SOLUTION BRIEF

ThreatQuotient and McAfee Active Response Integration

Prioritize threat intelligence to accelerate security operations

The ThreatQuotient and McAfee® Active Response joint solution enables security operations teams to accelerate investigations into potential threats and malicious activity. In the event of a malicious sighting, teams will have the associated context available to respond in ThreatQuotient, including tactics, techniques, and procedures associated with the threat, allowing for a more timely and accurate response.

McAfee Compatible Solution

- ThreatQ and McAfee Active Response

Connect With Us

The Business Problem

The volume of available threat data has increased dramatically over the last decade, making it challenging for security professionals to separate relevant data from the noise. Mature security organizations are racing to develop tools, teams, and processes to turn threat data into timely and useful 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 sightings.

Through their McAfee® Security Innovation Alliance partnership, McAfee and ThreatQuotient have developed integrations and use cases that help solve these problems.

McAfee Active Response and ThreatQuotient Joint Solution

As part of the ThreatQuotient integration with McAfee Active Response, analysts can query for malicious activity across the endpoints in their environment based on intelligence in their ThreatQuotient global Threat Library. The McAfee Active Response-ThreatQuotient integration enables analysts to quickly identify and isolate potential threats across their endpoints using real-time queries. This assists with decreasing mean time-to-detect and mean time-to-respond. Additionally, triggers can be crafted in McAfee Active Response based on ThreatQuotient's exports, allowing for enterprise-wide indicator sweeps across McAfee endpoints.

Features and Benefits

- Query environment-wide endpoints that have had a McAfee Active Response 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 McAfee Active Response agent installed to capture any NetFlow information for a source or destination IP address supplied by ThreatQuotient.

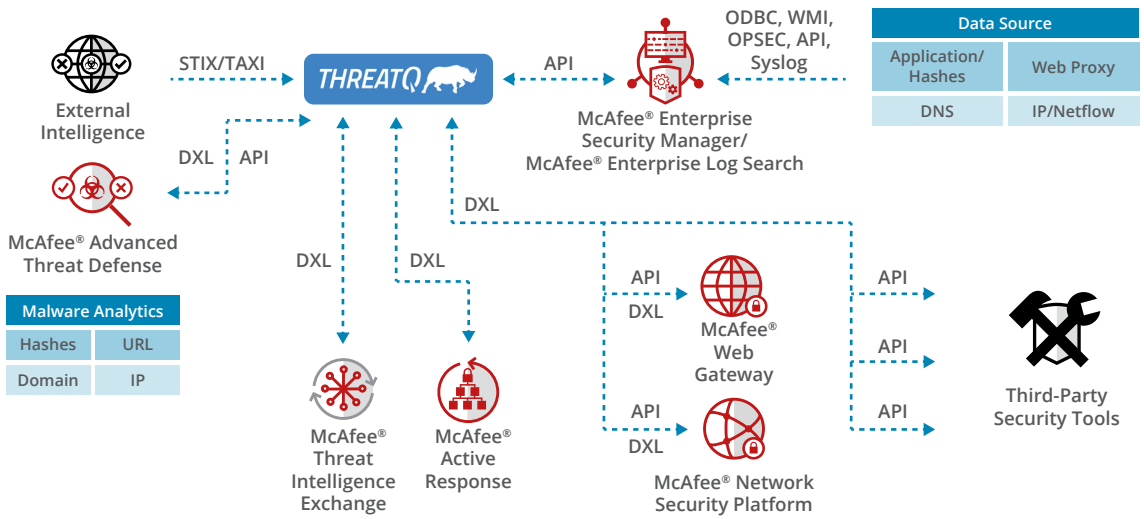

Figure 1. The power of McAfee and ThreatQuotient.

McAfee and ThreatQuotient Use Cases

ThreatQuotient brings in threat data from many different sources (ISACs, open source, DHS-AIS, and more). This threat data is de-duplicated and scored in the system and considered relevant enough to send to infrastructure products, like McAfee® Endpoint Security or McAfee Active Response, to hunt and determine whether that indicator has been found on the network.

About ThreatQuotient

ThreatQuotient understands that the foundation of intelligence-drive 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. ThreatQuotient is headquartered in Northern Virginia with international operations based in Europe and Asia-Pacific. For more information, visit **threatquotient.com**

About McAfee Active Response

Security-conscious entities today face a threat landscape that is changing at a dramatic pace. Attacks are created and propagated at ever faster rates. "Designer" attacks target individual organizations by using focused knowledge to improve their effectiveness and minimize detection. Attackers are more frequently penetrating preventive technologies. Forward-looking organizations are demanding easy-to-use, integrated tools that help better detect attackers' presence and then allow rapid investigation and remediation. The best detection and response solutions increase security efficiency even as they capture increasingly more information from a growing number of systems. By providing superior out-of-the-box capabilities, automated interaction with existing security management solutions, and user-customization, McAfee Active Response greatly narrows the window of opportunity for attackers to damage your computing assets and corporate brand.

Learn More

For more information, contact your McAfee representative or channel partner, or visit **www.mcafee.com**.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com