THREATQUOTIENT

USE CASE

Threat Intelligence Management

The Challenge

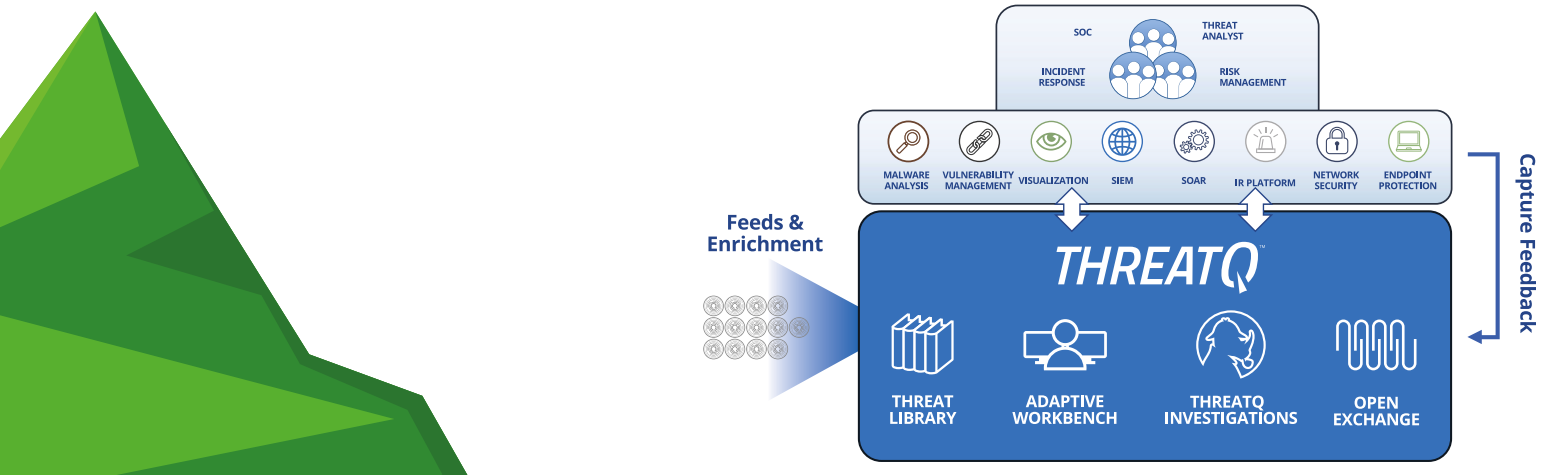
Analysts are bombarded with millions of threat data points every day from multiple sources in multiple formats. This includes external data from commercial sources, open source, industry and existing security vendors as well as internal sources. Each point product within their internal layers of defense, SIEM and other systems within their security infrastructure generates a massive amount of log and event data and alerts. The noise level is deafening.

Resources are scarce, so they pursue what seems high priority and go through a tedious and time-consuming process of manually correlating logs and events to see what is relevant and merits further investigation. Inevitably, they uncover conflicting information and duplication, which results in increasing confusion.

A New Approach

Analysts need a way to automatically ingest, consolidate, normalize and de-duplicate threat intelligence data in one manageable location. While this external cyber threat data is commonly well-defined and understood, additional context from within the organization can vary wildly between industry verticals and companies. It's vital that the solution be able to consume and store these different data types as well as provide the capability to tailor data models to fit security teams' needs.

The next step is to prioritize the vast amounts of threat data aggregated in this central repository. However, what is a priority to one company may not be relevant to another. What is needed is the ability for analysts to control how scoring, prioritization and expiration should be done — tell the system what is more important and less important once, and let the system automatically score and re-score when new data and context is learned. As more data



Security teams can operate from a single source of truth, passively collaborating through the instantaneous sharing of knowledge and using their tools of choice to improve security posture and reduce the window of exposure and breach.

comes in, the system will automatically tune itself, creating a threat library that provides consistent information tailored specifically for the company.

The repository serves as a centralized memory to facilitate future investigations. Security teams can operate from a single source of truth, passively collaborating through the instantaneous sharing of knowledge and using their tools of choice to improve security posture and reduce the window of exposure and breach.

Integration with an ecosystem of data sources is streamlined and cost effective using open APIs at no additional cost, and can be further tailored with an SDK. For broad visibility, the system must be designed to be integrated with all systems that provide or leverage threat data within the organization.

How ThreatQ meets the Threat Intelligence Management Challenge

- **Customer-defined Scoring:** Prioritize threat data automatically, understand why it is relevant and take action faster and with greater confidence.
- **Open Exchange:** Integrate ThreatQ with existing security tools, teams and workflows through standard interfaces to extend their value, knowledge and efficacy.
- **Threat Data Aggregation:** Create a single source of truth based on correlated, normalized and de-duplicated intelligence data and events across all tools and sources.
- **Threat Library:** Store global and local threat data in a central repository to provide relevant and contextual intelligence that is customized and prioritized for your unique environment.
- **Unstructured Data Import:** Parse and perform deep searching on documents and intelligence reports for threat data and clues as to the meaning of threats.

Outcomes

- Contextualized, relevant intelligence in a database that is customized for the organization's environment and risk profile.
- Focus, noise reduction and decision support during investigations and triage.
- Greater understanding of relationships across objects and object types to better support investigations and intelligence management.
- The freedom to spend more time performing analysis versus manual tasks.
- Threat intelligence is orchestrated and synchronized across all teams and tools so they can work in concert and increase effectiveness, efficiency and productivity.

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**.