Trellix

EDUCATION SERVICES

Network Forensics Administration

Instructor-Led Training

Highlights

Duration

1-day

Prerequisites

A working understanding of the command line interface (CLI) and the Linux Operating system, and familiarity with network security.

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 entry-level course covers deployment options, basic administration, and configuration of the integrated Trellix technologies for the Trellix Network Forensics appliances—Packet Capture and Investigation Analysis.

Hands-on activities include post-installation tasks, system health checks, pairing a Packet Capture appliance with the Investigation Analysis system, daily system administration tasks, configuring Event Based Capture, and integration of another Trellix system for alerts.

Learning Objectives

After completing this course, learners should be able to:

- Provide an overview of Packet Capture and Investigation Analysis appliances.
- Describe the common deployment of Packet Capture and Investigation Analysis in the context of other Trellix products and services.
- Access the various administration interfaces for Packet Capture and Investigation Analysis.
- Perform primary management and administration tasks for Packet Capture and Investigation Analysis.
- Configure and integrate Packet Capture and Investigation Analysis with various supported Trellix technologies

Who Should Attend

Network security professionals and system administrators who operate and administer Trellix Packet Capture and Investigation Analysis appliances and integrate them with other Trellix technologies.

Course Outline

1. **Appliance Overview and Network Placement**
   - Packet Capture
   - Packet Capture: Deployments
   - Investigation Analysis
   - Investigation Analysis: Deployments
   - Network Forensics: Appliance relationship
   - Basic hardware components
   - Network Forensics integrations overview
   - Lab: Start up the training environment
2. **Network Forensics Administration Interfaces**
   - Network Forensics administration interfaces
   - CLI via SSH
   - CLI via the IPMI
   - Accessing admin-level commands
   - Configuration mode
   - Accessing the Web UI
   - Lab: Configure Packet Capture (PX)
   - Lab: Configure Investigation Analysis (IA)
3. **Network Forensics Administration Tasks**
   - Identity management
   - Authentication
   - CLI authentication type
   - CAC/PIV authentication
   - Local users and roles
   - System management
   - Processes
   - Restarting processes
   - Logs
   - Web UI admin pages
   - Show command
   - IA appliance groups
   - Rules and software management
   - Uploading software on Investigation Analysis
   - Updating software from Investigation Analysis
   - Configuring and deploying EBC
   - Load management
   - PX metadata filtering
   - DNS aggregation management
   - Lab: Pair Packet Capture and Investigation Analysis
4. **Configuring Trellix Integrations**
   - Packet Capture and Helix
   - Packet Capture and Threat Intelligence
   - Packet Capture and Network Security
   - Investigation Analysis and Packet Capture
   - Investigation Analysis and Trellix alert aggregation
   - Investigation Analysis and Malware Analysis
   - Utilizing Network Security as a sensor
   - Investigation Analysis and Endpoint Security (HX for host metadata
   - Lab: Set up Network Forensics aggregated alerts with an integrated Trellix system

Trellix

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. 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, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.

09023-25