THREATQUOTIENT

INTEGRATION OVERVIEW

The Power of ThreatQ and McAfee

The volume of available threat data has increased dramatically over the last decade, gradually becoming a cacophony of noise. Mature security organizations have raced to develop tools, teams and processes to turn threat data into timely and relevant threat intelligence. Once this is accomplished, the intelligence must be distributed to existing security tools across networks that may be isolated from one another, and the intelligence team must get feedback from internal sighting matches.

McAfee™ and ThreatQuotient™ have strengthened our partnership to develop integrations and use cases that help solve these problems for customers.

ThreatQ and McAfee MVISION Endpoint Detection and Response (EDR)

- Capture threats that have been detected by MVISION EDR into dedicated events within ThreatQ — including indicators, attributes and MITRE ATT&CK Techniques.
- Correlate and identify relationships with existing threat data within the ThreatQ Threat Library automatically.
- Understand MITRE ATT&CK from MVISION EDR in context — who is attacking you, what software/malware might they use and what mitigations to apply.
- Perform visual analysis of potential threats in context using ThreatQ Investigations.
- Trigger deeper analysis within MVISION EDR directly from the ThreatQ interface. This triggers an MVISION EDR investigation that performs process analysis and provides additional Investigation Guides.
- Leverage ThreatQ Operations to query MVISION EDR for useful data on-demand, including Query Netflow using Source or Destination and Querying Hash Data.

ThreatQ and McAfee Advanced Threat Defense (ATD)

- Provide feed of analysis results from ATD.
- ThreatQ Operation enables users to submit files to ATD for analysis.
- Enable analysts to make better, more informed decisions by providing context and situational understanding of threats.
- Capture MITRE ATT&CK Techniques from ATD analysis results and provide additional layers of context via ThreatQ's MITRE ATT&CK feed, including Adversary association, associated tactics, tools and malware and mitigation techniques.

ThreatQ and McAfee Enterprise Security Manager (ESM)

- 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, more informed decisions by providing context and situational understanding of threats.
- Deliver qualified and contextual threat data to automate searching for relevant threats in ESM.
- Query ESM from ThreatQ for log data which relates to specific indicators.

ThreatQ and McAfee Threat Intelligence Exchange (TIE)

- Make third-party intelligence available for McAfee agents on DXL.
- Reduce and prioritize large amounts of threat intelligence to be made available for enforcement.
- ThreatQ provides TIE with information about the maliciousness of indicators.
- Distribute intelligence across large deployments.
- Share relevant security intelligence in real time to endpoint, gateway, network and data center security solutions.
- Query hashes against TIE from ThreatQ and add context to the ThreatQ Threat Library on-demand.

ThreatQ and McAfee Active Response (MAR)

- Query environment-wide endpoints that have had a MAR agent installed to see if a file has been deployed on that endpoint and capture its current status.
- Query environment-wide endpoints that have had a MAR agent installed to capture any NetFlow information for a source or destination IP address supplied by ThreatQ.

ThreatQ and McAfee Network Security Manager (NSM)

- Document NSM scan results such as related indicators and descriptive attributes in the ThreatQ Threat Library.
- Associate scan results with contextually relevant threat data and events automatically.
- Capture detection signatures from NSM and store in ThreatQ for reference and further analysis.