

THREAT INTELLIGENCE PLATFORM



Operationalize prioritized intelligence across detections and response.

Turn threat data into action

When threat volume spikes and AI increases signal variability, teams struggle to separate noise from real risk. ThreatQ, a Securonix company, curates, enriches, correlates, and scores threat data in one place, then automates high-fidelity intelligence into downstream detections and response workflows. The result is a continuous feedback loop that keeps intelligence relevant, prioritized, and ready to operationalize across your SOC and CTI program.

Turning Raw Intelligence into Actionable Defense

- ✔ **Higher-fidelity intelligence at scale**
 Prioritize and operationalize intelligence to improve detection and response outcomes.
- ✔ **Unify fragmented intelligence**
 Aggregate structured and unstructured sources, normalize formats, and correlate relationships into unified threat objects for a shared source of truth.
- ✔ **Prioritize what matters**
 Apply customer-defined scoring across internal and external context to reduce noise and focus analysts on high-priority threats and indicators.
- ✔ **Operationalize with confidence**
 Automate only when intelligence is relevant, pushing prioritized outputs into SIEM, EDR, and response systems to improve fidelity and speed.
- ✔ **Collaborate to accelerate investigations**
 Bring together threat data, evidence, and users to build timelines, streamline triage, and reduce SOC friction across teams.

ThreatQ Applications

Apply prioritized intelligence across detection engineering, triage, and threat response.



Threat intelligence management

Curate, enrich, and score intel to maintain relevance and reduce noise.



Detection engineering enablement

Operationalize prioritized intel into analytics and SIEM detections with closed-loop feedback.



Alert triage and investigation acceleration

Use relationships, TTPs, and shared context to speed up decisions and response.



Vulnerability prioritization

Align remediation priorities to active exploitation and observed adversary behavior.

“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

Data-driven intelligence operations

Curate first, automate second, and continuously improve intelligence quality.

DataLinq Engine → Unified context

Ingest, normalize, correlate, and translate data for downstream consumption.

Threat Library → Less noise

Self-tuning scoring prioritizes relevant intel and reduces false positives.

Integration Framework → Fits your stack

Bidirectional integrations and standards-based exchange across tools and teams.

Smart Collections → Smarter automation

Put only relevant intelligence on the platform to drive consistent, data-driven playbooks.










TDR Orchestrator → Efficient response

Reduce playbook runs by up to 80% while keeping outputs high priority.

ThreatQ Investigations → Faster collaboration

A shared “situation room” to build timelines, take action, and cut SOC friction.

Compare

CAPABILITIES	THREATQ	LEGACY TIP	MANUAL WORKFLOW
Prioritization	 Customer-defined scoring; unified context.	 Feed-heavy noise; manual tuning.	 Inconsistent and unscalable.
Operationalization	 Data-driven, closed-loop automation.	 Static exports; zero feedback.	 Slow handoffs; manual entry.
Collaboration	 Integrated situation room and timelines.	 Third-party app reliance.	 High friction team silos.

SPECIFICATIONS

Integration ecosystem:

530+ marketplace integrations; “bring your own” connectors; SDK/API customization

Standards support:

STIX/TAXII

Core components

DataLinq Engine, Threat Library, Smart Collections, TDR Orchestrator, Investigations, Open Exchange

Deployment options:

On-premises, cloud-based, hosted, air-gapped

Why Securonix

ThreatQ, a Securonix company, delivers intelligence operations designed for data-driven security outcomes: unified context across internal and external sources, customer-controlled scoring to reduce noise, and automation that operationalizes only what is relevant. With an ecosystem-first integration model and collaborative investigation workflows, teams improve detection fidelity, accelerate triage and response, and keep intelligence continuously prioritized as adversary behavior and business conditions change.

Visit securonix.com or contact sales@securonix.com.