

THREATQ™ AND FIREEYE

Technology Segment: Malware Analysis

The combination of FireEye Malware Analysis and the ThreatQ platform allows organizations to rapidly address malicious activity.

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.

FIREEYE MALWARE ANALYSIS

FireEye Malware Analysis is a forensic analysis solution that gives security analysts hands-on control over powerful auto-configured test environments to safely execute and inspect advanced malware, zero-day and advanced persistent threat (APT) attacks embedded in web pages, email attachments and files.

Malware Analysis uses the FireEye Multi-Vector Virtual Execution™ (MVX) engine to provide in-house analysts with a full 360-degree view of an attack, from the initial exploit to callback destinations and follow on binary download attempts. As cyber criminals tailor attacks to penetrate a specific business, user account or system, analysts need easy-to-use forensic tools that help them rapidly address targeted malicious activities.

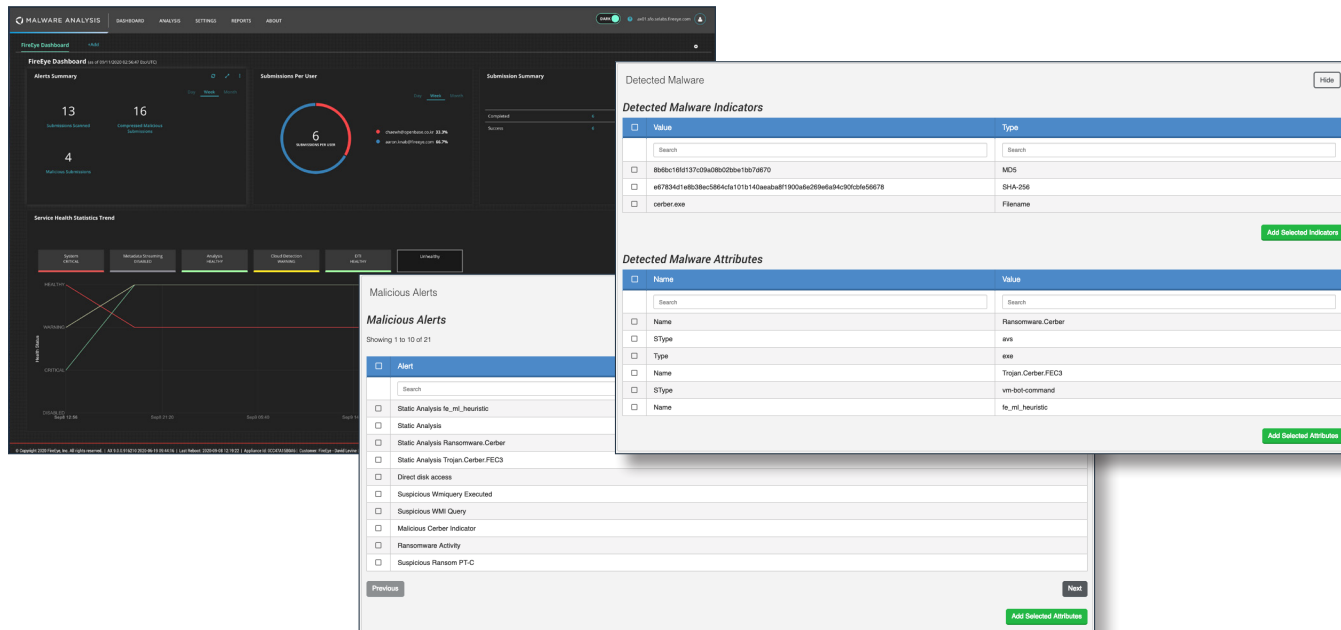
INTEGRATION HIGHLIGHTS

Submit files for analysis

Retrieve the reports back so the results can be added to ThreatQ as context

Query their FireEye Malware Analysis using indicators from ThreatQ to find any alerts related to those indicators

Seamlessly add and remove YARA rules from their FireEye AX series appliance.



INTEGRATION USE CASES:

The Integration supports a variety of use cases such as:

- Quickly and easily submit samples for analysis
- Retrieve results effortlessly
- Use ThreatQ for more simplified management of detection YARAs

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 more information, visit www.threatquotient.com.

ABOUT FIREEYE INC.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 9,300 customers across 103 countries, including more than 50 percent of the Forbes Global 2000.

For more information about this integration, contact the FireEye Technology Partners team at integrate@FireEye.com.