산 도용 및 기업 내 신기술 등
기밀 데이터 유출 위협에 대한 모니터링

전문 분석가 지원(TALON)

위협 전문가의 분석 분석이 필요할때 TALON팀의 지원을 요청할 수 있습니다.
TALON은 국내 최상위 분석가와 다크웹 전문가로 구성된 S2W의 위협 분석 그룹입니다.

- ✔ 침해사고 조사 · 대응
- ✔ Take-down 서비스
- ✔ 악성코드/위협 행위자 분석
- ✔ 전문가 분석 보고서
- ✔ 스킬업 세미나
- ✔ 사이버 위협 대응 전략

S2W

Use Case

QUAXAR에서 제공하는 다양한 인텔리전스를 통해 견고한 침해 대응 전략을 수립할 수 있습니다.

타 시스템 연계를 통한 실시간 확인 | SIEM 장비 연계

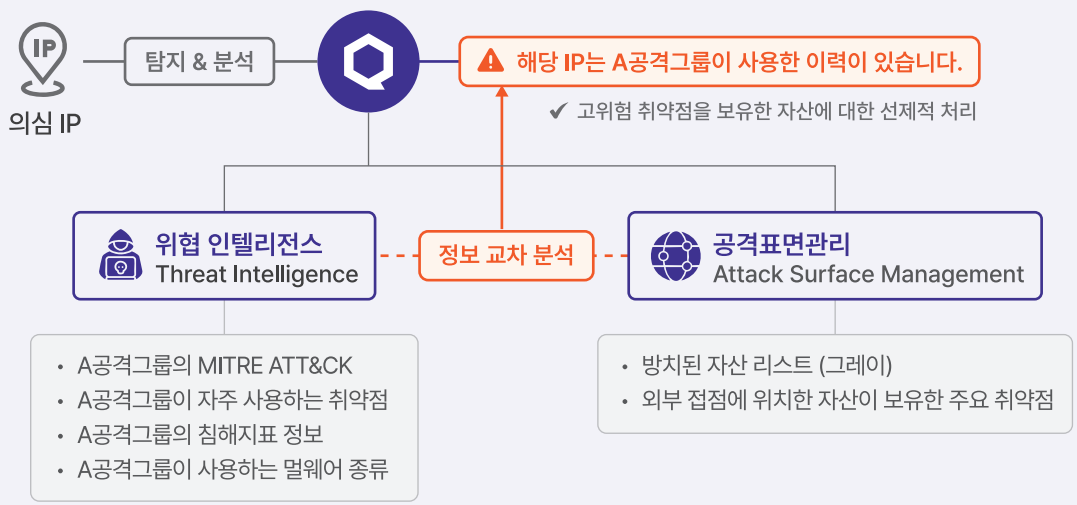
보안관제 시스템(SIEM)과 연동하여, API 및 YARA Rule, Snort Rule 기반의 신속한 위협 탐지를 지원

- 즉각적인 위협 탐지 알림
- API, YARA Rule, Snort Rule 활용

Threat Intelligence

공격그룹 정보와 외부 접점의 자산 | 침해 대응 전략 수립

해당 IP를 사용하는 공격그룹의 주요 공격방식을 확인하여 침해대응전략 수립



Threat Intelligence & ASM

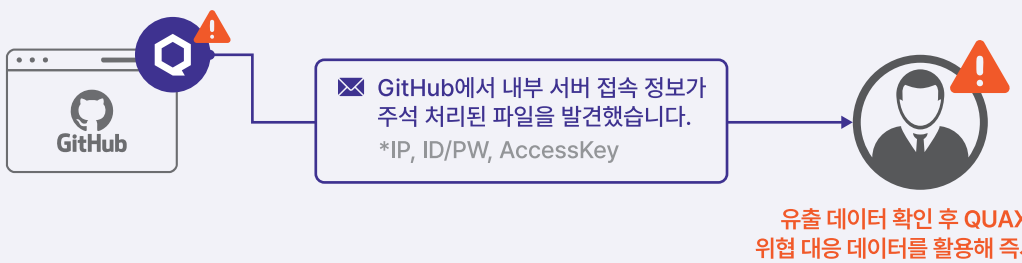
S2W

Use Case

QUAXAR에서 제공하는 다양한 인텔리전스를 통해 견고한 침해 대응 전략을 수립할 수 있습니다.

