Trellix

EDUCATION SERVICES

Alert Analysis and Investigations with Network Security and Endpoint Security (HX)

Instructor-Led Training

Highlights

Duration

4 days

Who Should Attend

This course is intended for security analysts, incident responders, and threat hunters who use Network Security or Endpoint Security (HX) to detect, investigate, and prevent cyber threats.

Prerequisites

Students taking this course should have a working knowledge of Windows operating systems, networking and network security, file system, registry and regular expressions, and experience scripting in Python.

Recommended Pretraining

- Network Security for System Administrators (eLearning)
- Endpoint Security (HX) for Analysts (eLearning)

How to Register

This course is available for purchase 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 examines how to triage alerts generated by the Trellix Network Security and Endpoint Security (HX) platforms, derive actionable information from those alerts, and inspect affected endpoints using live analysis and investigation fundamentals.

Hands-on activities span the entire analysis and live investigation process, beginning with a Trellix-generated alert, leading to discovery and analysis of the host for evidence of malware and other unwanted intrusion. Endpoint analysis focuses on investigation techniques using features of Endpoint Security (HX), such as the Triage Summary, Audit Viewer, and Acquisitions.

Learning Objectives

After completing this course, learners should be able to:

- Recognize current malware threats and trends
- Interpret alerts from Network Security and Endpoint Security (HX) products
- Locate and use critical information in Trellix alerts to assess a potential threat
- Define indicators of compromise based on an alert and identify compromised hosts
- Describe methods of live analysis
- Create and request data acquisitions to conduct an investigation
- Define common characteristics of Windows processes and services
- Investigate a data collection from Endpoint Security (HX) using a defined methodology
- Identify malicious activity hidden among common Windows events

Course Outline

Day 1

1. **Threats and Malware Trends**
   - Threat landscape
   - Attack motivations
   - MITRE ATT&CK framework
   - Emerging threat actors
2. **Initial Alerts**
   - Endpoint Security (HX) alerts
   - Triage with Triage Summary
   - Network Security alerts
   - Identifying forensic artifacts in the OS Change Detail
3. **MVX Alerts**
   - Trellix alert types
   - Identifying forensic artifacts in the OS Change Detail
   - Callbacks
   - SmartVision
   - Threat assessment

Day 2

1. **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
2. **Windows Telemetry and Acquisitions**
   - Live forensic overview
   - Windows telemetry
   - Acquiring data

Day 3

1. **Acquisitions**
   - Triage and real-time events
   - Live system acquisitions
   - Bulk acquisitions
   - Endpoint Security (HX) REST API
2. **Modules**
   - Administration
   - Detection and protection
   - Response

Day 4

1. **Investigation Methodology**
   - MITRE ATT&CK framework
   - Mapping evidence to attacker activity
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.

1. **Custom Detection Rules**
   - Yara malware framework
   - Snort rules
2. **Endpoint Security (HX): Extended Capabilities**
   - Trellix Market
   - HXTool
   - Open IOC editor

Trellix

Visit Trellix.com to learn more.

092023-18