THREATQUOTIENT™

THREATQ™ FOR INCIDENT RESPONSE TEAMS

Incident responders provide the backbone of an IT security team's cyber resolution capability — serving as the last tier of defense. ThreatQ™ offers incident responders a central repository combining external threat data with internal threat data and events, ensuring context and relevance. ThreatQ also automates threat data prioritization based on customer-defined parameters to remove noise and avoid chasing ghosts. With ThreatQ, your incident response (IR) team can react faster and identify the initial source of attacks through the ability to see relevant, high-priority threats all in one place.

ThreatQ was designed to arm your IR team with a platform to:

- **Accelerate threat detection and response**
- **Provide meaningful context and priority**
- **Maximize efficiency across simultaneous investigations**
- **Take immediate action based on TTPs**
- **Overlay previous attack investigations to make fast and informed investigation decisions**
- **Automate previously manual tasks**

These core IR functions provide a critical capability to detect and disarm threat actors before they do more damage within your organization and security infrastructure.

THREATQ™

WITH THREATQ, IR TEAMS CAN ...

AUTOMATE PRIORITIZATION OF THREATS AND SECURITY INCIDENTS

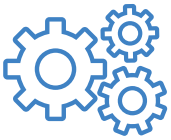
JUMP-START INVESTIGATIONS TO DISARM THREAT ACTORS

PUSH INTELLIGENCE AUTOMATICALLY TO DETECTION AND RESPONSE TOOLS

HOW DO IR TEAMS USE THREATQ?

With ThreatQ, IR teams gain better understanding, make more informed decisions and respond faster through context, prioritization and automation. ThreatQ simplifies incident response by:

- Providing a self-tuning threat library to understand relevance and priority
- Arming the IR team with contextual and relevant data to expedite investigation and response
- Centralizing threat data storage and indicator history for rapid processing and look-ups
- Developing and maintaining adversary dossiers
- Collecting and managing signatures for simplified action
- Simplifying expiration of stale indicators to enhance prioritization and focus
- Pushing internal and external intelligence to detection and response tools automatically
- Capturing learnings to continuously reprioritize threat data and accelerate future incident response



HOW DOES THREATQ STREAMLINE IR TEAM TASKS?

ThreatQ was built to automate frequent tasks around threat intelligence and indicator of compromise prioritization, enrichment and look-ups. It lightens the operational burden and empowers IR teams to respond more quickly and efficiently. With ThreatQ:

- View a single source of truth in one location
- Quickly access threat data and context
- Automatically prioritize threats and security incidents
- Focus only on important incidents instead of chasing false positives
- Confidently utilize contextualized, validated threat intelligence for response

THREATQ™

THREAT OPERATIONS AND MANAGEMENT

ThreatQ is the industry's first threat intelligence platform designed to enable threat operations and management. ThreatQ is the only solution with an integrated Threat Library™, Adaptive Workbench™ and Open Exchange™ that help you to act upon the most relevant threats facing your organization and to get more out of your existing security infrastructure.

IMPROVE SITUATIONAL UNDERSTANDING

ACCELERATE DETECTION AND RESPONSE

MAXIMIZE EXISTING SECURITY INVESTMENTS

ADVANCE TEAM COLLABORATION

BUILD AN EFFECTIVE AND EFFICIENT IR PRACTICE

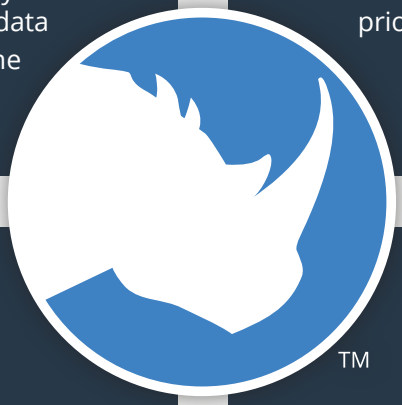
Manage threat intelligence to pro-actively meet the needs of your team.

- Start with context and understanding
- Don't be forced to use various browsers to manually consolidate threat intelligence
- Seamlessly integrate with existing security products to enable a unified defense
- Maintain a laser focus on only relevant and pertinent incidents and data
- Minimize adversary dwell time

SAVE TIME AND MONEY

Focus your cybersecurity team's efforts and accelerate time to response.

- Remove manual tasks from daily workflows
- Minimize data overload, noise and false positives
- Conduct active threat hunting to identify the source of the threat
- Investigate only truly malicious events
- Enable your team to be more efficient and effective by working on higher priorities



TM

DEEPEN YOUR INTELLIGENCE TO PROTECT YOUR ENTERPRISE

Correlate all types of threat intelligence, make sense of it and act on it to protect your business.

- Understand threats through context and adversary profiling
- Automatically connect security events, vulnerabilities and detected attacks to relevant aggregated data
- Evolve your situational awareness into situational understanding

GAIN INTELLIGENT SECURITY OPERATIONS AND RESPONSE

Build strong security processes and cut your response time from weeks to hours.

- Enrich, organize and contextualize data quickly
- Fine-tune your data to meet your IR team's needs
- Empower analysts with the context to make better decisions
- Easily prioritize data for effective response
- Automate tasks for accelerated response

FEATURES & BENEFITS

SELF-TUNING THREAT LIBRARY	Simplify indicator look-ups by utilizing a customizable Threat Library
CUSTOMER-DEFINED PRIORITIZATION	Automatically score and prioritize threat intelligence based on *your* parameters for efficient response
AUTOMATE NEXT STEPS	Automatically block threats in your security devices to ensure that only malicious incidents get escalated to IR
STREAMLINE TEAMWORK	Centralize intelligence sharing, analysis and investigation via an Adaptive Workbench that all teams can access
OPEN AND TRANSPARENT	Understand context, relevance and priority of all ingested data for enhanced response

INTERESTED IN LEARNING MORE?

Sign up for a ThreatQ demo at threatq.com/demo.

ABOUT THREATQUOTIENT™

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 threatq.com.

TQ_ThreatQ-for-IR Teams-Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • Sales and General Inquiries: +1 703 574-9885