OSINT 영역에 유출된 데이터 | GitHub 모니터링

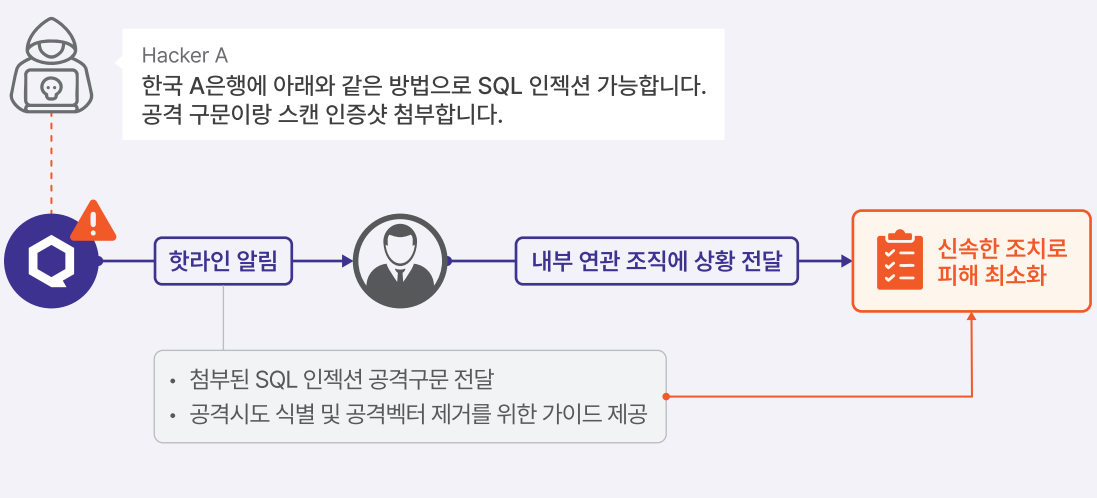
기업명을 비롯한 주요 키워드 탐지를 통해 OSINT 영역에 노출된 중요 데이터 모니터링



Digital Risk Protection

다크웹/텔레그램 게시글 모니터링 | 실시간 대응 사례

기업의 민감 정보가 다크웹/텔레그램을 통해 유포 시 이를 빠르게 탐지하고 대응 전략을 수립



Digital Risk Protection

S2W

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.

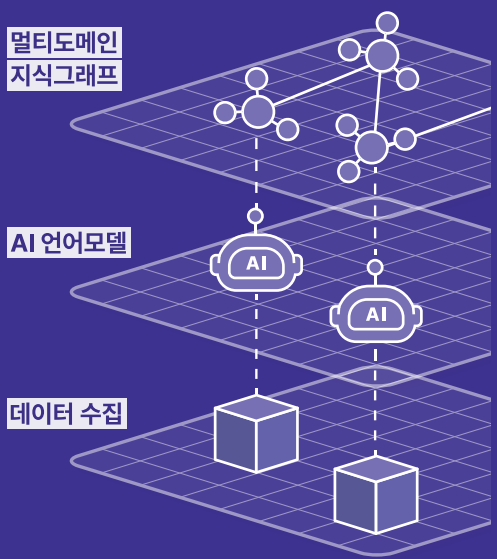
- 침해사고 조사 · 대응
- 전문가 분석 보고서
- 스킬업 세미나
- 테이크다운 (Takedown) 서비스

S2W

빅데이터 분석 AI 기업, 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.



논문

EMNLP 2025

Improbable Bigrams Expose Vulnerabilities of Incomplete Tokens in Byte-Level Tokenizers

NAACL 2024

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

61st ACL 2023

DarkBERT: A Language Model for the Dark Side of the Internet

KDD2025

Covering Cracks in Content Moderation: Delexicalized Distant Supervision for Illicit Drug Jargon Detection

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

최근 활동

Microsoft Copilot — 마이크로소프트 시큐리티 코파일럿 (Security Copilot) 파트너 (2024 - 현재)

NCSC National Cyber Security Center — 국가정보원 사이버안보센터 참여 기업 (2022 - 현재)

INTERPOL — 국제형사경찰기구 인터폴 협력 (2019 - 현재)
한국 최초 Gateway Initiative 파트너

WORLD ECONOMIC FORUM — World Economic Forum
100대 기술선도 스타트업 선정 (2023)

S2W

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