THREATQUOTIENT™

THREATQ™ FOR THREAT INTELLIGENCE ANALYSTS

The amount of threat data, both internally collected and externally sourced, that threat intelligence analysts have to process is overwhelming, but part of the job. Sifting through the noise, prioritizing analysis efforts, identifying patterns and finding true malicious threats is time-consuming and difficult to accomplish. The next step is even more complex — actually using the threat intelligence throughout your organization. This requires collaborating with the SOC and IR teams to make decisions and take action as well as defining the content, format and frequency with which to share threat intelligence with other stakeholders. When your teams finally find the needle in the haystack, connect threats to indicators of compromise and map out threat actors' goals and attack patterns, and communicate those findings to the proper teams, the damage may already be done.

ThreatQ was designed to arm threat intelligence analysts with a platform to:

- **Provide insights into adversaries, campaigns and malware**
- **Aggregate, unify, enrich and prioritize threat intelligence**
- **Focus on collecting, analyzing and acting upon relevant threats**
- **Leverage additional threat context to help make better, faster decisions to protect infrastructure and accelerate response time**
- **Become a single source of truth for intelligence, analysis and response activities across all cyber security teams**

Threat intelligence teams can better serve internal customers, like your SOC, IR team, vulnerability management, risk management and your leadership team, with the right data and the right reports.

THREATQ™

WITH THREATQ, THREAT INTELLIGENCE ANALYSTS CAN ...

EFFICIENTLY STRUCTURE, ORGANIZE AND UTILIZE THREAT INTELLIGENCE

QUICKLY UNDERSTAND CONTEXT, RELEVANCE AND PRIORITY OF ALL INGESTED DATA

BUILD ADVERSARY DOSSIERS AND TRACK THEIR ATTACK PATTERNS, INFRASTRUCTURE AND TOOLS

> *"ThreatQ automatically associates indicators to an event so we can quickly pivot and determine the right priority. Instead of wasting time on what ends up being "meh," we're focused on what matters. ThreatQ has saved us a lot of time — and that's incredibly valuable as a threat intel analyst."*
>
> — Threat Intelligence Analyst
> Global Hospitality and Entertainment Company

HOW DO THREAT INTELLIGENCE ANALYSTS BENEFIT FROM THREATQ?

With ThreatQ, threat intelligence analysts can aggregate, enrich, prioritize, deconflict and comment on relevant threat intelligence from both internal and external sources more effectively. ThreatQ automates time-consuming tasks and simplifies the threat intelligence analysis process by:

- Enabling customer-defined configurations within a transparent platform to support how you work
- Automating threat data aggregation of structured and unstructured data from external and internal sources
- Centralizing threat intelligence storage for rapid processing, tracking and look-ups
- Developing and maintaining adversary dossiers
- Providing a self-tuning Threat Library for continuous threat assessment and re-prioritization based on your organization's unique risk profile and parameters you set
- Simplifying expiration of stale indicators to ensure relevance
- Adding context and priority to existing and potential threats
- Accurately escalating event and security alert monitoring

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

ENABLE ANALYSTS TO HUNT FOR THREATS ACROSS THEIR NETWORK

Manage and grow your intelligence to track indicators of compromise to start proactively hunting for threats and building threat actor dossiers.

- Aggregate and share relevant threat intelligence through a self-tuning Threat Library and Adaptive Workbench
- Build adversary dossiers and track their attack patterns, infrastructure and tools
- Hunt for threats preemptively — before their attacks spread
- Automate dissemination of specific indicator types to various tools in your security stack

SAVE TIME AND MONEY

Focus your threat intelligence analysis teams so that they can proactively protect your network.

- Remove manual tasks from daily workflows
- Minimize data overload and time to analyze indicators of compromise
- Enable your team to be more efficient and effective by working on high-value objectives
- Normalize intelligence across feeds to maintain a unified focus
- Provide IR teams a single resource for intelligence

TM

INCREASE YOUR ABILITY TO PROTECT YOUR ENTERPRISE

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

- Automatically aggregate structured and unstructured data regardless of the source
- Analyze, validate, prioritize and act efficiently with relevant threat intelligence
- Understand threats through context and adversary profiling
- Connect security events, vulnerabilities and detected attacks to relevant aggregated data

ACCELERATE THREAT ANALYSIS & ACTION

Build strong security processes and cut your response time from weeks to hours by adding context and priority to the threats you face.

- Rapidly enrich data
- Fine-tune your data to match your security strategy
- Easily prioritize data for effective response
- Enable your security infrastructure to be threat context-aware
- Automatically send all of your curated threat intelligence to your security infrastructure to harden your sensor grid and integrate your defenses

FEATURES & BENEFITS

SELF-TUNING THREAT LIBRARY	Continuously assess your exposure to threats by building a customized threat library — whenever new data or context enters the system, the library will tune and re-prioritize threats
CUSTOMER-DEFINED PRIORITIZATION	Automatically score and prioritize threat intelligence based on *your* parameters
AUTOMATE NEXT STEPS	Automatically block threats in all of your security products — from network to endpoint. Integrate with SIEMs and incident response systems and automate threat operation processes
STREAMLINE TEAMWORK	Centralize intelligence sharing, analysis and investigation
OPEN AND TRANSPARENT	Understand context, relevance and priority of both internal and external data

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.

Copyright © 2018, ThreatQuotient, Inc. All Rights Reserved.

TQ_ThreatQ-for-TIAs-Rev1

THREATQUOTIENT™

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