사이버 위협 인텔리전스 솔루션

quaxar

quaxar

외부 위협 대응을 위한 CTI 솔루션

Quaxar는 내부 보안 시스템으로 탐지가 어려운 외부 위협을 모니터링하고 관리해 조직의 사이버 보안을 강화하는 CTI 솔루션입니다. 딥,다크웹을 비롯한 다양한 채널에서 방대한 양의 데이터를 수집하고, 수집한 데이터를 정제, 연결해 위협 인텔리전스(TI)를 도출합니다. 추출된 TI를 활용해 다양한 외부 위협을 선제적으로 예방하고, 예상치 못한 사이버 공격이나 탐지된 잠재적 위협에 신속하게 대응할 수 있는 실행 가능한 인텔리전스를 제공합니다.

Quaxar 핵심 서비스

디지털 리스크 프로텍션 (DRP)

기업의 브랜드 가치를 보호하고 고객 신뢰도를 향상시킵니다.

- 브랜드 어뷰징 사이트 탐지
- 피싱 사이트 탐지
- 비정상 모바일 앱 탐지
- 어뷰징 사이트/앱 테이크 다운 서비스

능동적 위협 및 취약성 관리

다양한 외부 위협 관련 유의미한 인텔리전스를 신속하게 제공합니다.

- 표면 공격 모니터링 (ASM)
- 랜섬웨어 활동 모니터링
- 최신 취약점 및 IoC 정보 제공
- 위협 행위자 프로파일링

데이터 침해 탐지

딥/다크웹 및 기타 채널에서 기업 핵심 자산 유출을 감지합니다.

- 개인 정보 유출 탐지
- 기업 정보 유출 탐지
- 금융 정보 유출 탐지

취약점 인텔리전스

최신 취약점 정보를 실시간으로 제공합니다.

- 리스크 점수(CVSS, EPSS)
- 취약점 영향을 받는 제품 및 제조업체 정보
- 취약점 관련 동향 뉴스

텔레그램 모니터링

텔레그램 상의 잠재적 위협 키워드를 실시간으로 모니터링합니다.

- 6000개 이상의 채널 모니터링
- 고객 맞춤형 탐지 규칙
- 특정 사용자 프로파일링
- 텔레그램정 연관 분석

침해 사고 대응

브랜드 어뷰징 요소를 제거하고 침해 사고 시 사고 조사를 지원합니다.

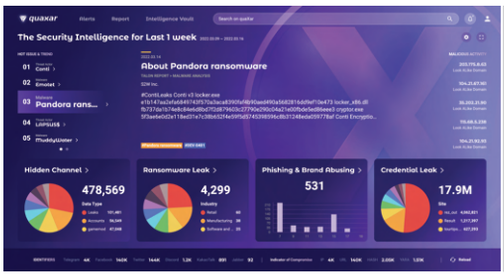
- 테이크다운 서비스
- 랜섬웨어 공격 대응
- 클라우드 계정 침해 대응

