XARVIS

AI 기반 사이버 범죄 인텔리전스 플랫폼

S2W

XARVIS

AI 기반 사이버 범죄 인텔리전스 플랫폼

XARVIS(자비스)는 AI 지원 사이버 범죄 지능 플랫폼입니다. 다크웹, 딥웹, 텔레그램을 포함한 사이버 범죄의 사각지대에 놓인 각종 익명 채널에서 데이터를 수집하며, 사용자는 하나의 플랫폼에서 사이버 범죄 수사에 필요한 유효 데이터를 취득하고 특정 사건을 추적할 수 있습니다.

오늘날의 사이버 범죄는 그 종류와 양이 급격히 증가하고 있어 신규 공격에 대한 파악과 대응에 어려움이 있습니다. XARVIS는 사이버 범죄에 특화된 데이터 추적 도구와 AI 기반 분석 엔진을 화용해 수동 수사 과정을 간소화하고 수사 시간을 단축해줍니다.

AI

사이버 범죄 특화
AI 엔진

Big Data

다크웹, 텔레그램,
가상자산 등

XARVIS for Law Enforcement Agencies

사이버 범죄의 사각지대 모니터링

딥/다크 웹 및 텔레그램을 포함한 각종 익명 채널 실시간 모니터링을 통해 신속한 신규 위협 정보 취득이 가능합니다.

불법행위 추적

다양한 채널에서 수집된 실시간 및 과거 데이터 분석을 통해 마약, 금전 등의 불법 거래 추적하거나 각종 범죄 활동에 대한 인텔리전스를 취득합니다.

위협 행위자 식별

사이버 범죄에 특화된 위협 데이터 추적 도구들을 사용하여 사건과 위협 행위자 간의 숨겨진 연결고리를 찾고 더 많은 증거를 수집하며 용의자를 추적할 수 있습니다.

국가 안보 강화

특정 국가를 대상으로 하는 사이버 공격이나 사회적 위협을 유발하는 각종 범죄 활동을 모니터링하며 잠재적 위협에 대한 가시성을 확보합니다.

Copyright © 2024, S2W Inc.

S2W

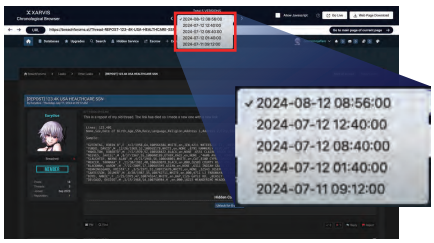
사이버 범죄 수사 플랫폼, XARVIS

XARVIS 주요 기능

통합 검색 엔진

딥/다크 웹 및 텔레그램을 포함한
각종 익명 채널에서 수집된
위협 데이터를 검색할 수 있습니다.

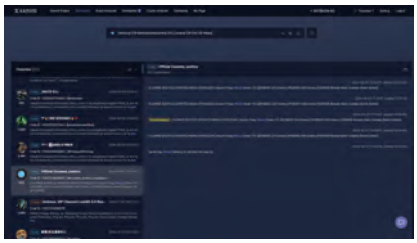
- 최신 딥/다크 웹 동향에 따른 검색 가이드
- 다양한 필터 옵션
  (언어, 이미지, 카테고리 등)



크로놀로지컬 브라우저

휘발성이 강한 다크웹 데이터 확보와 기록 추적을 위해 원본 컨텐츠를 실시간으로 수집하고 연대순으로 제공합니다.

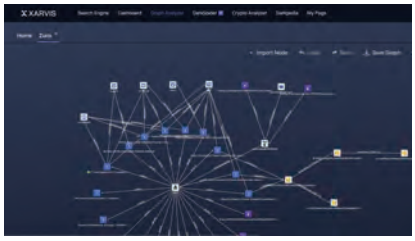
- 안전하고 직관적인 다크웹 데이터 취득
- 수정/삭제되는 다크웹 데이터 확보



텔레그램 모니터링

텔레그램에서 수집한 최신 컨텐츠와
데이터를 모니터링합니다.

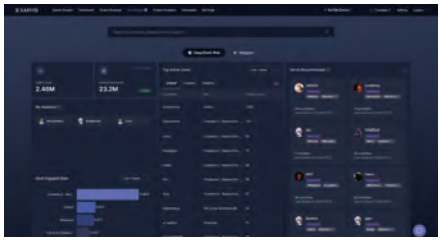
- 텔레그램 채널, 그룹, 메세지 모니터링
- 키워드 기반 검색
- 다양한 위협 행위자 채널 분석



멀티 도메인 교차 분석

흩어진 정보를 연결해 숨겨진 관계를
찾아내고 새로운 인사이트를
얻을 수 있습니다.

