QUAXAR

AI-Powered Cyber Threat Intelligence Platform

S2W

QUAXAR

AI-Powered Cyber Threat Intelligence for Enterprise

QUAXAR is an AI-based Cyber Threat Intelligence (CTI) platform tailored for enterprises. The AI assistant embedded in the platform selects and delivers the threat intelligence your company needs at the moment, from vast amounts of information. It also provides important keywords and trends related to notable cybersecurity threats.
Moreover, QUAXAR allows the management of Digital Risk Protection (DRP), Attack Surface Management (ASM), and Threat Intelligence (TI) within a single platform, providing comprehensive protection for an organization's key assets. With a diverse portfolio of international clients, QUAXAR offers valuable data and expertise for threat detection and response tailored to specific organizations and industries.

Real-time Cyber Threat AI Assistant

QUAXAR ASSISTANT

Today's Major TI issues related to our company(10th Sept, 2024).

- Attacker Distributing Malicious LNK Files Targeting South Korean IT Companies: KONNI (Detailed Report↗)

2 new vulnerabilities affecting our systems have been detected.

- CVE-2021-34473: Microsoft Exchange ProxyShell Vulnerability on the Server (Response Measures ↗)
- CVE-2021-26855: Microsoft Exchange ProxyLogon Vulnerability on the Server (Response Measures ↗)

Organizationa tailored all-round cyber threat intelligence

Digital Risk Protection

Supports organizations in addressing direct and indirect data breaches and brand threats encountered in the digital environment.

- ✓ Account Take Over Monitoring (ATOM)
- ✓ Ransomware Analysis and Monitoring
- ✓ Brand Threat Response Action Tool
- ✓ Provide company and industry insights from the Dark web and Telegram.

Attack Surface Management

Identify and visualize the organization's attack surface, offer insights on unofficial IT assets, assess their impact, and minimize the attack surface.

- ✓ Comprehensive port scan using an in-house scanner
- ✓ Vulnerability assessment and risk evaluation of assets
- ✓ Certificate expiration monitoring system
- ✓ Deliver vulnerability information linked to compromised accounts

Threat Intelligence

Collect and analyze cyber threat information from various channels, informing intelligence to proactively respond to potential threats.

- ✓ Indicators of Compromise (IoCs)
- ✓ Detection rules (Yara,Snort)
- ✓ OSINT(Google,GitHub)
- ✓ Analysis and information on attackers such as major ransomware groups.

S2W

AI-Powered CTI Platform, QUAXAR

QUAXAR Key Features

Corporate Tailored AI Assistant

Provides customized cyber threat status for corporates, along with cybersecurity information and trends.

- Daily briefing
- ASM status for corporate assets
- Corporate data and credential breach status
- Major cybersecurity keywords and trends

AI-Generated Automated Reports

AI auto-report allows organizations to easily create customized reports on their cyber threat status and security -related technology information.

- Corporate customized report (Brand Security Digest)
- Technology information report (Trend Security Digest)

Credential/Data Breach Management

Monitors breach status for corporate crdentials and confidential assets, enabling threat response.

- Deep/Dark web and Telegram monitoring
- Monitoring and detecting compromised account information
- Ransomware group monitoring
- Provide detailed information on threat sources

Brand Threat Management

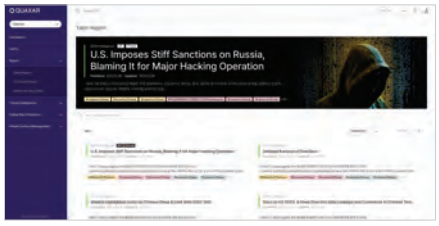
Monitors elements such as corporate brand impersonation and phishing that threaten brand value, offering intelligence for security responses.

- Brand impersonation/Phishing monitoring
- Threat group profiling information
- Indicators of Compromise (IoC)
- Detection rules (Yara/Snort)
- Vulnerability information

Corporate Asset Management

Manage IT assets through scanning entire ports of the attack surface, offering instantly usable intelligence for vulnerable assets.

