FMBusinessDaily

ThreatQuotient Enables Companies to Scale Security Operations Through Effective and Efficient Use of Threat Intelligence

10 months ago

ThreatQuotient™, a leading security operations platform innovator, recently announced Version 6 of the ThreatQ Platform, a major upgrade with significant enhancements to the platform and multiple modules. Dedicated to providing security operations centre (SOC) and cyber threat intelligence analysts with a simplified, data-driven approach to automating their work, the ThreatQ Platform has more than 30 new feature innovations and improvements since version 5.0.

- Scaling collaboration with easy intelligence sharing

With industries experiencing more attacks than ever before, collaborating and sharing threat intelligence is a vital capability to scale security operations. The platform focuses on human workflow management combined with data-driven automation, enabling internal teams to scale processes quickly to be more effective and to deliver more efficacy in their outcomes. It achieves this through a fine balance of human know-how combined with automation and machine intelligence.

The platform enables not only the quick sharing of threat intelligence but also a host of new integrations and enhanced STIX2.1/TAXII interoperability, providing superior ecosystem partner support. In the past 12 months, the number of available workflow actions has doubled to deliver further momentum to the ThreatQ Marketplace, including key use cases such as automated hunting in multiple SIEM platforms.

Leon Ward, Vice President Product Management, ThreatQuotient comments:

“Organisations have never experienced the volume and impact of attacks that they’ve witnessed in recent quarters, but on the positive side, defenders collectively have never had so much hands-on experience in responding to those same incidents. Through collaboration and sharing, defences can be scaled so others are able to respond faster and more accurately, which is what we aim to do through the enhancements that we have built into the ThreatQ Platform. Sharing of key intelligence at scale with third parties has never been easier through the new integrated TAXII server included in ThreatQ Data Exchange.”

- Scaling workflows by combining humans, automation, and AI

The ThreatQ Platform delivers scalable workflows that strike a balance between human management and automation. ThreatQ ACE uses natural language processing and keyword matching to automatically identify and extract valuable threat intelligence from unstructured text in data feeds.

Additionally, the platform has powerful integrations with generative AI tools such as ChatGPT to accelerate contextual information gathering and sharing. Security professionals can leverage generative AI through the ThreatQ Platform to draft plain text descriptions of detected threats.

- Scaling the ecosystem with the ThreatQ Integration Framework

ThreatQuotient delivers automation, scale, sharing and seamless support via an ecosystem of over 450 product and feed integrations available from its online marketplace. Integrations include intelligence feeds, security tools, enrichment services, sandboxes, and many more. In addition, ThreatQuotient provides the ThreatQ Integration Framework with intuitive tools to customise integrations or build custom integrations from scratch. ThreatQuotient continues to develop new capabilities to improve the user experience for analysts. This includes Batch Actions, a capability focused on the ticketing use case that enables users to reduce their workload by easily batching related tickets for remediation (e.g. a single ticket for a CVE that lists affected systems that need to be remediated instead of a ticket per system).

ThreatQuotient customer Thales has deep experience of using the ThreatQ Platform to scale its advanced, personalised threat intelligence service. The company has built one of the largest Cyber Threat Intelligence Services in Europe using the ThreatQ Platform delivering tailored, prioritised threat intelligence drawn from diverse threat data sources and cybersecurity tools. Ivan Fontarensky, Technical Director, CyberDetect and Response at Thales, said: “Our partnership with ThreatQuotient has helped us grow from a team of one to 50 in a few years and become the largest CTI provider in Europe. Today threat intelligence is strategic to our cybersecurity products and research and to our continued market leadership.”

The latest cybersecurity automation research from ThreatQuotient, which will launch in November 2024, highlights that to fight today’s adversaries, threat intelligence teams need to scale their capabilities. The research highlights that automation is providing tangible benefits in a continuously unpredictable environment with 98% of survey respondents seeing budget increases for cybersecurity automation and nearly 40% now securing net new budgets rather than diverting it from other areas. Additionally, trust in cybersecurity automation is rising as users gain confidence. The research reveals that more than half of organisations regularly share threat intelligence with partners and suppliers and 48% share threat intelligence through official industry channels, which underlines the value of developing solutions that enable faster and more comprehensive intelligence sharing.

In the last 12 months, ThreatQuotient has taken additional steps to partner with more industry peers, and recently announced that the ThreatQ Platform is now available in AWS Marketplace. ThreatQuotient's mission is to enable cybersecurity teams to optimise threat detection, investigation, and response. Additionally, as it has focused on extending its ecosystem, earlier this year it announced its membership in the Electricity Information Sharing and Analysis Centre's (E-ISAC) vendor affiliate program. This partnership marks a significant step forward in fortifying the cybersecurity defences of North America's electricity grid against evolving threats.

To learn more about the latest integrations and features available within the ThreatQ Platform, request a demo or visit our ThreatQ v6 resources for more information.