Trellix EDUCATION SERVICES

Investigations with File Protect

Instructor-Led Training

Highlights

Duration

1-day

Prerequisites

Students taking this course should have a working knowledge 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 analysts to triage and derive meaningful, actionable information from alerts on Trellix File Protect.

Learners assess threats using real-world scenarios in a hands-on lab environment. Activities include reviewing Trellix alerts and conducting in-depth analyses on the behaviors and attributes of malware.

Learning Objectives

After completing this course, learners should be able to:

- Recognize current malware threats and trends
- Understand the threat detection and prevention capabilities of your Trellix Security solution
- Locate and use critical information in a Trellix alert to assess a potential threat
- Examine OS and file changes in alert details to identify malware behaviors
- Identify indicators of compromise (IOCs) in a Trellix alert and use them to identify compromised hosts

Who Should Attend

This course is intended for security professionals and incident responders who use File Protect 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 File Protect**
    - Features and benefits
    - Configuring storage and scans
    - Accessing and reviewing
    - 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