THREATQUOTIENT

CUSTOMER SUCCESS STORY

Global Software Company Focuses on 5 Use Cases with ThreatQ

A U.S.-based, global software company providing cloud computing, virtualization and security software needed a centralized platform to improve security monitoring and accelerate detection and response.

Challenge

The global software company needed a more efficient and effective way to use their multiple sources of threat intelligence to understand and mitigate the risk of attacks. As they sifted through all the intelligence, it was difficult and time-consuming to correlate the activity in the wild with the threats they should look for and be concerned about in their environment. They needed a streamlined way to identify which groups were targeting them, which vulnerabilities to prioritize for patching based on these risks, and how attacks targeting their ecosystem of partners could put their customers, employees and infrastructure at risk.

- Ingesting data from open source, internal and commercial feeds
- Focusing on active threats to look for in their environment
- Prioritizing and managing vulnerabilities

"We needed to arm our threat intelligence analysts with a robust platform that would allow them to more rapidly assess and respond to cyber security threats targeting the company," said Senior Threat Intelligence Analyst. "Automation and collaboration were going to be critical since our team is small and dispersed across the globe in a follow-the-sun model."

Solution

The customer needed a platform that would serve as a centralized repository for all threat intelligence and enable the team to work efficiently and effectively across the five phases of the intelligence cycle — planning, collection, processing, enrichment and dissemination. They identified the following success criteria:

- Feed aggregation of their open source and premium intelligence services that include reports and indicator feeds.
- Data enrichment including the ability to build relationships between indicators and adding contextual information from internal systems.
- Prioritization to understand which threats to focus on first based on attackers' tools, techniques and procedures (TTPs) correlated with the organization's vulnerabilities and risk profile.
- Reporting capabilities so that analysts could quickly produce finished reports for executives detailing relevance to their threat landscape.
- A centralized library of all external and internal threat and event data, reports, digests and briefs in one, searchable location for a single source of truth.
- Collaboration capability to work with internal teams, tracking and coordinating activities to support investigations and reporting.
- Ability to share indicators with context with external groups as needed.

After an extensive evaluation of three vendors the company selected ThreatQ, determining it met all the

OVERVIEW

INDUSTRY: Global Technology Company

CUSTOMER SINCE: 2018

EMPLOYEES: 24,000+

REVENUE: 8 Billion+

LOCATION: Headquartered in US

CHALLENGE

Ingesting and prioritizing threat intelligence to be used in threat hunting, threat management, spear phishing, incident response and vulnerability management.

SOLUTION

Through automation and collaboration, the ThreatQ platform enables analysts to rapidly assess and respond to threats, collecting, correlating, evaluating and disseminating intelligence across a comprehensive portfolio of sources and technologies.

OUTCOME

- ✔ Increased efficiency and effectiveness of teams and technologies
- ✔ Accelerated turn-around time across five priority use cases
- ✔ Finished executive reports tracking key metrics
- ✔ Better ROI on existing security infrastructure

success criteria. ThreatQ is currently being used to support key use cases, including threat management, threat hunting, spear phishing investigations, incident response and vulnerability management. With the ability to score and filter threat data based on parameters the analyst team sets, they can understand threats to their environment for better threat management and prioritize activities such as which vulnerabilities to patch first. Threat intelligence is automatically reprioritized as new data and learnings are added to the platform. Fusing together threat data, evidence and users, all team members involved in an investigation can work together, be it to thwart spear phishing campaigns, hunt for threats, or accelerate incident response. Embedding collaboration into the investigation process ensures that teams work together efficiently to take the right actions faster to more effectively mitigate risk. Hand-offs across analysts, teams and time zones is seamless, which is important with team members in different geographies.

"ThreatQ is able to support our threat intelligence and investigation processes — we weren't forced to change our methods — and they did this with out-of-the-box integrations to our incoming feeds, complementary security tools and defensive controls. The addition of automation and collaboration at key points in the threat intelligence cycle takes our security monitoring, detection and response capabilities to new levels."

- Senior Threat Intelligence Analyst.

Outcome

Accelerated turn-around time

The combination of automation for data aggregation, correlation, prioritization and disseminating threat intelligence across all systems and teams, together with collaboration during the investigation process, allows the team to accelerate detection and response.

Standardized reporting templates

ThreatQ helps streamline reporting to key executives with templates designed to focus on metrics and findings delivered using business terms that resonate.

Single source of truth

All data is aggregated in a central repository that analysts can update with observations, learnings and documentation of investigations to help keep intelligence current and relevant, and drive further analyst productivity and efficiency.

Support for five use cases

The security team is using ThreatQ to improve security operations across five use cases: threat management, spear phishing investigations, threat hunting, incident response and vulnerability management.

Integration of technology with the infrastructure giving better ROI

Through a software development kit (SDK) and easy-to-use application programming interfaces (APIs), ThreatQ fully integrates with the customer's existing tools and technologies to extend and enhance the value of their existing security investments.

Work within their processes rather than adapt to a tool

Analysts can access the intelligence they need to do their jobs as part of their workflow using the tools they are accustomed to, and collaborate in a seamless environment to see the work of others and accelerate their investigations.

As the customer continues to use ThreatQ they are expanding the integration with additional enrichment and analysis tools within their existing security infrastructure. They are also increasing their threat hunting capabilities to include proactive threat hunting, where they learn of a threat from an external report and hunt for associated indicators within their environment. ThreatQ provides the context they need to ensure they don't waste time chasing ghosts, and the ability to collaborate to explore every corner of the organization to pinpoint adversary TTPs and find malicious activity for total remediation.

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA. For more information, visit **www.threatquotient.com**.