

Intrusion Prevention System Administration

Instructor-Led Training

Highlights

Duration

4-days

Prerequisites

Students taking this course should have a working knowledge of Microsoft Windows administration, system administration concepts, a basic understanding of computer security concepts, and a general understanding of internet services.

How to Register

This course is available for purchase 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 is a key resource for successful implementation of the Trellix Intrusion Prevention strategy for enterprises. The hands-on lab sessions help you learn how to deploy and configure the Intrusion Prevention System as a solution to protect against real-world attacks.

Learning Objectives

After completing this course, learners should be able to:

- Plan the deployment of Intrusion Prevention System (IPS)
- Install and configure the IPS Manager
- Install and configure Sensor(s)
- Create, configure, and manage administrative domains, users and user roles, and IPS policies
- Describe attack types and configure protection against attacks
- Analyze and respond to potential network threats
- Map and configure network appliance(s) (Sensors)
- Manage Firewall Policy configuration.
- Perform IPS database maintenance.

Who Should Attend

This course is intended for analysts and/or engineers responsible for configuration, management, and monitoring activity on their systems, networks, databases, and applications.

Course Outline

Day 1:

- Welcome
- Introduction to IPS
- Planning IPS Deployment
- Getting Started
- Notification Configuration
- User Management
- Administrative Domains

Day 2:

- Sensor Overview
- Basic Sensor Management
- Advanced Sensor Management
- Policy Configuration
- Policy Customization
- Virtualization (Sub-interfaces)

Day 3:

- Threat Explorer
- Attack Log
- DoS Attacks
- Advanced Malware Detection
- Advanced Callback Detection
- Inspection Options Policies

Day 4:

- Web Server Protection
- Firewall Policy Configuration
- Policy Tuning
- Report Generation
- Operational Status
- Database Maintenance
- Troubleshooting

Visit [Trellix.com](https://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>.