DATA SHEET

FireEye Endpoint Security Administration and Diagnostics

Instructor-led training

HIGHLIGHTS

Duration
2 Days

Prerequisites
Experience with network administration and support.

How to Register
Public sessions are listed on our course calendar.
https://www.fireeye.com/services/training/schedule/

Private sessions are available. Please contact your FireEye account representative for scheduling and pricing options.

This course introduces deployment, configuration and basic administration for FireEye Endpoint Security.

From this baseline, the workshop introduces a framework for troubleshooting the FireEye Endpoint Security Server and the FireEye agent. The course includes checklists, case studies and guidance for transitioning difficult cases to the FireEye support team. Optional modules expand this workshop to include FireEye core hardware and virtual appliances.

This workshop is experimental hands-on and will give learners experience with administering Endpoint Security, adjust common configurations, and resolving common issues.

Learning Objectives

After completing this course, learners should be able to:

- Identify the components needed for FireEye Endpoint Security deployment
- Identify the key phases of Endpoint Security operation
- Perform the initial configuration of Endpoint Security appliances and hosts
- Create custom rules
- Understand core analyst features of Endpoint Security such as alerting, enterprise search, and containing endpoints
- Resolve issues commonly encountered with Endpoint Security Agent whitelisting
- Validate endpoints to ensure that they are performing as expected
- Use Endpoint Security logs and diagnostics for troubleshooting
- Explore common issues across core installations
- Understand common issues with hardware and virtual appliances

Who Should Attend

Network security professionals and FireEye administrators and analysts who must set up or work with the FireEye Endpoint Security platform.

Course Outline

1. Administration and Configuration
   - Endpoint Security Operational Overview
   - FireEye Endpoint Security agent
   - Ring buffer
   - Appliance configuration
   - Agent management and configuration
   - Host management
2. Rules and Alerts
   - Rules
   - Alerts and Alert Types
   - Triage Summary
   - Searching across all hosts in the enterprise
   - Acquiring files, triage packages, other built-in acquisitions
3. Deployment Diagnostics
   - Checking hardware deployment
   - Agent compatibility and installation
4. FireEye Core Product Diagnostics
   - Diagnostic process
   - Basic Troubleshooting
   - Best practice
   - Common issues
     - Licensing
     - Operation
     - Notifications
     - Boot
     - Upgrade
5. Hardware Troubleshooting
   - Troubleshooting PSU and HDD issues
   - Universal LED and Raid configuration
6. Virtual Hardware Troubleshooting
   - Installation
   - Licensing and setup
7. Logs
   - Obtaining logs and configuration files
   - Searching and understanding logs
   - Creating endpoint diagnostics
8. Connectivity
   - Agent connectivity and validation
   - Determine communication failures
9. Containment and Whitelisting
   - Containment Settings
   - Whitelisting known files and 3rd party programs
   - Validating a whitelist
10. Performance
    - General performance settings
    - Understanding and editing polling
    - Evaluating individual endpoints
11. FireEye Support and Community
    - Transitioning a case to FireEye Customer Support
    - Using the FireEye Customer Portal

Optional Content

1. Audit Viewer
   - Types of Analysis Data
   - Searching and filtering acquisition data
   - Applying tags and comments

Instructor-led sessions are typically a blend of lecture and hands-on lab activities.

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

About FireEye

FireEye offers an innovative platform that eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.