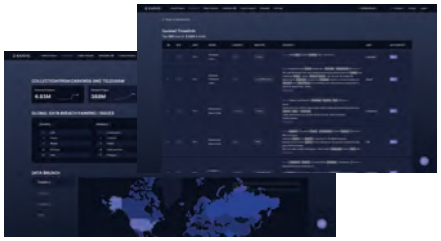
- 각종 침해지표 데이터 베이스
  (실시간 업데이트)
- 직관적으로 시각화된 그래프
- 원본 페이지 이동



유저 프로파일링 'Dark Spider'

잠재적인 위협 행위자를 직관적으로
식별하기 위한 다크웹/텔레그램 사용자
프로파일링 도구입니다.

- 주요 사이트별 사용자 규모 추이 추적
- 사용자별 새 게시물 업데이트 현황



맞춤형 위협 대시보드

AI 기반 맞춤형 위협 데이터 선별 시스템을
갖추고 있습니다.

- 대량 위협 정보 분류
- AI 기반 위협 위험도 산출
- 고위험 콘텐츠 선별 및 노출

Copyright © 2024, S2W Inc.

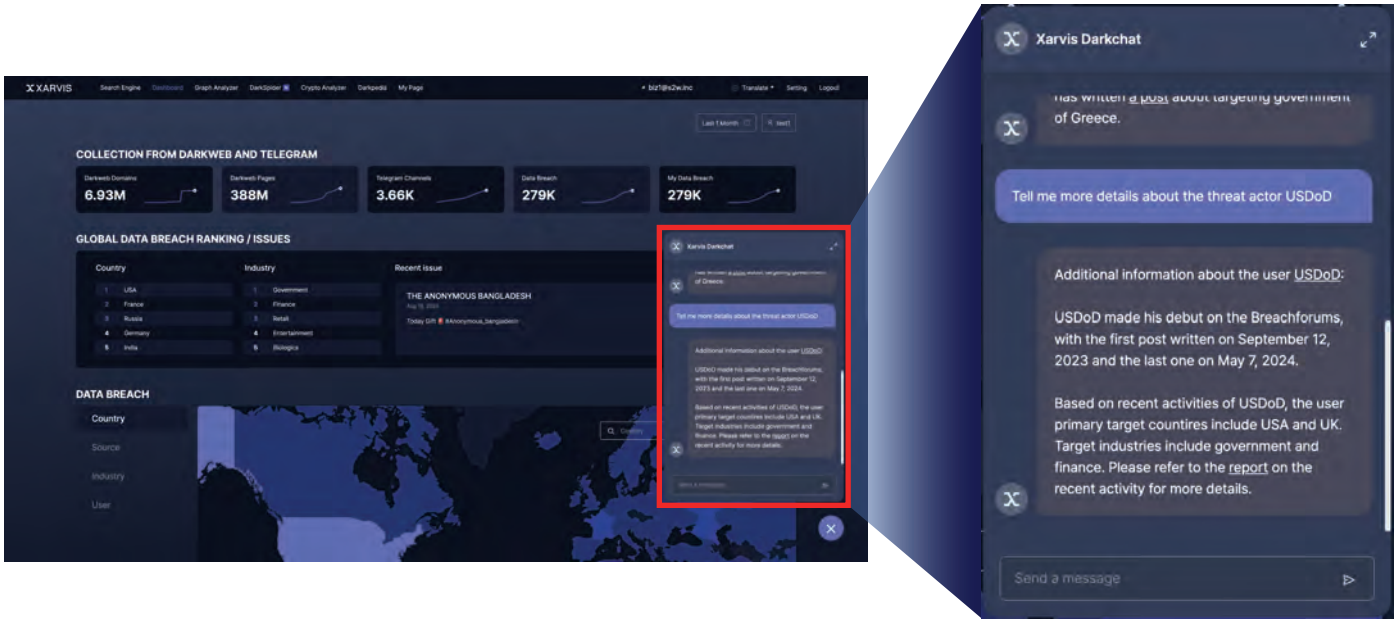
S2W

사이버 범죄 AI 챗봇, DarkCHAT

DarkCHAT: 사이버 범죄 AI 챗봇

DarkCHAT은 DarkBERT*와 S2W의 방대한 다크웹 데이터를 기반으로 한 사이버 범죄 챗봇으로, 사용자가 다크웹에서 정제된 데이터를 검색하고 얻을 수 있도록 합니다. DarkCHAT은 금융 사기나 사이버 범죄 서비스(암호화폐 믹서 등)를 위해 새로 생성된 다크웹 도메인을 빠르게 탐지합니다. 다크웹과 사이버 범죄 환경의 진화를 학습하고, 일반적으로 탐지와 추적이 어려운 잠재적인 사이버 보안 위협을 식별합니다.

더불어 DarkCHAT은 다크웹에서 발생하는 자금 세탁 등의 사건 분석이 필요할 때 손쉽게 챗봇에 도움을 요청할 수 있으며, 빠른 결과를 통해 불필요한 시간을 줄이고 보유 정보의 차이가 있는 사용자 간의 지식 격차를 최소화합니다. 예를 들어, 다크웹과 암호화폐에 익숙하지 않은 신입 수사관과 다크웹 관련 수사 경험이 있는 선임 수사관 간의 지식 차이를 좁힐 수 있습니다.



