CASE STUDY

Augmented Intelligence: Managed Security Service Provider Strengthens its Threat Intelligence with ThreatQuotient

Overview

"Since 2011, our threat intelligence service has worked very closely with our incident response teams. Among other things, this has allowed us to be very relevant and responsive when it comes to tracking attackers," explains the Product Manager for the Managed Security Service Provider.

This proximity has paid off, enabling the service to better contextualize alerts that would otherwise remain purely technical, such as lists of IP addresses and other indicators of compromise (IoCs). Technical alerts are effective in blocking specific attacks, often in an automated way. However, when they are enriched with relevant, contextual information they can become real decision-making tools allowing security analysts to answer questions, such as: What do we know about the attacker's current targets and campaigns? Are we a potential target for this group in particular?

In theory this is attractive, but to deliver this in practice the MSSP needed to be equipped to offer a robust, industry-ready service. "In 2015, we decided to create a dissemination offering that would allow customers operating their own SOC to benefit from this increased information. We first worked with flat files, and then we deployed MISP interfaces for our customers," continues the Product Manager.

Difficulty caling up

MISP (Malware Information Sharing Platform) is a must in the world of threat intelligence. Available as a free solution, MISP facilitates the sharing of IoCs between researchers. But before IoCs can be shared, they must be acquired and consolidated. This is where things get complicated. The Product Manager recalls, "MISP is very good for dissemination, but ingestion is not simple! We were forced to use many other open source tools in parallel, requiring a lot of scripting and manual operations before delivering the information to our customers, while remaining within the timeframes allowed by our SLAs."

"ThreatQ allows us to offer a richer threat intelligence service, with more context, but also faster. We are now able to continuously deliver cyber intelligence flows tailored to the needs of our customers."

- Product Manager for the Managed Security Service Provider

THE THREATQUOTIENT SOLUTION ALLOWS:

Enabling the service to better contextualize alerts

Customers to operate their own SOC

Customers to have the freedom to change their threat intelligence feeds and sources at any time

Analysts to respond better and faster to customer requests

To refine the information delivered to customers in order to better manage security posture

The dissemination service became so successful that the load on the MSSP Threat Intelligence team increased dramatically. As customers demanded more and more context and richer information, beyond what MISP can do with its tagging and commenting functionalities, it quickly became clear that a manual approach could not be scaled up.

The MSSP team then decided to research a new "cyber-intelligence back office" — a tool capable of natively managing concepts such as the freshness of information, reliability, context, and related data.

"We quickly saw in ThreatQuotient the vendor best suited to our needs. We shared the same vocabulary (coming from the defense sector). The ThreatQ platform met our criteria, and the technical level of the ThreatQuotient subject matter experts was excellent," explains the Product Manager.

From weekly delivery to continuous information

The deployment of ThreatQ allows the MSSP to meet their goals. "We can now deliver the same service and the same knowledge, with the same quality as before, but much more quickly and with far fewer technical manipulations," details the Product Manager. "And, obviously, it's our customers who benefit. The MSSP has gone from weekly information delivery to continuous information delivery."

Better still, for slightly more mature customers, who do not yet operate their own SOC, but still have an internal CSIRT team, the MSSP team can now offer an optional tool capable of helping them capitalize on their knowledge. The knowledge acquired during the customer's internal investigations is seamlessly integrated into the ThreatQ platform to enrich the information delivered back to the customer via the MSSP's service.

The ThreatQ platform is completely complementary to an existing MISP solution, allowing the customer to build up their own knowledge base adapted with their context. Customers also have the freedom to change their threat intelligence feeds and sources at any time, since they will keep all of their data within the ThreatQ Threat Library and therefore all the knowledge acquired by their CSIRT.

Better responsiveness in times of crisis

The ThreatQuotient solution allows the MSSP analysts to respond better and faster to customer requests. "Most SOCs work with a workflow system to investigate IoCs collected during an incident. It is often a manual process but since the ThreatQ platform can be integrated with a SIEM to do the research and automatically identify patterns and linkages and how to pivot from a given IoC, we have even been able to reduce our response time to our customers," says the Product Manager. "And obviously, in an incident, quickly identifying the pivots and monitoring malicious activities as closely as possible is a major advantage."

Personalized information

Finally, the choice of the ThreatQuotient solution allowed the MSSP to refine the information delivered to customers in order to better manage their security posture. The ThreatQ platform makes it possible to automatically "package" the most relevant flows according to the exposure of the client to specific risks, and thus take a strategic approach to mitigate risk.

ThreatQuotient improves security operations by fusing together disparate data sources, and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams 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. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC. For more information, visit **www.threatquotient.com**.

Sales@ThreatQ.com • 703.574.9885