Global Knowledge Course Name: IPS (Implementing Cisco Intrusion Prevention System v6.0) Code 5702

Course Overview:

Cisco Course v6.0 | Prepares you for Cisco Exam 642-533 IPS
In this Global Knowledge-enhanced 4-day course, you will gain the skills required to deploy Cisco's recently updated version 6.0 network-based intrusion prevention system. New features added to version 6.0 include virtual sensor support, passive OS fingerprinting and anomaly detection. The course introduces you to Cisco IDS detection platforms, including the 4200 series Sensors, the Catalyst 6000 series Intrusion Detection Module 2 (IDSM2), the Advanced Inspection and Prevention Security Services Module (AIP-SSM), and the IDS Network Module (NM-CIDS). The command line and the IPS Device Manager GUI are used to configure the sensor.

Why Take IPS from Global Knowledge?
Our IPS labs go above and beyond the standard Cisco IPS labs. The focus on signatures-the heart of IPS sensor technology-is our most significant enhancement. In fact, signatures are triggered in our very first IPS sensor lab. We also created an exclusive lab to demonstrate the internal specifications of different signature engines. In our labs, signatures are triggered via realistic intrusion attempts, not just arbitrary methods, and you'll learn why particular signatures are triggered when attack conditions are initiated, whether through the use of a network attack tool or entering a suspicious request in a web browser. Our labs take the mystery out of the sensor, allowing you to understanding how signatures are implemented and what causes them to trigger and making you comfortable with the technology.

What You'll Learn:

- How Cisco IPS protects network devices from attacks
- Basic intrusion prevention terminology
- Different intrusion prevention technologies and evasive techniques
- Cisco IPS Sensor platforms and their features
- Install and configure basic settings on a Cisco IPS 4200 Series Sensor
- Use the Cisco IPS Device Manager (IDM) to configure built-in signatures to meet the requirements of a given security policy
- Create and implement customized intrusion prevention signatures
- Create alarm filters to reduce alarms and possible false positives
- Configure IPS protective reactions such as TCP reset and deny attacker inline
- Configure a Cisco IPS Sensor to perform blocking on IOS routers and PIX firewalls
- Perform maintenance operations such as signature updates

- Configure and monitor anomaly detection, passive OS fingerprinting, and virtual sensors
- Initialize and install remaining Cisco IPS family of products
- Use the CLI and Cisco IDM to obtain system information
- Configure the Cisco IPS sensor to allow a SNMP NMS to monitor the Cisco IPS sensor

Who Needs to Attend?

- Internetwork professionals who want to ensure security on their network or who seek Cisco certification.

Course Content:

Intrusion Prevention Overview

- Explanation of Intrusion Prevention
- Cisco IPS Products
- Cisco IPS Sensor Software Solutions
- Evasive Techniques

Installation of a Cisco IPS 4200 Series Sensor

- Installing an IPS Sensor Using the CLI
- Using the Cisco IDM
- Configuring Basic Sensor Settings

Cisco IPS Signatures

- Configuring Cisco IPS Signatures and Alarms
- Signature Engines
- Customizing Signatures

Advanced Cisco IPS Configuration

- Advanced Tuning of Cisco IPS Sensors
- Monitoring and Managing Alarms
- Configuring a Virtual Sensor
- Configuring Advanced Features
- Configuring Blocking

Additional Cisco IPS Devices

- Cisco IDS Module
- Cisco ASA AIP-SSM

Cisco IPS Sensor Maintenance

- Maintaining Cisco IPS Sensors
- Managing Cisco IPS Sensors