THREATQ™ AND MCAFEE®

ThreatQ's integration with McAfee Advanced Threat Defense (ATD) gives the analyst the tools to easily send malware or URLs for detonation.

The joint solution of ThreatQ and McAfee ATD allows users to submit files for analysis and store resulting data in the Threat Library™. With this integration, customers can aggregate, prioritize and act upon the most relevant threats facing an organization.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

MCAFEE ADVANCED THREAT DEFENSE

McAfee Advanced Threat Defense enables organizations to detect advanced, evasive malware and convert threat information into immediate action and protection. Unlike traditional sandboxes, it includes additional inspection capabilities that broaden detection and expose evasive threats. Tight integration between security solutions — from network and endpoint to investigation — enables instant sharing of threat information across the environment, enhancing protection and investigation. Flexible deployment options support every network.

INTEGRATION HIGHLIGHTS

Provides feed of analysis results from ATD.

ThreatQ Operation enables user to submit files to ATD for analysis.

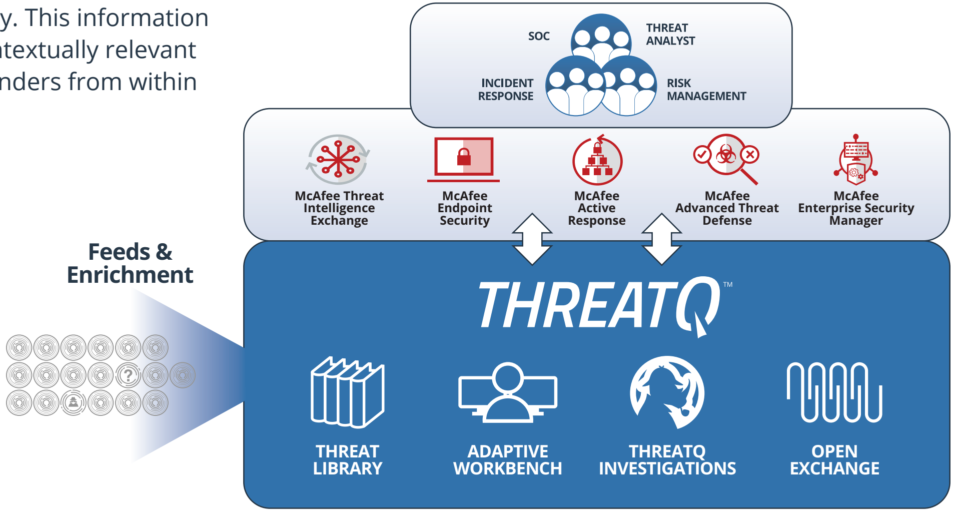
Enable analysts to make better-informed decisions by providing context and situational understanding of threats.

INTEGRATION USE CASES

ATD publishes any analysis result onto the DXL messaging fabric. ThreatQ captures any new messages and creates an event within the Threat Library. Threat data that is associated with the ThreatQ Event is then scored and sent to the infrastructure products in a mixed-vendor environment.

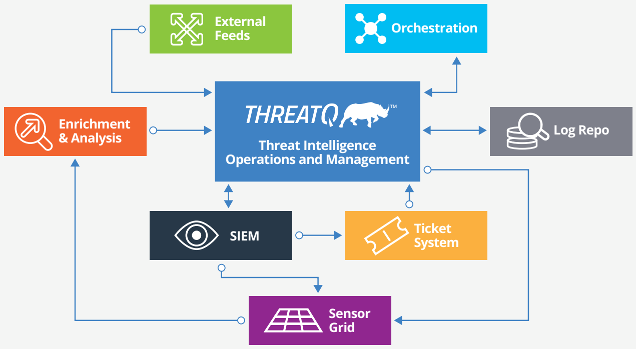
The analysis report and (optionally) malware samples are also captured and related to the relevant pieces of threat data within the Threat Library. This information may be used to offer additional contextually relevant data to analysts and incident responders from within the ThreatQ GUI.

ThreatQ receives sample malware from an external feed source. Users may then leverage a ThreatQ Operation to send files and URLs to ATD for evaluation and detection. All results are published back onto the DXL messaging fabric and made visible to all technologies that are subscribed to the ATD DXL topic. This includes passing data that scores above a user-defined threshold back to ThreatQ.



OPEN EXCHANGE ARCHITECTURE

ThreatQ's Open Exchange™ provides an extensible and flexible environment for analysts to achieve the optimal balance between system automation and expert analysis. Because no single security solution provides a silver bullet against attacks, ThreatQ's Open Exchange architecture supports standard interfaces for ingestion and exporting, including STIX/TAXII, XML, JSON, PDF, email and other formats of structured and unstructured data, along with an SDK and APIs for custom connections.



ABOUT THREATQUOTIENT™

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For additional information, please visit threatquotient.com.

ABOUT MCAFEE®

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place.

McAfee technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. No computer system can be absolutely secure. McAfee® and the McAfee logo are trademarks of McAfee, LLC or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others.

For more information, visit www.mcafee.com.