- Information on vulnerabilities existing in assets
- Account information linked to assets
- Alert and log management for assets requiring attention
- Certificate management



Expert Analyst Support (TALON)

Threat analysis experts support incident response, threat response training, and analysis reports.

- Incident response and investigation
- Expert analysis reports
- Skill up seminars
- Takedown service

S2W

QUAXAR Use Case

[Client A] Proactive Response Case
Proactive Threat Prevention

In 2023, while conducting threat monitoring, S2W detected a post on Breach Forums seeking manufacture company's data. S2W analyst contacted the postwriter to obtain target information and alerted the respective companies.

01 Detected a post on Breach Forums requesting data of manufacture companies.

02 Through conversations with the postwriter, S2W confirmed the type of data being sought and identified the targets. Eight manufacture companies were confirmed as based on domains.

03 Alerted each company with the relevant information and advised them on how to prepare for potential attacks.

[Client B] Proactive Response Case
Source Code Leak

In 2023, during routine monitoring, S2W detected the exposure of asset information containing keywords related to Client B on GitHub. S2W immediately notified the client and recommended corrective actions.

01 QUAXAR detected that certain services, either containing or likely associated with Client B's internal assets, were exposed on GitHub.

02 The exposed sensitive items included internal server access information, such as usernames, passwords, and access keys.

03 It was confirmed that the assets were in use within the internal network and, due to the high risk of sensitive data leakage, advised to block external exposure of the services.

[Client C] Real-Time Response Case
Vulnerability Disclosure

A file uploaded to a Chinese Telegram channel targeting South Korea disclosed an SQL injection vulnerability in a major Korean financial institute's website and shared tips for exploiting such vulnerabilities.

01 Hackers shared the attack script used for the SQL injection.

02 The attackers performed random vulnerability scans on various websites and shared a list of compromised sites in a Chinese Telegram group.

03 They provided useful tips for scanning vulnerabilities specifically on Korean websites.

04 Around 100 other websites were shared besides the major financial institute.

05 S2W alerted the client of the incident and offered guidance on detecting and eliminating the attack vectors.

[Client D] Real-Time Response Case
Credential Data Leak

During virus verification site monitoring, QUAXAR detected a post containing compressed file containing the solution from Company D, which is presumed to be equipment supplied to an S2W client. Upon analysis, it was discovered that the file included critical solution server and configuration information.

01 Various source codes, such as IP addresses and configuration files, required for the operation of Company D's solution server were found in the file.

02 Methods to bypass the solution were identified through comments within the configuration files.

03 S2W requested the virus scanning site to delete the file.

04 To prevent recurrence, S2W analyzed the source of the incident and provided countermeasures.

WHY S2W?

S2W is AI-based data operation company that offers innovative solutions through multi-domain cross-analysis

Our goal at S2W is to provide trustworthy AI-based data operation system. Collect and process vast amount of data and analyze it with the specialized domain language model, and build a knowledge graph based on the data. To secure the confidentiality of the data, we wrap the platform a safeguard. S2W will be an enabler for organizations and businesses to achieve their goals efficiently through user-centric AI technology and data management platforms.

Papers

KDD2025
Covering Cracks in Content Moderation: Delexicalized Distant Supervision for Illicit Drug Jargon Detection

NAACL 2024
Ignore Me But Don't Replace Me: Utilizing Non-Linguistic Elements for Pretraining on the Cybersecurity Domain

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

NDSS 2025
Tweezers: A Framework for Security Event Detection via Event Attribution-centric Tweet Embedding

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

Recent Performance

Microsoft Copilot for Security Partner Ecosystem (2024)

Participation of National Intelligence Service's Cyber Security Center (2022)

World Economic Forum 100 Startups Technology Pioneers (2023)

Korea's leading innovative Startup (2022)

S2W

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