

PRODUCT OVERVIEW

THREATQ™

A Platform Designed for Threat-Centric Security Operations

To stop threats more effectively and efficiently your existing security infrastructure and people need to work smarter, not harder. ThreatQ serves as an open and extensible threat intelligence platform that accelerates security operations. The integrated, self-tuning Threat Library, Adaptive Workbench, ThreatQ Investigations and Open Exchange allow you to quickly understand threats, make better decisions and accelerate detection and response.

PRIORITIZE



INTEGRATE



AUTOMATE



COLLABORATE



“ThreatQuotient’s ThreatQ platform seamlessly integrates with its customers’ existing technologies and tools, which allows ThreatQ to quickly self-adjust its threat library based on customer requirements.

This makes ThreatQ the perfect platform for customers wishing to monitor and block threats despite any changing business circumstance.”

~ Mohammed Riyaz Ahmed, Industry Analyst, Frost & Sullivan ~





THREAT LIBRARY

Relevant, Contextual Intelligence Shared Across Systems and Teams

The threat library automatically scores and prioritizes threat intelligence based on parameters you set. Prioritization is calculated across many separate sources, both external and internal, to deliver a single source of truth using the aggregated context provided. This removes noise and reduces the risk of false positives.

- Self-tuning
- Context from external + internal data
- Structured and unstructured data import
- Automatic prioritization based on all sources
- Custom enrichment source for existing systems



ADAPTIVE WORKBENCH

Combine Automation and Human Intelligence for Proactive Detection and Response

Customer-defined configuration and integrations work with your processes and tools to improve the effectiveness of your teams. Customizable workflow and customer-specific enrichment streamline analysis of threat and event data for faster investigation and automation of the intelligence lifecycle.

- Consolidated view, unified opinion
- Continuous threat assessment
- Push-button operations using existing tools and processes
- Customizable, use case-specific dashboards



OPEN EXCHANGE

Open and Extensible Architecture Enables Robust Ecosystem

Import and aggregate external and internal data sources, integrate with existing enrichment and analysis tools, and export the right intelligence to the right tools at the right time to accelerate detection and response. Get more from your existing security investments by integrating your tools, teams and workflows through standard interfaces and an SDK/API for customization.

- Bring your own connectors and tools
- Marketplace apps for easy integrations
- SDK / API for customization
- Standard STIX/TAXII support



THREATQ INVESTIGATIONS

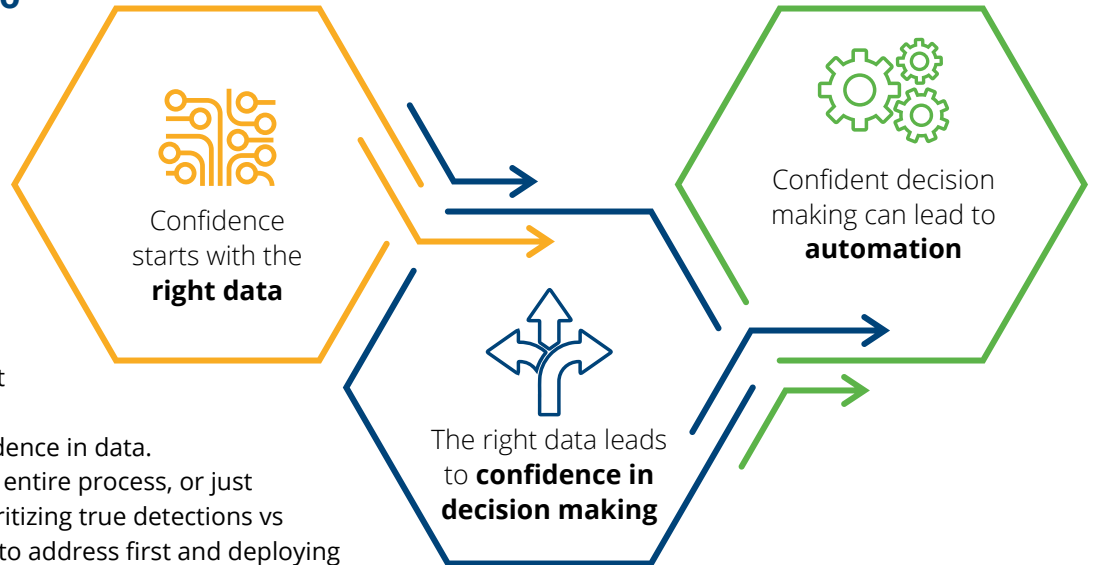
The Industry's First Cybersecurity Situation Room

