QUAXAR

Comprehensive Cyber Threat Intelligence(CTI) Platform

S2W

QUAXAR

Comprehensive Cyber Threat Intelligence(CTI) Platform

QUAXAR is a Comprehensive Cyber Threat Intelligence(CTI) Platform. It manages Digital Risk Protection(DRP), Threat Intelligence(TI), and Attack Surface Management(ASM) all within a single platform. QUAXAR enables businesses to protect their critical internal assets and proactively respond to potential threats through immediately actionable intelligence.

We are continuously expanding the collection of channels including the Deep and Dark Web, Telegram, and OSINT. It filters valid information from vast data, providing users with actionable items and strategies for immediate response.

QUAXAR Core Service

Digital Risk Protection

Protects the corporate brand and gains the trust from customers.

- Brand abuse site detection
- Phishing site detection
- Abnormal mobile app detection
- Abuse sites/apps take-down

Active Threat Management

Quickly provides meaningful intelligence against various external threats.

- Ransomware activity monitoring
- Latest IoC information
- Attack Surface Management
- Threat actor profiling

Data Breach Detection

Detects corporate core asset leakage on the deep/dark web and other channels.

- Corporate data leakage detection
- Financial data leakage detection
- Credential data leakage detection

Vulnerability Intelligence

Provides the latest vulnerability information in real-time.

- Risk scoring (CVSS, EPSS)
- Information on products and manufacturers affected by vulnerabilities
- Trending news on vulnerabilities

Telegram Monitoring

Monitors keywords of potential threat on telegram in real-time.

- Monitors 6000+ channels
- Customer tailored detection rule
- Target user profiling
- Telegram association analysis

Incident Response

Eliminates brand abuse elements and provides accident investigation in the case of infringement accidents.

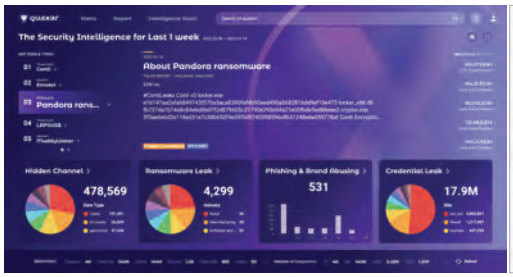
- Takedown Service
- Ransomware Attack Response
- Cloud Account Breach Response

S2W

QUAXAR Key Features

Dashboard

- Hot Issues & Trends
- TI Status
- Latest Cyber Threat Related Contents



▲ Main Dashboard

▲ Latest Cyber Threat Related Contents

Digital Risk Protection

- Brand Abuse Site/App Monitoring
- Account Take-Over Monitoring
- Ransomware Activity Monitoring

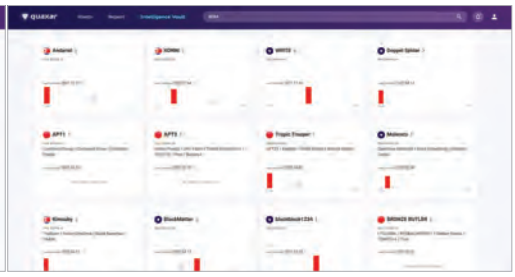
▲ Brand Abuse Site/App Detection

▲ Account Take-Over Monitoring

Threat Intelligence

- Attack Surface Monitoring
- IoCs Navigator
- Signature Vault
- Threat Actor Profiling

▲ Attack Surface Monitoring

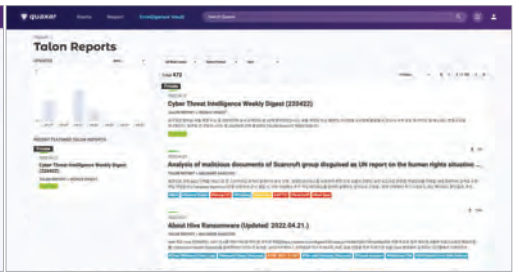


▲ Threat Actor Profiling

Reports

- Talon Reports
- Security News
- Vulnerabilities
- Open IoCs

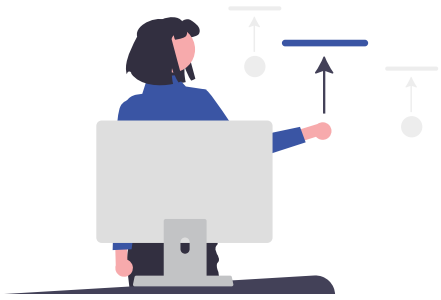
▲ Intelligence Relation Graph



▲ Talon Analyst Reports

S2W

Client Testimonial



Global Automotive Company | Manager

One of the best things about using Quaxar is that S2W preemptively gives information of threat actors. Even in this LAPSUS$ incident, we were able to prepare and prevent attacks in advance, thanks to S2W. S2W informed us about LAPSUS$'s attack techniques long before they attempted to attack us.

Without the information from S2W, we could have suffered a major security breach. Through this incident, I realized how important preemptive external threat defense is.

Global E-Commerce Company | Senior Manager

I heard that major domestic conglomerates are constantly exposed to state-sponsored hacking group based overseas.

Quaxar was the first to detect and inform that a malicious code created by a particular threat group was spreading. Quick respond was needed as the threat the group was famous for targeting large domestic companies for confidential information. S2W could detect the threats quickly with its abundance of IoCs for major threat groups and malicious codes. As such, we managed to respond against the threat on the same day by blocking the base of the distributed malicious code.

E-commerce
C Company

" I'm receiving domain information for phishing sites that are not active yet. "

It's the kind of information I've never received before, and it's highly effective in preventing accidents.

Telecom
S Company

" It has outstanding detection rate and accuracy in detecting internal major asset and credential leakage. "

Thanks to S2W's accurate analysis of the cause of the leak, the response became easier.

Automotive
H Company

" S2W identifies and delivers information on the latest threat groups and attack indicators before anyone else. "

Thanks to this, we were able to prepare for threats and prevent accidents.

WHY S2W?

S2W is a data intelligence company that offers innovative solutions through the convergence of technology.

Our goal at S2W is to provide trustworthy AI-based data intelligence. We analyze big data using advanced AI technology and safeguard it within secure boundaries. By detecting hidden data, we uncover relationships between data that were previously unseen and visualize them. Our role and objective are to create a secure data society through an AI-based data intelligence platform developed by a company well-versed in security.

국제 논문

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

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

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

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

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

수상 이력

World Economic Forum
100대 기술선도 스타트업 선정 (2023)

한국 대표 혁신 스타트업 선정 (2022)

Korea AI Startup 100 선정 (2022)

국가정보원 사이버 안보센터 참여기업 (2022)

S2W

info@s2w.inc | +82 70 7008 5278 | www.s2w.inc