THREATQUOTIENT

PRODUCT BRIEF

ThreatQ Investigations

Take the Right Actions, Faster

Introducing the industry's first cybersecurity situation room designed for collaborative threat analysis, shared understanding and coordinated response. ThreatQ™ Investigations embeds visualization and documentation in a single, shared environment for a greater understanding and focus throughout the analysis process.

It provides a unique window into the chaotic world of threats, incidents and operations where multiple people and teams are working on related, yet separate tasks.

ThreatQ Investigations is built on top of the ThreatQ Platform and allows for capturing, learning and sharing of knowledge. This results in a single visual representation of the complete investigation at hand, who did what and when, based on a shared understanding of all components of the investigation -- threat data, evidence and users.

With security teams dispersed all over the world, it becomes more and more difficult to collaborate and coordinate both within and across teams in an organization. ThreatQ Investigations streamlines collaboration while also giving individuals the freedom to test theories prior to sharing with the group to ensure accuracy and relevance. Team leaders can direct actions, assigning tasks and seeing the results unfold in near real-time.

ACCELERATE UNDERSTANDING

IMPROVE COLLABORATION

COORDINATE ACTION

Accelerate Understanding

- Instantaneously transfer knowledge
- Reduce mean time to detect (MTTD) and mean time to respond (MTTR)
- Investigate multiple hypotheses at once

Improve Collaboration

- Increase awareness among and across teams
- Streamline communication between analysts, responders and management
- Test theories prior to sharing with the group to ensure accuracy and relevance

Coordinate Action

- Know who was working on what and when
- Improve understanding of actions taken during an investigation
- Bring order to security operations and improve process efficiency

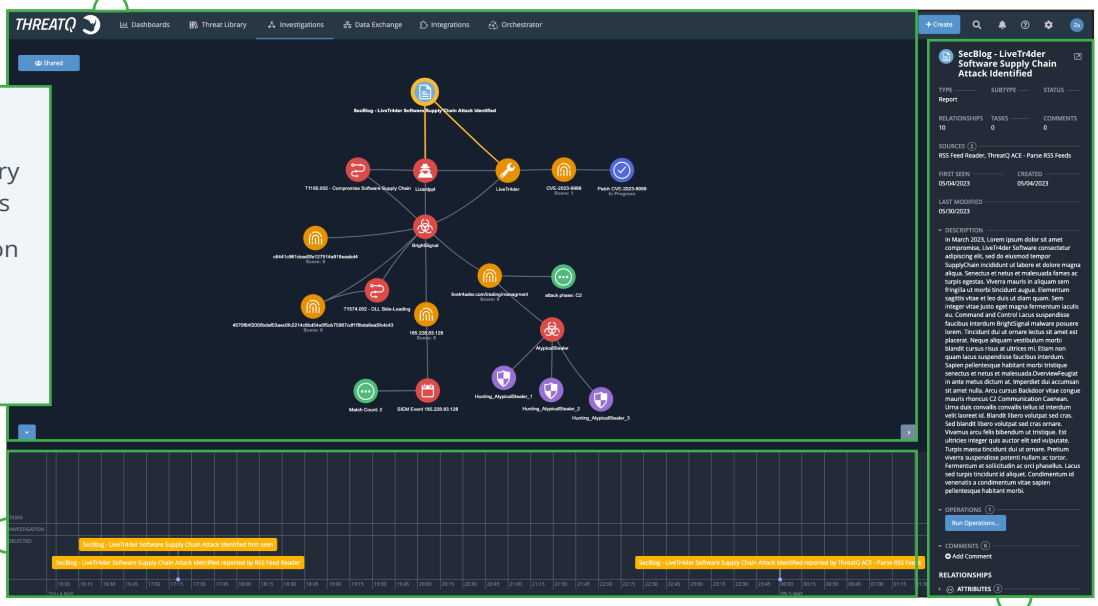
ThreatQ Investigations Features

Evidence Board

- Fuse together threat data, evidence and users
- Accelerate investigation, analysis and understanding of threats in order to update your security posture proactively
- Drive down MTTD and MTTR

Timeline

- Build incident, adversary and campaign timelines
- See who was working on what and when
- Understand how the response unfolded



Action Panel

- Bring order to the chaos of incident response and threat investigation
- See how the work of others impacts and extends your own
- Incident handlers, malware researchers, SOC analysts and investigation leads gain more control and are able to take the right steps at the right time

ThreatQ Investigations Use Cases

Alert Triage

Automation

Incident Response

Spear Phishing

Threat Hunting

Threat Intelligence Management

Vulnerability Management

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, 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. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC.

For more information, visit www.threatquotient.com.