THREATQUOTIENT™
A SECURONIX COMPANY

PRODUCT OVERVIEW

THREATQ™

A Threat Intelligence Platform Designed for Data-Driven 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 platform that accelerates security operations. DataLinq Engine, Threat Library, Smart Collections, ThreatQ TDR Orchestrator, ThreatQ Investigations and the 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 ~

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

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

THREATQ INTEGRATION FRAMEWORK

Framework drives depth & breadth of bidirectional integrations

A set of tools and technologies to enable easy creation and maintenance of integrations with external feeds and internal security infrastructure, resulting in the largest technology ecosystem, with the most capability, in the market. 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

SMART COLLECTIONS

Puts the “smarts” in the platform and not the individual playbooks

ThreatQ TDR Orchestrator puts the “smarts” in the platform and not the individual playbooks by using Smart Collections™ and data-driven playbooks. The application of Smart Collections and data-driven playbooks provides for simpler configuration and maintenance, and provides a more efficient automation outcome. This approach further addresses all three stages of automation – Initiate, Run and Learn – easily and efficiently by enabling users to curate and prioritize data upfront, automate only when relevant, and simplify actions taken. To improve the platform “smarts”, it will also capture what has been learned to improve data analytics, which in turn improves the initiation stage of automation.

Smart Collections improves detection and response by automatically:

- Generating dashboard analytics
- Controlling data shared via ThreatQ Data Exchange feeds
- Sharing data with select ThreatQ integrations to support a wide range of use cases
- Launching automated workfLOWS

DATALINQ ENGINE

Make sense of data in order to accelerate detection, investigation and response

Connecting disparate systems and sources, this adaptive data engine imports and aggregates external and internal data; curates and analyzes data for decision making and action; and exports a prioritized data flow across the infrastructure for improved prevention, and accelerated detection and response.

- Ingest and aggregate structured and unstructured data via Marketplace apps and an open API
- Normalize automatically from different sources, formats and languages into a single object
- Correlate across atomic pieces of data to identify relationships and provide a unified view
- Prioritize via customer controlled, dynamic scoring to ensure relevance and filter noise
- Translate data into the format and language necessary for consumption across systems

THREATQ TDR ORCHESTRATOR

Simplify Security Automation, TIP and SOC initiatives by making them data-driven, open and efficient

ThreatQ TDR Orchestrator is the industry's first solution to introduce a simplified, data-driven approach to Security Automation, TIP, and TDIR initiatives that accelerates threat detection and response across disparate systems, resulting in more efficient and effective security operations.

Key Benefits:

- Easy to set up and maintain
- Reduce playbook runs by 80%
- Ensure output is relevant and high priority
- Learn from the actions taken, and improve over time

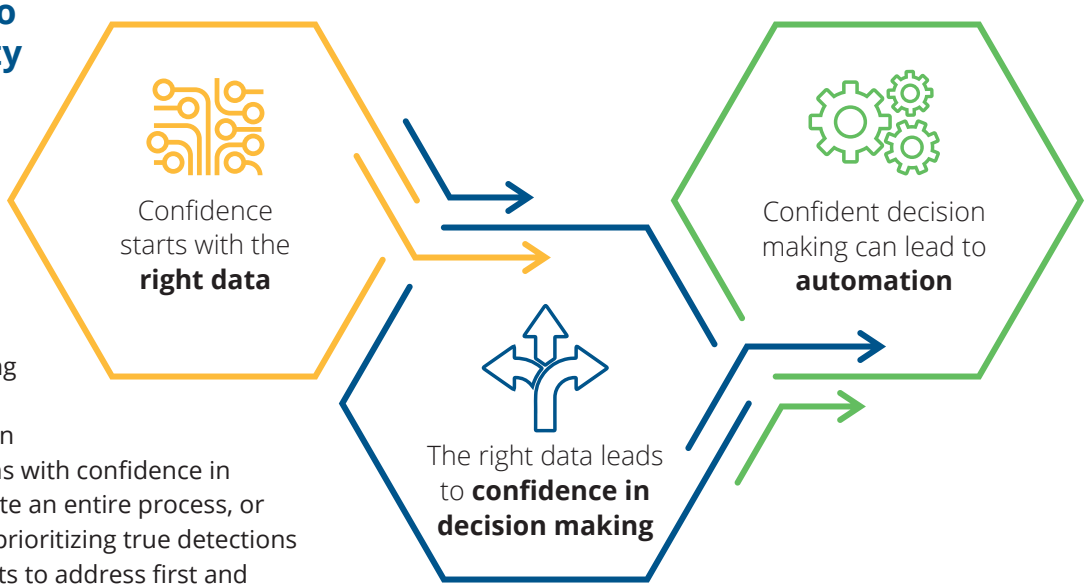
THREATQ INVESTIGATIONS

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 Security Automation



ThreatQuotient believes a data-driven approach to 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 automate the prioritization based on user-defined scoring and relevance.

THREAT HUNTING

Empower teams to automate the hunt and 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. Automatically enrich content and pull additional data from integrated internal or external sources.

SPEAR PHISHING

Automatically ingest suspected spear phish emails, processing them with content parsers and artifact extractors, though bi-directional email product integrations, direct API access, and manual import.

ALERT TRIAGE

Automatically prioritize the most relevant data, remove noise, and ensure effective use of valuable resources, both human and machine.

VULNERABILITY MANAGEMENT

Focus resources where the risk is greatest and automat the prioritization of 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
- Air-gapped

ThreatQuotient (now part of Securonix) improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection, investigation and response (TDIR). ThreatQ is the first purpose-built, data-driven threat intelligence platform that helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading integration marketplace, data management, orchestration and automation capabilities support multiple use cases including threat intelligence management and sharing, incident response, threat hunting, spear phishing, alert triage and vulnerability management. For more information, visit www.securonix.com.

TQ-DTS02-1008-02