Alert Analysis and Investigations with Network Security

Instructor-Led Training

Highlights

Duration

3 days

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and regular expressions, and experience scripting in Python.

Recommended Pretraining

- Network Security for System Administrators (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 three-day course examines how to triage alerts generated by Trellix Network Security, derive actionable information from those alerts, and apply the fundamentals of live analysis and investigation to investigate associated endpoints.

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. Analysis will be performed using Trellix products and freely available tools.

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 Redline® triage collection using a defined methodology
- Identify malicious activity hidden among common Windows events
- Validate and provide further context for alerts using Redline®

Who Should Attend

Security analysts, incident responders, and network security professionals who use Trellix Network Security to detect, investigate, and prevent 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
   - 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
     - Memory artifacts
     - System information
     - Processes
     - File system
     - Configuration files
     - Services
     - Scheduled tasks
     - Logging
   - Acquiring data

Day 3

1. Investigation Methodology
   - Areas of evidence
   - 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.

Custom Detection Rules

- Yara malware framework
- Snort rules

Endpoint Security (HX): Extended Capabilities

- Trellix Market
- Endpoint Security (HX) modules
- HXTool
- Open IOC editor
- Endpoint Security (HX) REST API

Visit Trellix.com to learn more.

Trellix

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