Stay ahead of cyber threat

quaxar

quaxar

Cyber Threat Intelligence (CTI) solution for external threat

Quaxar is a CTI solution that enhances the organization's cybersecurity by monitoring and managing external threats that are difficult to detect with internal security systems. It collects vast amount of data from various hidden channels and derives Threat Intelligence(TI) by refining and connecting data.
With the extracted TI, it provides actionable intelligence to preemptively prevent various external threats and to quickly respond to unexpected cyber attacks or detected potential threats.

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.

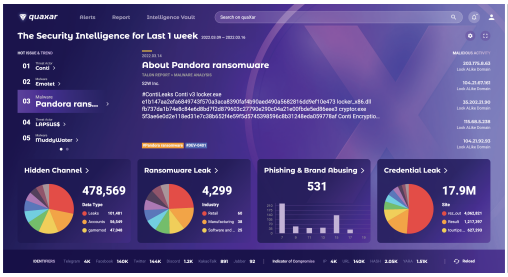
- Takedown Service
- Ransomware Attack Response
- Cloud Account Breach Response

S2W

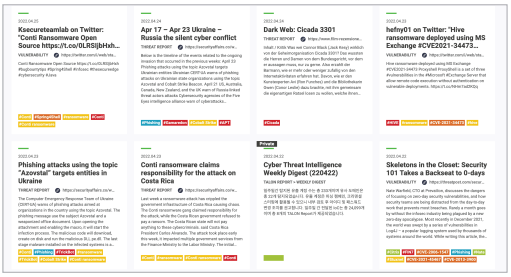
Quaxar Key Features

Dashboard

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



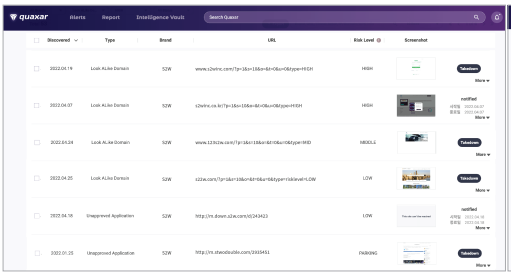
▲ Main Dashboard



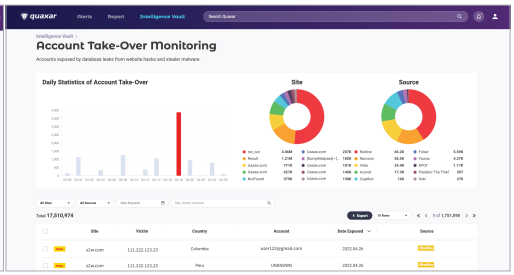
▲ Latest Cyber Threat Related Contents

Digital Risk Protection

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



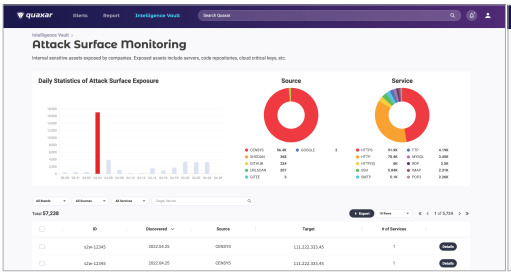
▲ Brand Abuse Site/App Detection



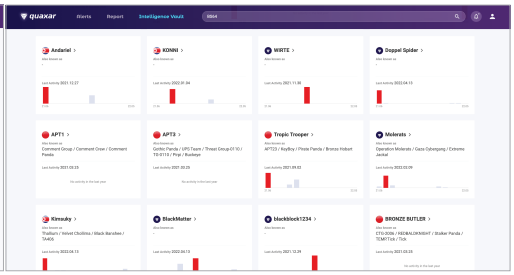
▲ Account Take-Over Monitoring

Threat Intelligence

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



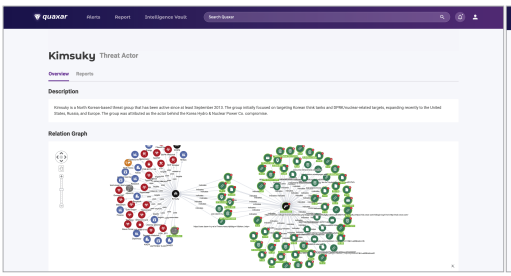
▲ Attack Surface Monitoring



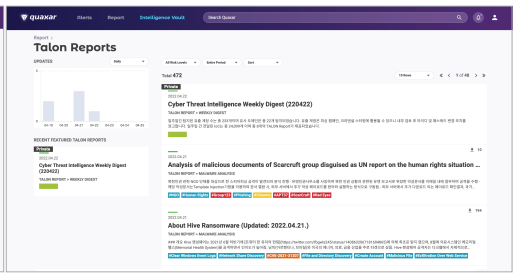
▲ Threat Actor Profiling

Reports

- Talon Reports
- Security News
- Vulnerabilities
- Open IoCs



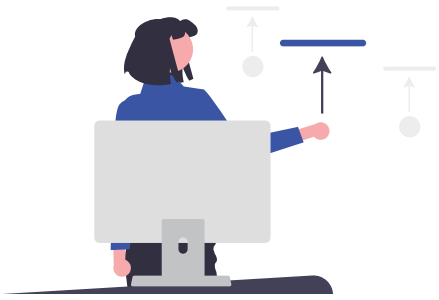
▲ Intelligence Relation Graph



▲ 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.

About S2W

S2W provides intelligence solutions for cyber threats, brand/digital abuse, and virtual assets.

In a data-oriented hyperconnected society, we derive optimal problem-solving methods and propose customized solutions to protect organizations from external threats and realize corporate brand value.

S2W utilizes various big data analysis, machine learning, deep learning, and other technologies to provide Threat Intelligence, Digital Abuse Intelligence, and Virtual Asset Intelligence solutions.

Publications

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)

Patents

Methods and systems for analyzing cryptocurrency transactions

Methods, devices and computer programs for providing cybersecurity using knowledge graphs

Methods and devices for analyzing cryptocurrency transactions

Methods and devices for collecting data in multi-domain

S2W

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