Securing Cisco® Networks with SourceFire FireSIGHT Intrusion Prevention System v2.0 (SSFIPS)

Course Overview

This is a 5-day class

Securing Cisco Networks with Cisco FireSIGHT Intrusion Prevention System (IPS) is an instructor-led, lab-intensive, course that introduces students to the powerful features of the Cisco FireSIGHT system, in-depth event analysis, IPS tuning and configuration, and the SNORT rules language.

You will learn how to use and configure next-generation Cisco IPS technology, including application control, firewall, and routing and switching capabilities. You will also learn to properly tune systems for better performance and greater network intelligence while taking full advantage of powerful tools for more efficient event analysis, including file type and network-based malware detection.

This course combines lecture materials and hands-on labs throughout to make sure you are able to successfully deploy and manage the Cisco FireSIGHT system. This course prepares you to take the Securing Cisco Networks with FireSIGHT IPS exam (exam ID 500-285).

Who Should Attend

This course is designed for technical professionals who need to know how to deploy and/or manage a Cisco FireSIGHT system in a network environment. The primary audience for this course includes:

Security administrators
Security consultants
Network administrators
System engineers
Technical support personnel
Channel partners and resellers

Course Objectives

Securing Cisco® Networks with SourceFire FireSIGHT Intrusion Prevention System v2.0 (SSFIPS)

Upon successful completion of this course and it's labs you should be able to:

Describe the FireSIGHT system training infrastructure
Navigate the user interface and administrative features of the FireSIGHT system, including reporting functionality to properly assess threats
Describe how to deploy and manage Cisco FireSIGHT devices
Describe the various detection technologies used in the FireSIGHT system
Describe, create, and implement objects for use in Access Control policies
Describe advanced policy configuration and FireSIGHT system configuration options
Analyze events
Write and configure basic SNORT rules

Other Prerequisites

The following prerequisites are recommended:

Technical understanding of TCP/IP networking and network architecture
Basic familiarity with the concepts of intrusion detection systems (IDS) and IPS

Course Outline

1 Module 1

FireSIGHT System Overview and Classroom Setup

2 Module 2

Hardware Overview and Architecture

3 Module 3

Device Management

4 Module 4

User Account Management

5 Module 5

Object Management

6 Module 6

Access Control Policy

7 Module 7

FireSIGHT Technology

Securing Cisco® Networks with SourceFire FireSIGHT Intrusion Prevention System v2.0 (SSFIPS)