THREATQUOTIENT

CUSTOMER SUCCESS STORY

Accelerating Detection and Response with ThreatQ

A U.S.-based, global financial services firm prides itself on helping its customers manage risks so that they can better realize their full potential. Now the firm needed a way to unleash the full potential of its existing resources to better manage its own risks.

Challenge

The financial services firm subscribes to numerous global threat data feeds from multiple sources and also receives a continuous and growing volume of log and event data from their internal defenses and SIEM. Disparate information in different places had become unwieldy. Because their tools didn't work together, analysts had to switch between several portals to view the data, manually pull what appeared to be relevant based on which threat actor group was currently the subject of review, and then figure out what steps to take and how.

Disparate threat data; both external and internal

• • •

Updating internal control with the latest IOCs

• • •

Thinly staffed security operations teams

• • •

Siloed organizations

> ***"Ad-hoc analysis and action was time consuming, disjointed and inefficient … When we weren't putting out fires, we were reacting to the next big attack in the news and urgent calls from management."***
>
> *~ Security Engineer*

Solution

The customer needed a platform to aggregate all external and internal threat and event data in one place to help them assess risks and take action. They wanted a way to use threat intelligence for security operations through a single control point. The team had the following key requirements:

- The platform had to be on-premises so that they could have complete control of their data and the security of it.
- It had to support existing and future data feeds and allow for customization. When doing their research, the evaluation team found that some vendors had built-in data feeds you can't turn off, so if they aren't relevant to your environment they just create more noise.
- They needed the ability to automatically apply business context to external data coming in and make the data relevant to the organization's pressing issues, so they could prioritize and focus their efforts.
- The platform also needed to provide centralized management and control over the distribution of data to internal security controls in an automated fashion.

OVERVIEW

INDUSTRY: Financial Services

CUSTOMER SINCE: 2017

EMPLOYEES: 2,000+

REVENUE: 4 Billion+

LOCATION: US

DEPLOYMENT: On-Premises

CHALLENGE

Disparate threat data in different places and ad-hoc analysis and action by siloed teams was time consuming, disjointed and inefficient.

SOLUTION

The ThreatQ platform allows teams and technologies to work together to detect relevant, priority threats and accelerate response, including automatically updating security controls.

OUTCOME

✔ Proactively detect and respond to threats within hours or days

✔ More effectively use existing resources without retooling

✔ Demonstrate business impact and ROI from security operations

> ***"We now have IoC data from trusted sources being sent proactively to detection-only watch lists in various internal security controls, without daily oversight required by the team's personnel … What's more, because we're selectively exporting data to the tool specifically designed to consume it, we aren't pushing massive amount of data across the network and slowing things down."***
>
> *~ Director of Threat Response*

The firm selected ThreatQ after making the determination that it met all these requirements. ThreatQ is continuously updated with global threat data from the firm's existing feeds and enriched with internal threat, event, and incident data for context. With the ability to score and filter threat data based on parameters the firm sets, threat intelligence is continuously prioritized and reprioritized. Every member of the security team, even those who aren't highly technical, can access the relevant threat intelligence they need to do their jobs and can continue to use the security tools they already know and rely on. ThreatQ also supports bidirectional integration so that threat and event data can be imported from the SIEM, ticketing system and other security tools into the TIP to add context and relevance to global threat data. Threat intelligence can also be exported as part of existing workflows and processes to the SIEM and layers of defenses to strengthen defenses.

Outcome

With the ThreatQ platform, the customer's security teams and tools work together to detect specific incidents and take action in a matter of hours or days.

Accelerated Security Operations

ThreatQ addresses the security team's requirement for control and customization so they can make better use of the resources they already have to accelerate their security operations.

Data Ownership and Control

The on-premises platform allows them to maintain ownership of their data and control data sharing.

Flexibility

The flexibility and openness of the platform through custom connectors make it highly configurable to work with whatever processes, data and tools they have within the organization, without any rearchitecting required.

> ***"ThreatQ provides improved visibility into the nature of activity that may be taking place on the company's networks or assets, and near real-time inclusion of trusted IoC data into internal security controls so we can be more proactive and act with confidence."***
>
> *~ Director of Threat Response*

The customer is seeing how ThreatQ naturally becomes more and more robust over time. The cyber threat intelligence and incident response teams use this centralized repository to keep and share their data and work, allowing everyone to work more efficiently and effectively. Because ThreatQ allows custom data models to be applied and their tools are no longer siloed, they have traceability from indicators to attribution to business impact, which allows them to demonstrate increased ROI from their security operations.

Just as they do for their own clients, they are better managing risk to unleash the full potential of their business.

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 and APAC. For more information, visit **www.threatquotient.com**.