PRODUCT BRIEF

THREATQUOTIENT™

ThreatQ™ Investigations

Take the Right Actions, Faster

ACCELERATE UNDERSTANDING

IMPROVE COLLABORATION

COORDINATE ACTION

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 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 threat intelligence 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 the dispersed nature of today's security teams, 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, assign tasks and see the results unfold in near real-time.

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

Collaborative Threat Investigation	Incident Response
Threat Hunting	Breach Investigation
Adversary Profiling	Vulnerability & Threat Mapping
Intelligence Link Analysis	Incident Retrospectives

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit Threatquotient.com.

THREATQUOTIENT™

Threatquotient.com | sales@ThreatQuotient.com | 1.703.574.9885
11400 Commerce Park Drive, Suite 200, Reston, VA 20191