TECHNOLOGY PARTNERSHIP BRIEF

THREATQUOTIENT™

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 Visualization Tools

ThreatQ and ThreatQ Investigations are designed to augment and integrate with existing visualization tools that exist within the customer's environment. While ThreatQ Investigations provides powerful, integrated, threat data visualizations, existing investments in visualization tools can be leveraged through API integrations. Visualization tools are normally data focused for analysis, whereas ThreatQ Investigations enables the coordination of the investigation between multiple team members.

HOW EXTERNAL VISUALIZATION SYSTEMS BENEFIT THREATQ

- Data visualization enhances a user's ability to understand a threat
- External visualization systems rarely publish threat data back for consumption by ThreatQ

HOW THREATQ BENEFITS VISUALIZATION SYSTEMS[1]

- Provides a scalable Threat Library™ for query by external visualization tools
- Allows linking of data between adversaries, campaigns, indicators, files and events
- Delivers deep context consumed by external and internal sources
- Provides customer-specific threat scoring for all search data

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

FUNCTIONS OF THREATQ AND VISUALIZATION TOOLS

	ThreatQ & ThreatQ Investigations	External visualization systems
Becomes the central knowledgebase for all threat data relevant to the organization	Yes	No
Coordinates an investigation between people / teams	Yes	No
Collaborates in real-time	Yes	Depends on tool
Assigns investigation tasks to users	Yes	No
Works with custom threat objects created in ThreatQ	Yes, automatically	May need updates

	Integrates wIth	Augments Workflow	Strategy & Vision
SIEM / Event Log Management	✓	✓	**Strategy:** Bidirectional product integrations with SIEM specific applications available for some products. **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. **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. **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). **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. **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. **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.