S2W

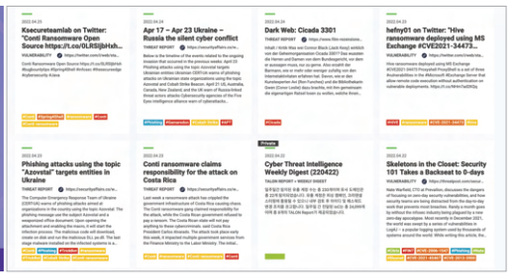
Quaxar 주요 기능

대시보드

- 사이버 보안 관련 핫 이슈 및 동향
- 위협 인텔리전스 현황
- 최신 사이버 위협 관련 콘텐츠



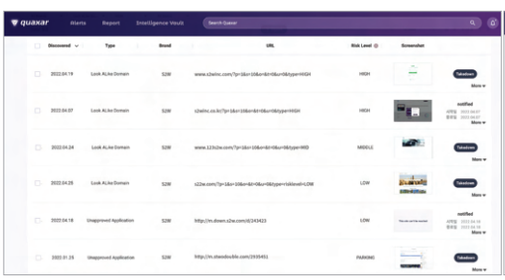
▲ 메인 대시보드



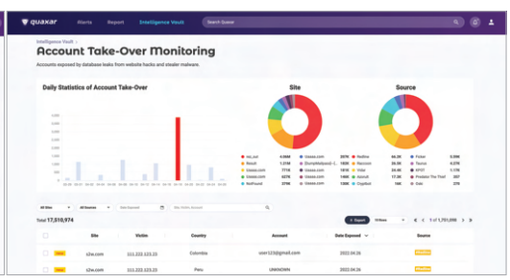
▲ 최신 사이버 위협 관련 콘텐츠

디지털 리스크 프로텍션

- 브랜드 어뷰징 사이트/
  앱 모니터링
- 계정 탈취 모니터링
- 랜섬웨어 활동 모니터링



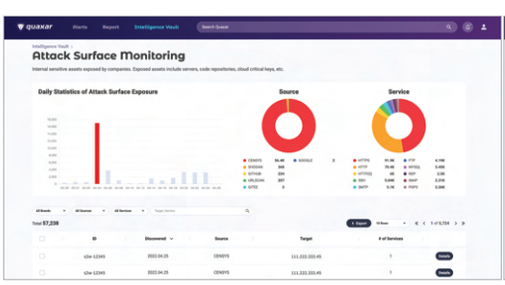
▲ 브랜드 어뷰징 사이트/앱 모니터링



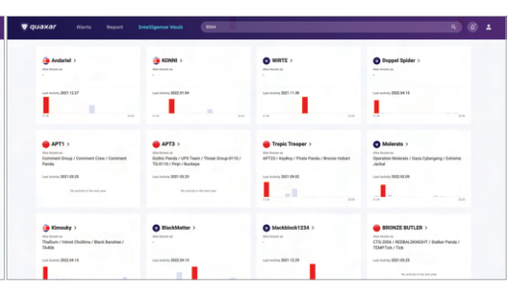
▲ 계정 탈취 모니터링

위협 인텔리전스

- 공격 표면 모니터링 (ASM)
- IoC(침해지표) 네비게이터
- 탐지룰 정보
- 위협 행위자 프로파일링



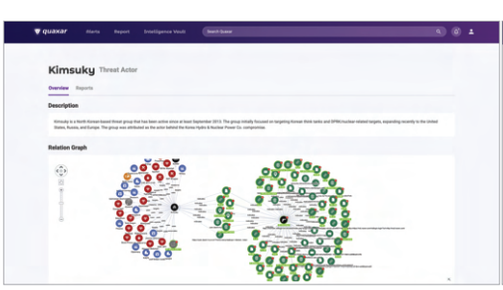
▲ 표면 공격 모니터링 (ASM)



