



Securing Hosts Using Cisco Security Agent

HIPS

2 day

Overview :

HIPS is a two-day, lab-intensive Instructor-Led course which develops the knowledge and skills to deploy, configure and administer the Cisco Security Agent product to protect server and workstation hosts. It takes a task-oriented approach, using lecture and hands-on labs to teach the skills. The Cisco Security Agent functions to protect from intrusions, as compared to simply detecting attempted intrusions.

Target Audience :

- Engineers who support sales of Cisco security product solutions.
- Cisco Channel Partners, who sell, implement and maintain secure networks.
- Cisco Customers who implement and maintain secure networks.

At the end of the course, delegates will be able to:

- Describe the need for network security; understand attack types, methods and Cisco security wheel.
- CSA overview – functionality, components and architecture.
- CSAMC install – overview, system requirements for management console.
- CSAMC quick start configuration –configure a group, build an agent kit, view registered hosts, configure a policy, attach a policy to a group and generate rule programs
- CSAMC administration—accessing and using the management console.
- Configure groups and manage hosts. Build agent kits and distributing software updates.
- Develop a security policy.
- Configure policies and rules for Windows and UNIX.
- Use system correlation and heuristics.
- Understand and configure application classes.
- Configure variables—file sets, network address sets, network services, registry sets, COM component sets.
- Use CSA Profiler for data analysis and as policy creation tool.
- Configure and manage event logging, alerts and reports. Understand and use CSAMC utilities—start / stop service for servers and agent, webmgr utility, backup configurations, COM extract utility and export / import configurations.

Course Content :

Security Fundamentals

- Need for Network Security
- Network Security Policy
- Network Attack Taxonomy

Cisco Security Agent Overview

- Defense in Depth
- Cisco Security Agent Architecture
- Anatomy of an Attack and Response
- Key Features of Cisco Security Agent

Cisco Security Agent Quick Start Installation

- CSAMC System Requirements
- CSA System Requirements
- Installing the CSAMC
- Configuring the CSAMC
- Installing the CSA

Cisco Security Agent Management Center Administration

- Using Cisco Security Agent Management Center

Using Event Logs and Generating Reports

- The Event Log and Event Monitor
- Configuring Event Sets
- Configuring Alerts
- Generating Reports

Configuring Groups and Managing Hosts

- Configuring Groups
- Building and Agent Kit
- Managing Hosts
- Deploying Scheduled Software Updates

Building Policies

- Developing a Security Policy
- Rule Basics
- Policy Components
- Configuring and Managing Policies
- Rules common to Windows and Unix
- Windows-Only Rules
- Unix-only Rules

Defining Application Classes

- About Application Classes
- Configuring Static Application Classes
- Dynamic Application Classes

Working with Variables

- Data Sets
- File Sets
- Network Address & Services Sets
- Registry Sets
- COM Component Sets

Using Cisco Security Agent Profiler

- Basics of Profiler
- Configuring an Analysis Job
- Starting Analysis
- The profiler Policy
- Profiler Reports

Course Prerequisites :

Delegates are required to meet the following prerequisites:

- CCNA or equivalent knowledge

Testing and Certification :

Recommended as preparation for exam(s):

There is currently no exam associated with this course.

- 6 months practical experience of configuring

Cisco IDS Routers

- Competency in using the Windows NT Operating system
- Familiarity with implementing network security policies and the following networking concepts:
 - Perimeter Security System Components
 - Perimeter Router
 - Firewall
 - Bastion Host/Servers and Hosts

Follow on Courses :**Further Information :****HIPS/**

For more information, or to book your course, please call Global Knowledge Denmark
Address: Kirkebjerg Alle 88, 2605 Brøndby
Telephone: +45 44 88 18 00
Email: training@globalknowledge.dk
Web: www.globalknowledge.dk