Trellix EDUCATION SERVICES

Network Forensics for System Administrators

Self-Paced Online Training

Highlights

Duration

4-hours

Prerequisites

Students taking this course should have a working understanding of the command line interface (CLI) and the Linux Operating system, and familiarity with network security.

How to Register

This course is available for purchase at 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—Trellix Packet Capture and Trellix Investigation Analysis.

Learning Objectives

After completing this course, learners should be able to:

- Describe the function and purpose of the Trellix Network Forensics appliances
- Illustrate the deployment of Network Forensics appliances in a typical network.
- Perform system readiness checks on a standalone deployment of Trellix Network Forensics appliances post baseline configuration.
- Perform administration tasks pertaining to access, processes, rules, and software management.
- Configure the various integrations between the Network Forensics appliances and other supported Trellix appliances.

Who Should Attend

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

Course Outline

1. **Platform Introduction**
   - Trellix Packet Capture
   - Trellix Investigation Analysis
   - Analysis Workflow Example
2. **Network Forensics Deployment**
   - Packet Capture Deployment Options
   - Trellix Investigation Analysis Deployment Options
3. **Network Forensics System Readiness**
   - System Readiness Checks
   - The Command Line Interface (CLI)
   - CLI Checks
   - Web UI Checks
   - Health Status
   - The CLI Show Command
4. **Access Management**
   - Network Forensics Authentication Methods
   - Setting the Authentication Type
   - SmartCard (CAC/PIV) Authentication
   - Creating Users and Assigning Roles
5. **Process Management**
   - Processes
   - Restarting System and Processes
   - Logs
   - Setting Log Levels
6. **Rules and Software Management**
   - Configuring an EBC Rules Set
   - Appliance Groups
   - Deploying EBC Rules
   - Deploying Software Updates
7. **Metadata Load Management**
   - Configuring Metadata Filters
   - Setting DNS Flow Aggregation
8. **Configuring Trellix Integrations**
   - Trellix Network Security Integration
   - Helix Integration
   - Trellix Packet Capture and Helix Integration
   - Trellix Packet Capture and Threat Intelligence
   - Trellix Investigation Analysis Master Node and Trellix Packet Capture
   - Trellix Investigation Analysis and Threat Intel Integration
   - Alerts Aggregation
   - Trellix Malware Analysis Integration
   - Utilizing Trellix Network Security as a Sensor
   - Add Trellix Network Security as a Sensor

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.