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 Endpoint Detection & Response (EDR) Systems

ThreatQ and ThreatQ Investigations are designed to augment and integrate with Endpoint Detection & Response (EDR) systems. EDR systems provide defenders with the ability to observe endpoints, see what files exist on them and how those files behave upon execution. Custom lists of file hashes and endpoint indicators can be searched for and, if found, reported to the SIEM and, therefore, consumed by ThreatQ as sightings.

Most EDR systems have limitations on the quantity of external threat data they can consume and search for. It's important that they are provided with the most relevant and important data for that organization. The unique prioritization capabilities built into ThreatQ can ensure the right data is published to the right tools.

HOW EDR SYSTEMS BENEFIT THREATQ & THREATQ INVESTIGATIONS[1]

- Automatically consumes sightings in ThreatQ to enable customer-specific scoring, allowing the identification of relevant threats
- Provides a key data source for ThreatQ Investigations
- Drives indicator prioritization based on local sightings
- Depending on the EDR vendor, integrations may be available to search for the presence of an object during an investigation

HOW THREATQ & THREATQ INVESTIGATIONS BENEFIT EDR SYSTEMS[1]

- Provides a central store of endpoint detection signatures, e.g. YARA and OpenIOC
- Links endpoint detection rules with attack motivation and campaign data
- Exports lists of accurate, relevant threat data to optimize any capacity limitations on the EDR system
- Understands the details and context behind event-associated indicators
- Enriches data with information about the motivations of the campaign, attackers and their intent

[1] Exact EDR capabilities and integration functions vary between products and vendors.

AT A GLANCE: FUNCTIONS OF THREATQ AND THE EDR SYSTEM

	ThreatQ	EDR
Automatically consume / publish relevant threat data	Publishes	Consumes
Aggregation of all threat intelligence to build a customer-specific Threat Library®	Yes	No
Build a contextual understanding of external threats	Yes	No
User tasking	Yes*	No
Operationalize threat intelligence by deploying to protection tools (Firewalls, endpoint, IPS, etc.)	Yes	No
Perform investigations that span multiple threat data sets and tools	Yes	No
Watch endpoint activity	No	Yes
Perform mitigation actions on the endpoint	No	Yes

*Focused on threat investigation and analysis.

	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 referential 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 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.

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885