THREATQUOTIENT™

THREATQ™ FOR SECURITY OPERATIONS CENTERS

The amount of threat data, both internally collected and externally sourced, that Security Operations Centers (SOCs) have to deal with is unconscionable. Sifting through the noise, prioritizing analysis and response efforts, and actually using threat intelligence to make valid decisions is extremely difficult.

Alerts flood SOC dashboards at an unmanageable rate. The majority of the threat data and alerts are just noise. SOC teams are charged with constantly monitoring and assessing their networks, so that they can uncover which data is relevant and important to their environment. Only then can SOC teams validate, verify and prioritize their alerts and concurrent response efforts.

ThreatQ™ was designed to arm SOC analysts with a platform that manages and enriches their threat intelligence for them. This includes:

- **Collection and prioritization of threat data**
- **Creation and warehousing of threat intelligence**
- **Automatically adding, correlating and collecting rich context**
- **Expiration of benign or old indicators of compromise**
- **Deployment of actionable data to your security infrastructure and tools**

THREATQ™

WITH THREATQ, SOC ANALYSTS CAN ...

QUICKLY ANALYZE THREAT DATA

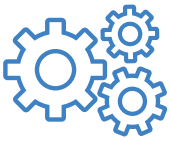
PRIORITIZE THREAT INTELLIGENCE TO REDUCE NOISE AND FALSE POSITIVES

LEVERAGE ADDITIONAL THREAT CONTEXT TO MAKE BETTER DECISIONS TO PROTECT THEIR INFRASTRUCTURE

HOW DO SOC TEAMS USE THREATQ?

With ThreatQ, SOC analysts and engineers can analyze, organize and utilize their threat intelligence more effectively. By deploying threat intelligence to sensors, the SIEM and other security products, they can ensure their threat intelligence is working for them. ThreatQ eases the pain by:

- Automating threat data aggregation
- Centralizing threat data storage for rapid processing and look-ups
- Providing a self-tuning Threat Library for continuous threat assessment
- Enabling SOC teams to define scoring parameters for custom prioritization based on their preferences and risk profile.
- Automating prioritization of threats and security incidents
- Simplifying expiration of stale indicators to ensure focus
- Streamlining threat data sharing and team analysis
- Developing and maintaining adversary dossiers
- Pushing internally developed and externally sourced intelligence to detection and response tools
- Accurately escalating event and security alert monitoring



HOW DOES THREATQ STREAMLINE SOC TASKS?

ThreatQ was built to minimize time spent on manual tasks and lighten the operational burden. It empowers the analysts through automation and allows them to focus on higher priority threats.

- Single source of truth for threat intelligence
- No more manual copying and pasting of threat data from emails or spreadsheets
- No more multi-window third-party indicator research
- No more manual threat data look-ups or analysis
- No more sifting through noise and false positives from irrelevant or low priority threats
- No more spreadsheet updates or email-based team collaboration
- No more “guesstimating” threat analysis or response priorities
- Quickly understand context about threats

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 SOC

Manage your intelligence to get more out of your existing security infrastructure and strengthen your ability to protect your business.

- Adaptive Workbench and a self-tuning threat intelligence library
- Seamless integrations with existing security products to enable a unified defense
- Laser focus on only relevant and pertinent data
- Improve your cyber security situational awareness

SAVE TIME AND MONEY

Focus your SOC's efforts and make sure the work done is meaningful.

- Remove manual tasks from daily workflows
- Minimize data overload and time spent reviewing false positives
- Conduct active threat hunting
- Enable your team to be more efficient and effective by working on high-value objectives

TM

DEEPEN YOUR INTELLIGENCE AND ABILITY TO PROTECT YOUR ENTERPRISE

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

- Automated aggregation of structured and unstructured data
- 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

INTELLIGENT SECURITY OPERATIONS AND RESPONSE

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

- 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
- 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 reprioritize 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 all ingested 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.

TQ_ThreatQ-for-SOCs-Rev1

THREATQUOTIENT™

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