NEWS RELEASE

ThreatQuotient Bridges Artificial Intelligence with Threat Intelligence in the SOC

10/3/2023

Security operations teams work smarter, not harder, with the latest enhancements to the ThreatQ Platform including ThreatQ TDR Orchestrator and a data-driven approach to automation

ASHBURN, Va.--(BUSINESS WIRE)-- **ThreatQuotient™**, a leading security operations platform innovator, is announcing key enhancements to ThreatQ and **ThreatQ TDR Orchestrator**. Since ThreatQuotient was founded in 2013, the company has provided security operations center (SOC) analysts with a simplified, data-driven approach to automating their work that disrupted the prior standards of process-driven SOAR platforms. The continued innovation of the ThreatQ Platform and ThreatQ TDR Orchestrator bolsters prior investment in machine learning (ML). Now, capabilities focus on merging automation, artificial intelligence (AI) and threat intelligence, with new integrations for generative AI and natural language processing (NLP).

The **latest research** from ThreatQuotient, planned for full release in November 2023, digs into the state of adopting cybersecurity automation across industry verticals and regions and offers a wide range of insights. One finding that is especially clear is that hiring and retaining enough people to fill necessary security roles is only getting harder, and ThreatQuotient's research confirms that one of the top challenges facing security leaders today is high employee turnover rates. The data also shows that for leaders surveyed in the study, the number one way to address this challenge will be with smarter tools that simplify work. Additionally, over 60% of leaders expect automation to positively affect employee satisfaction and retention.

To address these challenges and support the evolving needs of security teams, the latest version of the ThreatQ Platform and ThreatQ TDR Orchestrator includes the following advancements:

- Generative AI
  A new, powerful integration between ThreatQ and Generative AI, such as **ChatGPT**, enables security professionals to quickly gather contextual information on elements like indicators, adversaries, malware and many others to optimize threat detection and response. The integration solves a wide range of problems from crafting plain-text descriptions for reports, emails, and collaboration with other teams, to acquiring additional contextual information and generating recommendations.

- ACE workflows
  ThreatQ ACE is a sophisticated tool that harnesses the power of natural language processing and keyword matching to automatically identify and extract valuable threat intelligence. This is particularly useful for extracting content from unstructured text in data feeds, as well as parsing reports, files, or PDFs already in a customer's ThreatQ Threat Library.

- A growing marketplace
  ThreatQ now supports an ecosystem of nearly 400 product and feed integrations available from an online marketplace. Integrations include intelligence feeds, security tools, enrichment services, sandboxes, and many more. In addition, ThreatQ provides easy-to-use tools to customize these integrations or build custom integrations from scratch. In addition to releasing new integrations regularly, ThreatQ continues to develop new capabilities within the integrations such as Batch Actions. This capability is focused on the ticketing use case enabling 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 has been helping security teams work smarter **for years** with no-code solutions like ThreatQ TDR Orchestrator. We are committed to continuously meeting the needs of SOC leaders and analysts through ongoing product innovation,” said Leon Ward, Vice President of Product Management, ThreatQuotient. “Our tools are built to enable more experienced analysts to achieve their desired outcomes faster, and to help less experienced analysts build their skills and contribute positively to their teams. With these latest capabilities, ThreatQuotient is providing faster access to contextual information and valuable insights for effective threat detection and response.”

Eric Hoffman, Director of Partners and Alliances at GreyNoise, a ThreatQuotient integration partner, added, “Heading into the rest of 2023 and beyond, automation of any kind can be expected to produce efficiency gains. As the market matures, what separates the leader is the ability to produce gains in areas outside basic efficiency. ThreatQuotient’s integrations with ChatGPT, along with other forms of AI like NLP and ML, demonstrates the power of these technologies that organizations should harness to better protect their assets. The future of cybersecurity relies on collaboration between human expertise and AI advancements, using AI to augment the human ability to adapt and solve problems. We look forward to deepening GreyNoise’s work with ThreatQuotient to help forge stronger defenses against evolving threats.”

In the last 12 months, ThreatQuotient has taken additional steps to assist with closing the security skills gap. For example, through the launch of **ThreatQ Academy Online** earlier this year, ThreatQuotient is enabling stronger staff retention and supporting existing employees with custom online training that allows them to grow and gain skills for more security operations roles.

To learn more about the latest integrations and features available within ThreatQ TDR Orchestrator, which is built into the ThreatQ Platform, **request a demo** or visit our resources page of **automation use cases**. For more of ThreatQuotient's perspective on AI in security operations, **read our blog**.

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 and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit **www.threatquotient.com.**

Media Contact (North America)

Taylor Hadley
LaunchTech Communications for ThreatQuotient
(978) 877-2113
taylor@golaunchtech.com

Source: ThreatQuotient