Endpoint Security (HX) Administration
Instructor-Led Training

Highlights

Duration

1 day

Prerequisites

Students taking this course should have a working knowledge of network administration and support.

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 provides a framework for troubleshooting the Trellix Endpoint Security (HX) server and the Trellix Agent.

The course introduces deployment, configuration and basic administration for Endpoint Security (HX), and includes checklists, case studies and guidance for transitioning difficult cases to the Trellix support team.

Attendees will gain hands-on experience administering the appliance and diagnosing common issues.

Learning Objectives

After completing this course, learners should be able to:

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

Who Should Attend

This course is intended for system administrators responsible for implementing and maintaining the Trellix Endpoint Security (HX) server and endpoint agent (xAgent).

Course Outline

Section 1: Administration

1. Deployment, Administration, & Configuration
   - Appliance management
   - Host management
   - Agent management

2. Detection and Containment
3. Modules

Section 2: Diagnostics

1. Hardware Diagnostics
2. Core Product Diagnostics
3. Endpoint Security Server logs
4. Troubleshooting the Agent
5. Agent Policies and