THREATQ™ AND QUAXAR

Technology Segment: Intel Feeds

QUAXAR provides tailored intelligence to enable effective responses to external threats.

1. **Extensive external threat monitoring coverage.**
2. **AI based accurate threat detection and threat source identification.**
3. **Immediately actionable intelligence.**

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ data-driven security operations platform is both open and extensible, supporting the integration of disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

QUAXAR

QUAXAR is a Cyber Threat Intelligence solution that protects the organization's asset and value by monitoring and managing external threats that are difficult to be detected with internal security systems. With outstanding monitoring coverage and analytics, QUAXAR provides immediately actionable intelligence in the event of threats.

INTEGRATION HIGHLIGHTS

Digital risk Protection: Protects the corporate brand and gains the trust from customers.

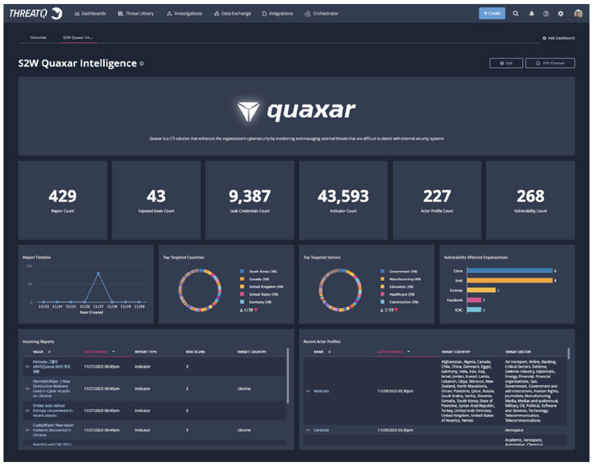
Active threat and vulnerability management: Quickly provides meaningful intelligence against various external threats.

Data breach detection: Detects corporate core asset leakage on the deep/dark web and other channels.

INTEGRATION USE CASES:

The Integration supports a variety of use cases such as:

- **Account take-over monitoring:** Monitors and detects corporate and employee account leaks. This service allows visualization of corporate credential leakage.
- **Attack surface monitoring:** Monitors the attack surface of a corporation. Manages the exposure of corporation's sensitive information that is out of internal control, such as corporate infrastructure, internal assets, etc.
- **Brand abuse monitoring:** Detects brand abuse sites, impersonation phishing sites/apps, and provides take-down services upon request. It protects brand value from related potential threats.
- **Ransomware activity monitoring:** Monitors ransomware attack status and groups. You can view related information, such as victim corporates and leaked files.
- **IoC Database:** Provides immediately applicable IoCs. This enables quick responses to various external threats.
- **Threat actor information:** Provides information about various threat groups, including existing APT groups and active cybercriminals on the Deep/Dark web.
- **Credit card leakage management:** Detects leaked customer credit card account information to prevent additional harm to customers.



S2W Quaxar Intelligence

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

429	43	9,387	43,593	227	268
Report Count	Exposed Asset Count	Leak Credentials Count	Indicator Count	Actor Profile Count	Vulnerability Count

Incoming Reports

VALUE	DATE CREATED	REPORT TYPE	RISK SCORE	TARGET COUNTRY
Kimsuky 그룹의 xRAT(Quasar RAT) 유포 정황	11/27/2023 08:45pm	indicator	3	
HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine	11/27/2023 08:45pm	indicator	3	Ukraine
Dridex bots deliver Entropy ransomware in recent attacks	11/27/2023 08:45pm	indicator	3	
CaddyWiper: New wiper malware discovered in Ukraine	11/27/2023 08:44pm	indicator	3	Ukraine
WatchGuard CVE-2022-				

Recent Actor Profiles

NAME	LAST MODIFIED	TARGET COUNTRY	TARGET SECTOR
Molerats	11/29/2023 03:30pm	Afghanistan, Algeria, Canada, Chile, China, Denmark, Egypt, Germany, India, Iran, Iraq, Israel, Jordan, Kuwait, Latvia, Lebanon, Libya, Morocco, New Zealand, North Macedonia, Oman, Palestine, Qatar, Russia, Saudi Arabia, Serbia, Slovenia, Somalia, South Korea, State of Palestine, Syrian Arab Republic, Turkey, United Arab Emirates, United Kingdom, United States of America, Yemen	Air transport, Airline, Banking, Critical Sectors, Defense, Defense industry, Diplomatic, Energy, Financial, Financial organizations, Gas, Government, Government and administrations, Human Rights, Journalists, Manufacturing, Media, Medias and audiovisual, Military, Oil, Political, Software and Services, Technology, Telecommunication, Telecommunications
Darkside	11/29/2023 03:30pm		Aerospace
			Academic, Aerospace, Automotive, Chemical

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage, vulnerability prioritization and threat intelligence management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For more information, visit www.threatquotient.com.

ABOUT S2W INC.

S2W Inc. is a data intelligence company that utilizes its own advanced technology to effectively collect, refine, and analyze difficult-to-obtain data from sources including the deep/dark web, Telegram, social media, GitHub, and many others. As an official partner of INTERPOL, it offers security solutions in Cyber Threat Intelligence, addressing dark web threats, defending against ransomware, APT attacks, and external threats like phishing. In data intelligence, S2W provides defensive solutions for automatic analysis and detection of internal data in commerce and service platforms. S2W gained significant global recognition by unveiling the dark web-specific artificial intelligence language model 'DarkBERT'.