DATA SHEET

FireEye Network Forensics: Administration and Integration (WBT)

Self-paced online training

HIGHLIGHTS

Duration
4 Hours

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

How to Register
Please contact your FireEye account representative for pricing options.

An instructor-led version of this course is also available as an optional delivery with the Fundamentals of Network Traffic Analysis using FireEye Network Forensics course. Visit https://www.fireeye.com/services/training/courses for more details.

This entry-level, self-paced, online course covers deployment options, basic administration, and configuration of the integrated FireEye technologies for the FireEye Network Forensics appliances—Packet Capture (PX) and Investigation Analysis (IA).

There are no lab exercises in this course.

Learning Objectives

After completing this course, learners should be able to:

- Describe the function and purpose of the FireEye Network Forensics appliances (PX and IA Series)
- Illustrate the deployment of Network Forensics appliances in a typical network.
- Perform system readiness checks on a standalone deployment of FireEye 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 FireEye appliances.

Who Should Attend

Network security professionals who administer and operate FireEye Packet Capture (PX) and Investigation Analysis (IA) appliances, and integrate them with other FireEye technologies.

Course Outline

1. Platform Introduction
   - FireEye Packet Capture (PX)
   - FireEye Investigation Analysis (IA)
   - Analysis Workflow Example

2. Network Forensics Deployment
   - Packet Capture (PX) Deployment Options
   - FireEye 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 PX Metadata Filters
   - Setting DNS Flow Aggregation

8. Configuring FireEye Integrations
   - PX-NX Integration
   - PX-Helix Integration
   - Packet Capture (PX) and Helix Integration
   - Packet Capture (PX) and Threat Intelligence
   - Investigation Analysis (IA) Master Node and Packet Capture (PX)
   - Investigation Analysis and Threat Intel Integration
   - Alerts Aggregation
   - Malware Analysis Integration
   - Utilizing NX as a Sensor
   - Add NX as a Sensor on IA
   - IA-HX for Host Metadata

For more details, or to view our full course catalog, please visit https://www.fireeye.com/services/training/

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.