Trellix

Network Traffic Analysis with Network Forensics

Instructor-Led Training

Highlights

Duration

2 days

Prerequisites

A working understanding of networking and network security, knowledge of Wireshark recommended.

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 and concepts of network traffic analysis—how to search, filter, analyze, reconstruct, and preserve network traffic; and how to apply techniques learned to conduct a network forensics investigation utilizing the Trellix Network Forensics solution.

Hands-on activities include building an analysis dashboard, executing queries, filtering results, and reconstructing network traffic. On Day 2, learners will pursue an alert and identify anomalies in network traffic to uncover and document indicators of compromise (IOCs) that build a case for a real-world advanced threat.

Learning Objectives

After completing this course, learners should be able to:

- Describe networking models, network data, critical application protocols, network flow, and common attacks on protocols
- Perform network traffic analysis and investigations using Trellix Network Forensics
- Customize the analysis environment with dashboards, network visualizations, scheduled queries, and lists
- Reconstruct carved artifacts/files from network packet data and submit them for malware analysis
- Investigate an advanced persistent threat (APT) attack based on aggregated alerts and network traffic anomalies

Who Should Attend

Network security professionals and incident responders who use Trellix Packet Capture and Investigation Analysis appliances to analyze cyber threats through packet data.

Course Outline

Day 1: Fundamentals

1. Appliance Overview and Network Placement
   - Trellix Packet Capture
   - Trellix Investigation Analysis
   - Analysis workflow example
   - The Trellix Packet Capture and Trellix Investigation Analysis relationship
   - Common deployments
2. Network Traffic Analysis Foundations
   - Network models and encapsulation: TCP/IP, UDP
   - The three-way handshake
   - Network forensics data
   - Packet captures
   - Flow data
   - Network flow analysis
   - Critical application protocols
   - Protocols in the TCP/IP stack
   - Common attacks on protocols
3. Queries, Reconstruction and Alerts with Investigation Analysis
   - Working with dashboards
   - Searching for network data
   - Constructing queries
   - Network metadata analysis
   - Stacking metadata
   - Filtering traffic using network metadata
   - Scheduling queries and reporting
   - Lists
   - Extracting endpoint information
   - Trellix alerts from integrated appliances
   - Configuring event-based capture rule sets
   - Working with rule sets
   - Network data reconstruction

Day 2: Investigation Workshop

1. Network Investigation Scenario
   - Investigation tools
   - Six steps of an attack
   - Common indicators of compromise
   - Threat group overview
   - Trellix Network Forensics investigations
   - Documenting the investigation
   - Threat group intelligence
   - Attack phases covered in class
   - Investigation labs overview
2. Starting with Leads
   - Alerts on Trellix Investigation Analysis
   - Alerts on Trellix Network Security
   - Unusual HTTP user agents
   - Unusual POST requests
   - Trellix Investigation Analysis components
   - Other possible leads
3. Investigating the Leads
   - Dive deeper
   - HTTP artifacts analysis
   - Encrypted flows
   - Email analysis
4. Investigation Summary and Conclusions
   - Investigation summary
   - Stages of the attack
   - Creating a case

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.

- Queries, reconstruction, and alerts with Trellix Packet Capture

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.