THREATQUOTIENT™

McAfee™

THREATQ™ AND MCAFEE®

The integration of McAfee Enterprise Security Manager (ESM) and ThreatQ helps organizations reduce noise, minimize false positives and accelerate detection and response.

The joint solution of ThreatQuotient and McAfee ESM provides integrated workflows that optimize time and user experience for intelligence and security analysts alike.

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 ENTERPRISE SECURITY MANAGER

McAfee ESM—the foundation of the SIEM solution family from McAfee—delivers the performance, actionable intelligence and real-time situational awareness at the speed and scale required for security organizations to identify, understand and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

INTEGRATION USE CASES

ThreatQ's integration with McAfee ESM allows the threat intelligence team to publish relevant, targeted indicators to multiple ESM instances. Each ESM instance will then have curated watchlists based on the latest expertise of the threat intelligence team.

In the event an item on a watchlist, such as an IP address or a file hash is seen by the ESM, an alarm will be generated and an event created in the ThreatQ

INTEGRATION HIGHLIGHTS

Accelerate event triage by providing a searchable and single source of threat knowledge.

Automatically consume sightings in ThreatQ to deliver customer-specific scoring, allowing for the identification of relevant threats.

Understand the details and context behind indicators and their associated events.

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

Deliver qualified and contextual threat data to automate searching for relevant threats in the ESM.

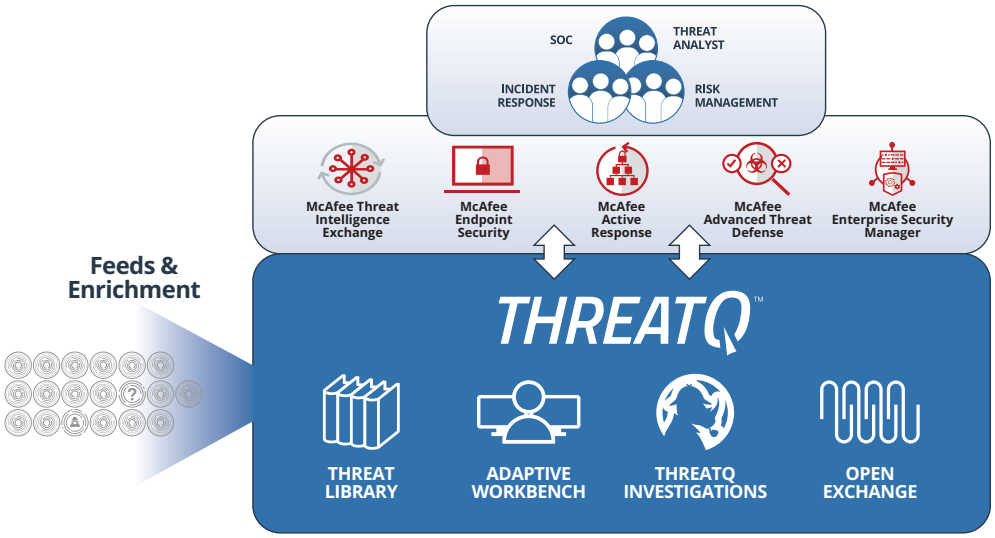
Threat Library™. The event in the Threat Library will include important context, such as any additional and relevant indicators.

The additional context the ESM returns can be used in the ThreatQ customizable scoring policy. The threat intelligence team is therefore able to automatically re-evaluate the relevance of certain features to the organization based on external reports and internal sightings.

Additionally, ThreatQ is able to use the backtrace functionality provided in ESM. This capability enables the analyst in ThreatQ to look back over the events that have occurred in a given user-definable time period to identify any matches that may have been missed or previously unknown.

ThreatQ brings in threat data from many different sources (ISACs, open source, DHS-AIS, etc.). After threat data is deduplicated and scored, high-relevance indicators are sent to ESM watchlists. The integration is bidirectional, meaning a sighting by the ESM will be reflected in the Threat Library as an additional source. The score is then edged higher and the indicator is pushed to the infrastructure products, like McAfee Endpoint Security or McAfee Active Response (MAR), to automatically block this particular indicator.

An analyst pivots on the indicator within ThreatQ and realizes it is related to a particular adversary. The scoring algorithm is adjusted to automatically increase the score of any indicator associated with this adversary. Based on the new scoring policy, the system recalculates all the indicators associated with that adversary and, as a result, new indicators exceed the threshold for export and are sent to ESM and other enforcement infrastructure for blocking.



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.

TQ_ThreatQ-McAfee-ESM-Solution-Overview_Rev1