



5051 Westheimer
Suite 500
Houston, Texas 77056
(713) 871-8411
866-88-C-TREC
Fax (713) 622-1915

Class Code: iPS
Number of Days: 4
Format: Instructor-Led

Implementing Cisco Intrusion Prevention Systems (6.0)

Course Description: Securing Networks Using Intrusion Prevention Systems (IPS) v6.0 is an update to Securing Networks Using Intrusion Prevention Systems (IPS) v5.0, an existing five-day instructor led course on using the Cisco Intrusion Detection System v. 5.0 product to protect network systems from intrusions and security threats. The course covers important new IPS 6.0 features. The IPS 6.0 course takes a task-oriented approach to teaching the skills to deploy, configure and administer Cisco IPS sensors.

Prerequisites: To fully benefit from this course, learners should have the following prerequisite skills and knowledge:

- CCNA or the equivalent knowledge
- Basic knowledge of Windows operating system
- Familiarity with the networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications)

Delivery Method: Instructor led, group-paced, classroom-delivery learning model with structured hands-on activities.

Course Objectives

Students will deploy, configure, and administer Cisco IPS sensors to protect network devices as well

Course Outline

- Intrusion Prevention Overview
- Getting Started with the IPS Command Line Interface
 - a. Lab Exercises: Getting Started with the IPS Command Line Interface
- Using the IPS Device Manager
 - a. Lab Exercise: Using the IPS Device Manager
- Basic Sensor Configuration
 - a. Lab Exercise: Basic Sensor Configuration
- Cisco Intrusion Prevention System Signatures and Alarms
 - a. Lab Exercise: Signatures and Alarms
- Signature Engines
- Signature Configuration
 - a. Lab Exercise: Signature Configuration
- Turning the Sensor
 - a. Lab Exercise: Tuning the Sensor Using IDM

Course Outline - Continued

- Alarm Monitoring and Management
 - a. Lab Exercise: Alarm Monitoring and Management
- Configuring Blocking
 - a. Lab Exercise: Configuring Blocking
- Cisco Intrusion Detection System Module
- Capturing Network Traffic
- Maintaining Sensors
- Verifying System Configuration
 - a. Lab Exercise: Verifying System Configuration
- Configuring Anomaly Detection, Passive OS fingerprinting, and CSA Collaboration