ThreatQ Investigations solves the silo challenge and eliminates inefficiencies that exist across security operations to accelerate detection and response. As the first cybersecurity situation room, it streamlines investigations and improves active collaboration among and across teams.

- Fuse together threat data, evidence and users
- Accelerate investigation, analysis and understanding of threats in order to update your defense posture proactively
- Drive down mean time to detect (MTTD) and mean time to respond (MTTR)
- Build incident, adversary and campaign timelines
- Perform standard actions and responses throughout your security infrastructure from the investigation interface

ThreatQ's Approach to Implementing SOAR

ThreatQuotient believes a threat-centric approach to SOAR and Security Operations improves overall efficiency, consistency and effectiveness. By starting with an understanding of the threat and the customer-specific threat landscape, you can make better automated decisions with confidence in data. You may decide to automate an entire process, or just select aspects, for example prioritizing true detections vs noise, determining which alerts to address first and deploying the best responses and counter-measures.



How we do it:

- ✓ Continuous assessment and prioritization of threat data, events and alerts
- ✓ Customer-specific scoring; resulting in high fidelity and highly relevant intelligence and context
- ✓ Dynamic prioritization to compare events and alerts
- ✓ Capture feedback in a central database for instantaneous knowledge sharing
- ✓ Optimize automatically as more data and context is learned
- ✓ Increase efficiency and effectiveness of downstream processes

“ThreatQ cut our investigating time by over 80% and reduced the rate of false positives and false negatives by 50%.”

~ Antonin Hilly, MSSP Executive Director, COO & CTSO, Sopra Steria ~

THE POWER OF THREATQ

The ThreatQ platform supports the following use cases:



THREAT INTELLIGENCE MANAGEMENT

Turn threat data into threat intelligence through context and automatically prioritize based on user-defined scoring and relevance.



THREAT HUNTING

Empower teams to proactively search for malicious activity that has not yet been identified by the sensor grid.



INCIDENT RESPONSE

Gain global visibility to adversary tactics, techniques and procedures to improve remediation quality, coverage and speed.



SPEAR PHISHING

Simplify the process of parsing and analyzing spear phish emails for prevention and response.



ALERT TRIAGE

Send only threat intelligence that is relevant to reduce the amount of alerts that need to be investigated.



VULNERABILITY MANAGEMENT

Focus resources where the risk is greatest and prioritize vulnerabilities with knowledge about how they are being exploited.

THREATQ CAPABILITIES:

Ingest Threat data from internal and external sources
 Ingest Structured (XML, JSON, CSV, etc) and Unstructured Intelligence
 Commercial, OSINT, ISAC feed integration
 Aggregate, deduplicate, normalize, and enrich threat data
 STIX 1.1, STIX 1.2, STIX 2.0, TAXII
 Store malware samples, reports and incidents
 Customer-defined scoring

Customizable Dashboards
 Watchlists
 Signature and Rule Management (YARA, OpenIOC, Bro/Zeek, Surricata, Snort)
 Built-in Operations to automate manual tasks
 Bulk data actions
 Automated Expiration
 Customizable Data Sharing
 Team Tasking
 User-Defined Reporting (PDF, and JSON)
 TLP

Detailed TLP Markings
 Custom data model/objects
 Open API/SDK
 Bi-directional integration with SIEM, EDR, Incident Response, etc.
 Threat Visualization
 Full-text search capabilities/ document index
 MITRE ATT&CK framework integration
 Event timelines and analysis
 Spear Phish Analysis
 Proactive Feed Health Monitoring

DEPLOYMENT OPTIONS:

On-premise
 Cloud-based
 Hosted
 Virtual Instance
 Air-gapped

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA. For more information, visit www.threatquotient.com.