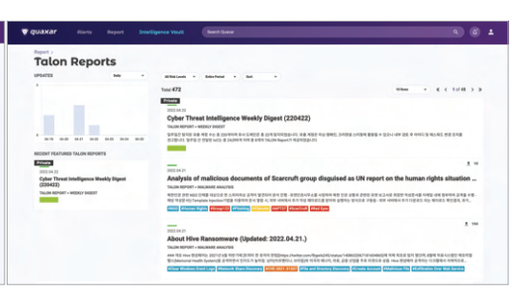
▲ 위협 행위자 프로파일링

보고서

- Talon 보고서
- 보안 뉴스
- 취약점
- OSINT IoC



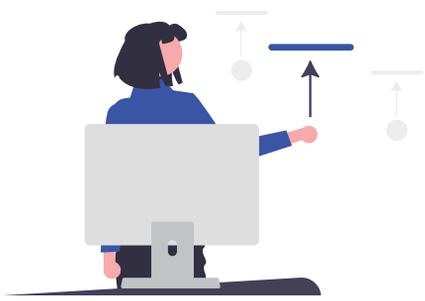
▲ 인텔리전스 관계 그래프



▲ Talon 분석 보고서

S2W

고객사 후기



글로벌 오토모티브 기업 | 매니저

Quaxar를 사용하면서 가장 좋은 점 중 하나는 S2W가 위협 행위자의 정보를 선제적으로 제공한다는 것이었어요. LAPSUS$ 사건에서도 S2W 덕분에 사전에 공격을 준비하고 예방할 수 있었어요. S2W는 LAPSUS$가 우리를 공격하려고 시도하기 훨씬 전에 LAPSUS$의 공격 기법에 대해 알려주었어요.

S2W의 정보가 없었다면, 우리는 큰 보안 사고를 겪을 수도 있었어요. 이번 사건을 통해 선제적 외부 위협 방어가 얼마나 중요한지 깨닫게 되었습니다.

글로벌 이커머스 기업 | 선임 매니저

국내 주요 대기업들은 해외를 근거지로 둔 국가지원 해킹그룹에 지속적으로 노출되고 있다고 들었어요.

Quaxar는 특정 위협 그룹이 만든 악성코드가 퍼지고 있음을 가장 먼저 감지해서 알려주었어요. 국내 대기업의 기밀 정보를 노리는 것으로 유명한 그룹인 만큼 신속한 대응이 필요했어요. S2W는 주요 위협 그룹과 악성 코드에 대한 풍부한 IoC를 보유하고 있어서 신규 위협을 빠르게 탐지해주었어요. 그 덕분에 악성코드 유포 사실을 인지한 당일에 근거지를 파악하고 차단해 위협에 대응할 수 있었네요.

이커머스
C 기업

" 아직 활성화되지 않은 피싱 사이트에 대한 도메인 정보를 받고 있습니다. "

처음 받아보는 정보들을 제공해주고 있는데요, 그것들이 보안사고 예방에 큰 도움을 줍니다.

텔레콤
S 기업

" 내부 주요 자산과 개인 정보 유출 탐지율과 정확도와 탐지율이 굉장히 높아요. "

S2W의 정확한 유출 원인 분석 덕분에 위협 대응이 한결 수월해졌어요.

오토모티브
H 기업

" S2W는 최신 위협 그룹 및 공격 지표에 대한 정보를 누구보다 먼저 파악해서 알려줘요. "

신속한 정보 전달 덕분에 위협에 대비하고 사고를 예방할 수 있었어요.

S2W

S2W는 사이버 위협, 브랜드/디지털 어뷰징 및 가상 자산을 위한 인텔리전스 솔루션을 제공합니다.

데이터 중심의 초연결 사회에서 최적의 문제 해결 방법을 도출하고, 외부 위협으로부터 조직을 보호하고 기업 브랜드 가치 향상을 위한 맞춤형 솔루션을 제안합니다.

S2W는 빅 데이터 분석, 머신 러닝, 딥 러닝 등 다양한 기술을 활용해 위협 인텔리전스, 디지털 어뷰징 인텔리전스, 가상 자산 인텔리전스 솔루션을 제공합니다.

발표

DarkBERT
A Language Model forthe Dark Side of the Internet
(ACL 2023)

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

OPERATION NEWTON
HI KIMSUKY? DID AN APPLE(SEED) REALLY
FALL ON NEWTON'S HEAD? (Virus Bulletin 2021)

Doppelgangers on the Dark Web
A large-scale Assessment on phishing
Hidden Web Services (WWW 2019)

특허권

암호화폐 거래 분석 방법 및 시스템

지식 그래프를 활용한 사이버 보안 제공
방법과 장치 그리고 프로그램

암호화폐 거래 분석 방법과 장치

다중 도메인에서 데이터를 수집하는 방법과 장치

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