THREATQUOTIENT

USE CASE

Incident Response

The Challenge

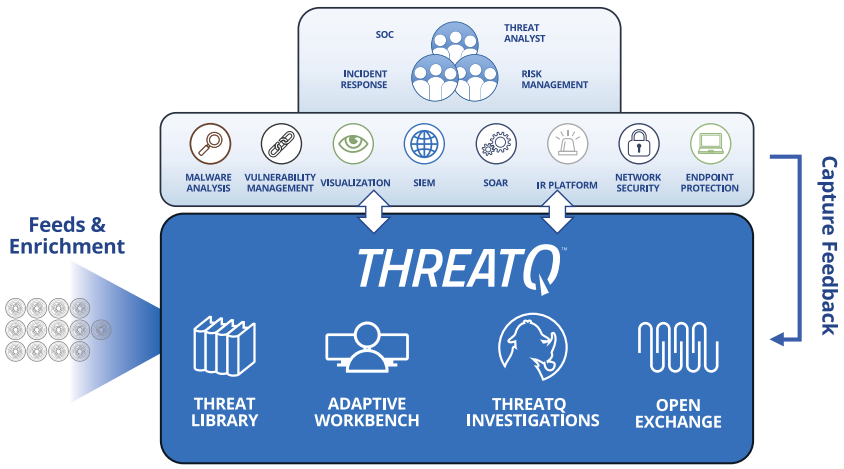
Once an event/alert is escalated to an incident, the investigation gains resources and visibility. Additional efforts need to be applied as quickly as possible to understand the scope, impact and the actions required to mitigate damage and recover. Gathering all the required information is a difficult and often manual process, and it comes in a great variety of formats from many different teams and tools.

If an incident under investigation can be related to a known campaign or adversary, the analysis and response time can be drastically reduced, since key tactics, techniques and procedures (TTPs) are already documented providing the proverbial breadcrumbs that lead to hiding places to look. Maintaining adversary profiles and historical incident response (IR) reports provides a jumpstart to any incident response investigation. But there is typically no central repository to store, share and update key learnings across teams, and no easy way to work collaboratively to accelerate investigation and response.

Our Approach

ThreatQ and ThreatQ Investigations are designed to support the fact that incident response is a team sport. Start by importing an event/investigation along with any peripheral intelligence into a shared investigation environment. This instantly allows an incident responder to quickly assess what other research has been performed and by whom, what tasks need to be assigned, and how all the data relates. The ability to include the necessary resources from outside the immediate security department (i.e., database administrators, application specialists, etc.) ensures complete situational understanding and engages the full set of capabilities of the organization. As the necessary responders from around the organization complete tasks and publish them to the larger incident canvas, the team progresses towards identifying patient-0 and re-arming the organization against the next wave of attacks.

If a team knows their attackers' tactics, techniques and procedures (TTPs), then as that intelligence comes in, they can be scored appropriately and even be added to



> *When adversary profiles are frequently updated and maintained with the latest attributes, new analysts can learn about the adversary exponentially faster.*

a "watchlist" for visibility. This is a subtle and proactive way to keep a finger on the pulse of malicious activity. When adversary profiles are frequently updated and maintained with the latest attributes, new analysts can learn about the adversary exponentially faster.

IR teams tend to work within specialized IR platforms. A two-way integration with a threat intelligence platform ensures that the user can focus on their processes and procedures without the need to switch back and forth between multiple interfaces and platforms.

Documenting investigations that can be correlated to future cases, results in organizational memory and ability to correlate investigations that may have seemed to be separate, but are in fact part of a single campaign.

How ThreatQ meets the Incident Response Challenge

- **Timelines:** Document a chronological record of an incident automatically, and relate it to key events and breach artifacts.
- **Customer-defined Scoring:** Prioritize threat data automatically, understand why it is relevant and take action faster and with greater confidence.
- **Collaboration:** Share indicators, relevant data, events and incidents with different members of the team automatically and simultaneously as well as external parties through reporting and export capabilities.
- **Watchlist:** Add specific IoCs, adversaries or other threat-related data to your dashboard to highlight changes.
- **Tasking:** Collaborate and coordinate response and investigations between members of cross functional teams.
- **Threat Library Search:** Quickly research and understand context behind possible threats by keyword, attribute and object name. Group and pivot on associated data and quickly take bulk actions across a full group of data.
- **Open Exchange:** Integrate ThreatQ with existing security tools, teams and workflows through standard interfaces to extend their value, knowledge and efficacy.
- **Reporting:** Build strategic, operational and tactical reports — including those for malware, campaigns and adversaries to share with other teams, management or clients.

Outcomes

- Better analysis is performed.
- Faster response time and time to resolution.
- More incidents can be completed.
- Current incident resolution is faster by applying past learnings.
- Better team collaboration and productivity.
- Increased new hire 'time-to-value' (TTV).
- Faster and more complete understanding of how to orchestrate a coordinated response.

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**.