*This series of technology partnership briefs describes how ThreatQ and ThreatQ Investigations augment and integrate with modern security tools and are able to replace legacy processes and systems.*

# How ThreatQ™ and ThreatQ Investigations work with Ticketing Systems

ThreatQ and ThreatQ Investigations are designed to augment and integrate with security ticketing systems that exist within the customer's environment. Both tools are designed with different use cases and goals in mind and, when combined, provide powerful workflows that optimize time and efficiency for both intelligence analysts and incident responders.

## HOW TICKETING SYSTEMS BENEFIT THREATQ INVESTIGATIONS

- Gains local context about indicators that have been seen in real incidents within the organization
- Enables automated scoring to create a relevant and customer-specific Threat Library™
- Allows tasks in the ticketing system to be created and tracked to resolution by teams outside of the ThreatQ interface

## HOW THREATQ INVESTIGATIONS BENEFITS TICKETING SYSTEMS[1]

- Queries for objects (e.g., indicators) that are attached to tickets
- Discovers related artifacts attached to the case
- Queries details of campaigns and adversaries
- Uncovers artifacts that may have been used in different attacks or campaigns against other entities
- Marks threat artifacts as false positives where applicable

[1] Features available in ticketing systems vary by vendor and product, as do integration possibilities.

## FUNCTIONS OF THREATQ AND TICKETING SYSTEMS

| | ThreatQ | Security Ticketing System |
|---|---|---|
| Becomes the central point for knowledge for threat data that is relevant to the organization | Yes | No |
| Incident workflow templates | No | Yes |
| Coordination of an investigation | Yes | Supports |
| Real-time collaboration in a threat investigation | Yes | Supports |
| Tasking external teams outside of ThreatQ for action | No | Yes |

| | Integrates wIth | Augments Workflow | Strategy & Vision |
|---|---|---|---|
| **SIEM / Event Log Management** | ✓ | ✓ | **Strategy:** Bidirectional product integrations with SIEM specific applications available for some products.<br>**Vision:** Provision of actionable threat intelligence and context to the SIEM. Automatically harvest sightings to inform customer-specific threat scoring. Collection, analysis and adaptation of threat intelligence as seen from either a disparate environment with independent tools reporting to a SIEM or a coordinated security architecture with integrated tools leveraging a common intelligence data set. |
| **Ticketing** | ✓ | ✓ | **Strategy:** Integration with ticketing and IR systems currently in the customer's environment.<br>**Vision:** Enable availability of threat context while working on incident tickets, and recording of actions taken on threat artifacts to further help investigation coordination (ThreatQ Investigations) and threat scoring. |
| **Orchestration** | ✓ | ✓ | **Strategy:** Integration with orchestration systems enabling complex, multi-stage actions to be taken when needed.<br>**Vision:** Enables complex actions that may be needed before or during an investigation or as part of a singular analysis or detection. By serving as the referencial library for requests, storage and modifications, ThreatQ can drive not only customer-specific scoring on threats, vulnerabilities or risks, but also real-time logical branching in complex orchestrations. |
| **Visual Link Analysis** | ✓ | ✓ | **Strategy:** Deliver powerful investigation visualizations by combining threat data, user actions and analyst tasks. Ensure data is published via API for integration with external visualization tools (e.g., Maltego).<br>**Vision:** Visual analysis helps people to determine what actions needed to be taken during an investigation or as part of threat analysis. By storing and providing visual analysis of the output of coordinated actions, ThreatQ can better drive customer-specific threat scoring. |
| **Spreadsheets and PDFs of Indicators** | ✓ | Replaces | **Strategy:** Import existing documents into ThreatQ to replace the process of analysts keeping separate and disparate threat data — and to provide an internal evidence trail.<br>**Vision:** To deliver a company-specific threat library that is scored and prioritized to reflect current threat or make predictions on future ones. To make this scored, referenced and actionable threat data available for the right tools, processes or people to allow immediate action. |
| **Endpoint & Network Protection** | ✓ | ✓ | **Strategy:** Deliver actionable threat data automatically encoded into formats that can be consumed by defense tools and the sensor grid as defined by customer needs.<br>**Vision:** Provide an intelligence-driven, customer-specific threat dataset that can be used to detect, track and interdict, as required, across all company security systems. |

## ABOUT THREATQUOTIENT™

ThreatQuotient™ understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization and prioritization needed to make better decisions, accelerate detection and response, and advance team collaboration. Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management system.

For additional information, please visit threatq.com.