Threatquotient™ and Cybersixgill Darkfeed™

Technology Segment: Threat Intelligence

Darkfeed ✚ **THREATQUOTIENT**

Key Solution Benefits:

- **Automatically integrate IOCs** into the ThreatQ platform (machine-to-machine)

- **Supercharge ThreatQ** with seamless integration of contextual data in real-time

- **Receive automated early warnings** of new malware threats

- **Get actionable insights** to effectively mitigate threats

- **Level-up your threat hunting** for malicious IOCs in corporate networks

- **Better understand malware** TTPs and trends

Predictive Actionable Threat Intelligence

The combination of Darkfeed and the ThreatQ threat intelligence platform delivers actionable threat intelligence to organizations. When connected to the ThreatQ platform, Darkfeed's predictive indicators from undercover sources provide your SOC with insights into unique threats with deeper context so users can take swift and confident action.

ThreatQuotient

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates 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.

Cybersixgill Darkfeed

Darkfeed is the industry's most comprehensive deep and dark web intelligence stream of IOCs. With Darkfeed, ThreatQ users can get early warnings of malware threats and block items that compromise their organization.

Powered by Cybersixgill's intelligence collection, Darkfeed is based on the widest and deepest closed data sources available on the market today. This contextual threat intelligence stream is highly accurate, covert, and fully automated.

The feed is structured in the STIX format allowing ThreatQ users to automatically consume and integrate it with their security systems, processes and methodologies.

cybersixgill

The Integration supports a variety of use cases such as:

Preventing Attacks

Darkfeed is sourced from underground sources where cyber-criminals buy and sell domains, URLs, malware and post compromised IP addresses. By providing these indicators directly from the underground, Darkfeed gets you ahead of a threat instead of reacting to an attack.

Incident Investigation

Darkfeed provides critical information around each indicator, such as threat actor name, forum, and title of the post from underground sources to accelerate your response or investigation.

Threat Hunting

Darkfeed's deeper context enables you to not only react to an indicator in your network, but also pivot to all indicators from an actor, allowing you to understand a campaign and take appropriate widespread action.

THREATQUOTIENT

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations with a platform that accelerates and simplifies investigations and collaboration within and across teams and tools. Integrating an organization's existing processes and technologies into a unified workspace, ThreatQuotient's solutions reduce noise, highlight top priority threats and automate processes to provide greater focus and decision support while maximizing limited resources. ThreatQuotient's threat-centric approach supports multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability management, and also serves as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For more information, visit threatquotient.com
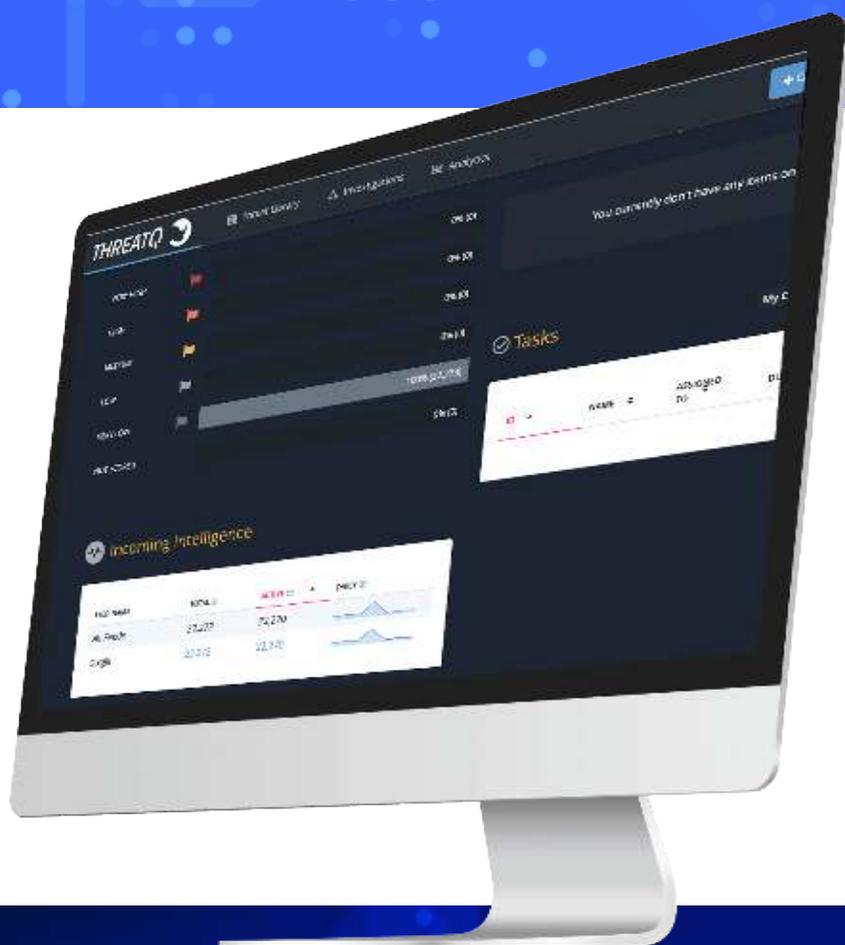
cybersixgill

Cybersixgill's fully automated threat intelligence solutions help organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response – in real-time. The Cybersixgill Investigative Portal empowers security teams with contextual and actionable insights as well as the ability to conduct real-time investigations. Rich data feeds such as Darkfeed™ and DVE Score™ harness Cybersixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems. Most recently, Cybersixgill introduced agility to threat intel with their CI/CP methodology (Continuous Investigation/Continuous Protection). Current customers include enterprises, financial services, MSSPs, governments and law enforcement entities.

To learn more, visit www.cybersixgill.com and follow us on Twitter: @cybersixgill and LinkedIn.