Alert Triage with Malware Analysis

Instructor-Led Training

Highlights

Duration

1 day

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry, and use of the command line interface (CLI).

How to Register

Public sessions are listed at https://trellix-training.netexam.com.

Private sessions are available. For further details and pricing, please contact your Trellix account representative.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities. To view our full course catalog, please visit https://trellix-training.netexam.com.

This course is designed to prepare learners to perform alert triage from MVX engine analysis using the Trellix Malware Analysis appliance.

Learners will develop knowledge and skills on the administration and use of the Trellix Malware Analysis appliance. The course offers a hands-on lab environment in which learners can submit malware samples for deep analysis and then interpret analysis results.

Learning Objectives

After completing this course, learners should be able to:

- Describe malware behaviors, stages of attack (malware lifecycle) and current trends in the threat landscape
- Explain the process and initial steps of conducting malware analysis
- Differentiate between static and dynamic analysis
- Understand the features and functions of the Malware Analysis appliance
- Submit malware samples to the appliance for deep analysis and alert triage
- Locate and use critical information in analysis results to assess a potential threat
- Identify indicators of compromise in analysis results
- Examine the use of YARA rules on Trellix appliances

Who Should Attend

Security professionals and incident responders who use Trellix Malware Analysis to detect, investigate, and prevent cyber threats.

Course Outline

1. Threats and Malware Trends
   - Malware overview and definition
   - Motivations of malware
   - MITRE ATT&CK framework
   - Types of malware
   - Emerging threat actors
2. Trellix Malware Analysis Appliance
   - Features and benefits
   - Deployment and analysis modes
   - Configure batch Malware Analysis
   - Manually submit a malware for analysis
   - Review analysis results
3. MVX Alerts
   - APIs
   - File and folder actions
   - Code injection
   - Processes
   - Mutexes
   - Windows Registry events
   - Network access
   - User Account Access (UAC)

Elective Content

The following additional lessons are available at no extra fee. These lessons are not relevant for all audiences, and are provided upon customer request, if time permits. Please coordinate with your Trellix instructor.

Custom Detection Rules

- YARA malware framework file signatures
- YARA on Trellix appliances
- YARA hexadecimal
- Regular expressions
- Conditions
- Snort rule processing
- Enabling Snort rules
- Creating a Snort rule

Trellix

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

112022-07