DarkBERT

세계 최초 다크웹 특화 AI 언어모델

대량의 비정형
다크웹 데이터

+

트랜스포머 기반
범용 언어 모델

DarkBERT
Language Model for the Dark Side of the Internet

- S2W와 KAIST 연구진이 공동 개발한 다크웹 특화 언어 모델
- 600만개 이상의 다크웹 페이지를 학습해 다양한 유형의 위협 데이터를 효과적으로 탐지하고 분류
- 인터폴과 국제 정부 기관에서 사용됨

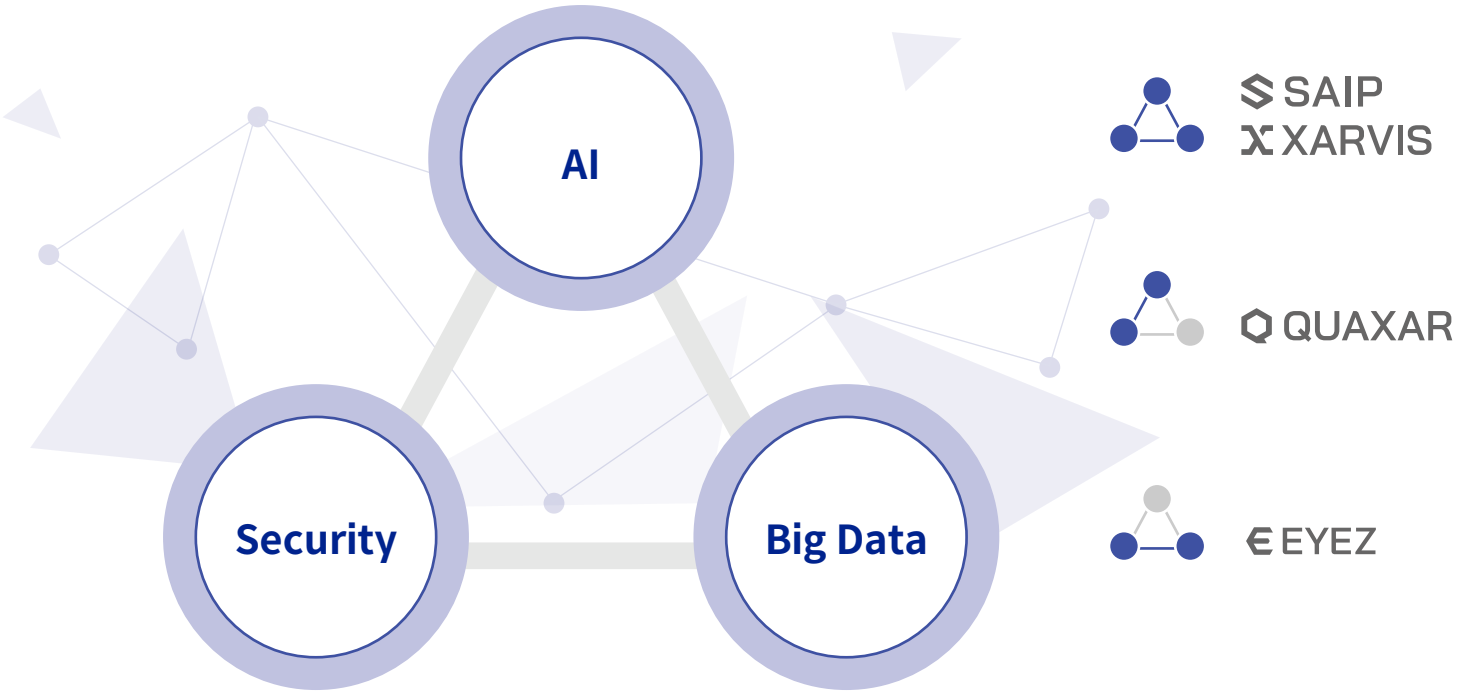
Copyright © 2024, S2W Inc.

S2W

WHY S2W?

S2W는 데이터 인텔리전스 기업으로 기술의 융합을 통해 창의적인 솔루션을 제안합니다.

S2W는 믿을 수 있는 AI 기반 데이터 인텔리전스 제공을 목표로 합니다. 정교한 AI 기술을 기반으로 빅데이터를 분석하고 그것을 안전한 울타리로 보호합니다. 숨겨진 데이터를 탐지해, 전에는 볼 수 없었던 데이터 간의 관계를 찾아내 가시화합니다. 보안을 잘 아는 회사가 만들어가는 AI 기반 데이터 인텔리전스 플랫폼, 그것이 안전한 데이터 사회를 만들어가기 위한 우리의 역할이자 목표입니다.



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)

Copyright © 2024, S2W Inc.

S2W

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

Copyright © 2024, S2W Inc.