

Cisco® Secure Intrusion Detection System (CSIDS)

(4 day Instructor-Led Course)

Course Description

Gain the knowledge and skills needed to design, install and configure a Cisco Intrusion Protection solution for small, medium and enterprise networks. This hands-on course covers CIDS detection platforms including the 4200 series Sensors and the Catalyst® 6000 series Intrusion Detection Module (IDSM). The Cisco IDS Host Sensor is also introduced.

Who Should Attend

- Cisco customers who implement and maintain IDS solutions
- Cisco Systems® Engineers who support sales of Cisco IDS and security product solutions

Prerequisites

- *CCNA Training*
- *Strong user level experience with Windows operating systems and a basic understanding of the UNIX operating system*
- *Familiarity with networking and security terms and concepts*

What You Will Accomplish

- Describe the basic intrusion detection terminology
- Explain the different intrusion detection technologies and evasive techniques
- Design a Cisco IDS protection solution for small, medium and enterprise customers
- Identify the Cisco IDS Sensor platforms and describe their features
- Install and configure a Cisco IDS Sensor including a network appliance and IDS module
- Tune CIDS signatures to work optimally in unique network environments
- Create and implement customized intrusion detection signatures
- Create alarm exceptions to reduce alarms and possible false positives
- Configure a CIDS Sensor to perform device management of supported blocking devices
- Describe the CIDS signatures and determine the immediate threat posed to the network
- Perform maintenance operations such as signature updates, software upgrades, data archival and license updates
- Describe the CIDS architecture including supporting services and configuration files
- Manage a large scale deployment of CIDS Sensors with CIDS Management and Monitoring software

What You Will Receive

- Study guide: Cisco Secure Intrusions Detection Systems

Certification Preparation

This course helps prepare you for CCIP, CCSP, and Security certifications. It maps to exam 9E0-100 ISIDS.

Course Outline: CSIDS™ (Cisco Secure Intrusion Detection System)

Establishing Network Security with Cisco

- Understanding the need for network security
- Recognizing network security threats
- Comparing attack types and methods
- Analyzing the Cisco security wheel
- Describing SAFE/AVVID

Studying Intrusion Detection

- Discussing intrusion detection terminology and technology
- Studying host/network based IDS
- Practicing intrusion detection evasive techniques

Protecting against Intrusion

- Working with network/host sensor platforms
- Communicating with IDS
- Deploying IDS

Installing the Sensor Appliance

- Initializing the sensor
- Performing basic sensor commands

Employing Cisco IDS Device Manager and Event

- Viewer
- Installing and implementing IDS device manager
- Installing and implementing IDS event viewer
- Working with the network security database

Configuring a Sensor

- Setting up the sensor
- Communicating with the sensor host
- Logging the sensor

Recognizing Cisco IDS Alarms and Signatures

- Explaining alarms and signatures
- Describing IDS micro-engines

Setting Up Sensing

- Configuring for global sensing
- Configuring for signatures
- Filtering signatures
- Recognizing custom signatures
- Tuning the signatures

Configuring IP Blocking

- Considering ACL
- Configuring IP blocking sensor
- Understanding manual IP blocking functions

Capturing Network Traffic for IDS

- Practicing capture techniques
- Setting up switch SPAN
- Configuring the Catalyst 6500 switch
- Capturing advanced traffic

Setting Up the IDS Module

- Introducing IDSM
- Analyzing IDSM ports and traffic
- Initializing IDSM
- Practicing commands
- Troubleshooting

Maintaining Cisco IDS

- Maintaining software
- Updating sensors
- Updating IDSM

Establishing Cisco IDS Architecture

- Building software architecture
- Communicating
- Setting up directory architecture
- Installing service files

Managing Enterprise IDS

- Installing IDS management center
- Studying architecture directories and elements
- Setting up sensors and sensor groups
- Configuring sensors
- Generating, approving, and deploying configuration files
- Administering the IDS management center server

Monitoring and Reporting Enterprise IDS

- Installing
- Configuring security monitor
- Working with event viewer
- Reporting