FIREEYE™

SOLUTION BRIEF

Intelligence-Based Enhancement of Malware Analysis

Technology Segment: Malware Analysis

HIGHLIGHTS

- Easily submit files for analysis
- Retrieve reports and add results to ThreatQ as context
- Query FireEye Malware Analysis (AX series) appliance using indicators from ThreatQ to find any alerts related to those indicators
- Seamlessly add and remove YARA rules from the Malware Analysis appliance.

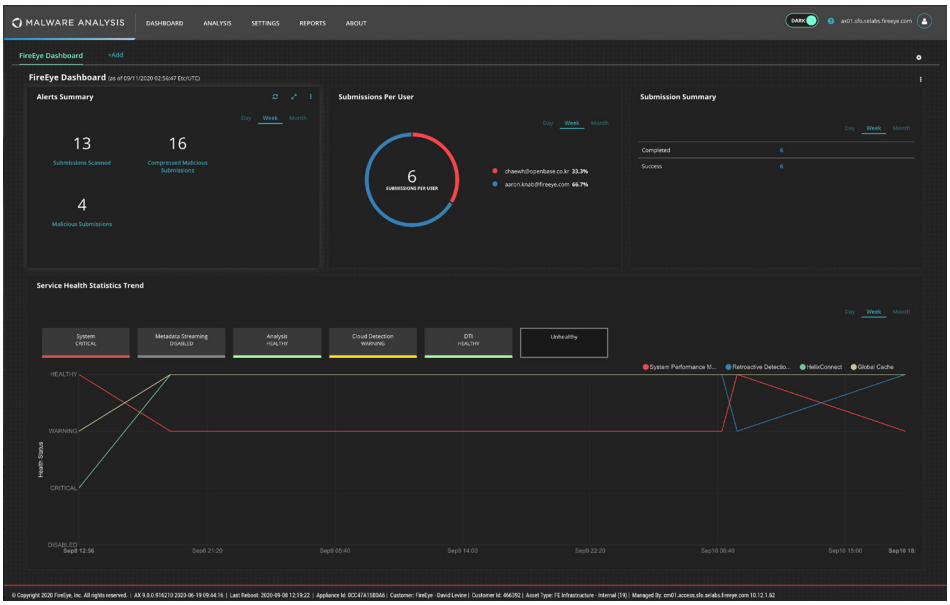
By combining FireEye Malware Analysis (AX series) with the ThreatQ platform, organizations can rapidly submit suspect files for analysis, receive results in reports that can be added to ThreatQ for future queries, and modify YARA rules in the Malware Analysis appliance.

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 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 to take the right actions faster.

Malware Analysis from FireEye
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.

THREATQUOTIENT



The integration of ThreatQ and FireEye Malware Analysis supports various use cases, such as:

Quickly and easily submit samples for analysis

- ThreatQ users can submit files to FireEye Malware Analysis, which 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.
- Through a pre-configured, instrumented Microsoft Windows and Apple MacOS X virtual analysis environment, the MVX engine fully executes suspicious code to allow deep inspection of common web objects, email attachments and files.

Retrieve results effortlessly

- Malware Analysis frees administrators from time-consuming setup, baselining and restoration of the virtual machine environments used in manual malware analysis.
- Security operations center analysts can use built-in customization and granular control over payload detonations
- Malware Analysis enables forensic analysts to arrive at a comprehensive understanding of the attack that is suited to the needs of the enterprise.

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 **https://threatquotient.com**.

For more information, contact the FireEye Technology Partners team at **integrate@FireEye.com**.

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2020 FireEye, Inc. All rights reserved. FireEye and Mandiant are registered trademarks of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.
NS-EXT-SB-US-EN-000326-01

About FireEye

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.