Trellix

EDUCATION SERVICES

Investigations with Endpoint Security (HX)

Instructor-Led Training

Highlights

Duration

3-days

Prerequisites

Students taking this course should have a working knowledge of Windows operating systems, networking and network security, file system, registry, and regular expressions. Scripting experience with Python or PowerShell is beneficial.

Recommended Pre-Training

Endpoint Security (HX) for Adminstrators eLearning

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 covers the fundamentals of live analysis and investigation for endpoints with Trellix Endpoint Security (HX).

Hands-on activities span the entire investigations process, beginning with a Trellix-generated alert, leading to discovery and analysis of the host for evidence of malware and other unwanted intrusion. Analysis of computer systems will be performed using Trellix products and freely available tools.

Learning Objectives

After completing this course, learners should be able to:

- Describe methods of live analysis
- Use core analyst features of Endpoint Security (HX) such as alerting, enterprise search, and containing endpoints
- Validate and provide further context for Trellix alerts
- Demonstrate the ability to plan, execute and report on a digital investigation
- Analyze a data collection from Endpoint Security (HX) using a defined methodology
- Identify malicious activity hidden among common Windows events

Who Should Attend

This course is intended for Network security professionals and incident responders who must use Endpoint Security (HX) to investigate, identify and stop cyber threats, as well as security analysts who want to learn investigation techniques used to respond to today's cyber threats.

Course Outline

Day 1

1. **Threats and Malware Trends**
   - Threat landscape
   - Attack motivations
   - MITRE ATT&CK framework
   - Emerging threat actors
2. **Initial Alerts**
   - Trellix Endpoint Security (HX) alerts
   - Triage with Triage Summary
   - Trellix Network Security alerts
   - Identifying forensic artifacts in the OS Change detail
   - Mapping artifacts in an alert to host activity
3. **Using Audit Viewer and Redline®**
   - Access triage and data collections for hosts.
   - Navigate a triage collection or acquisition using Redline® or Audit Viewer
   - Apply tags and comments to a triage collection to identify key events
4. **Windows Telemetry**
   - Live investigation overview
   - Windows telemetry
     - **Memory artifacts**
     - **System information**
     - **Processes**
     - **File system**
     - **Configuration files**
     - **Services**
     - **Scheduled tasks**
     - **Logging**
   - Choosing Data to acquire

Day 2

1. **Acquisitions**
   - Triage and real-time events
   - Live system acquisitions
   - Bulk Acquisitions
   - Endpoint Security (HX) REST API
2. **Endpoint Security (HX) extended capabilities**
   - Endpoint Security (HX) modules
   - HXTool

Day 3

1. **Investigation Methodology**
   - MITRE ATT&CK framework
   - Mapping evidence to attacker activity:
     - **Evidence of initial compromise**
     - **Evidence of persistence**
     - **Evidence of lateral movement**
     - **Evidence of internal reconnaissance**
     - **Evidence of data exfiltration**
2. **Capstone Capture the Flag (CTF)**

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.

Endpoint Security (HX)
Extended Capabilities

- Open IOC Editor
- GoAuditParser

Trellix

Visit Trellix.com to learn more.

092023-20