

Symantec Security Information Manager 4.6

COURSE DESCRIPTION

The Symantec Security Information Manager 4.6 course is designed for security professionals and network security administrators who are tasked with proactively identifying, prioritizing, and resolving critical security incidents to reduce security risk against their key network resources.

This course delivers an overview of the Symantec Security Information Manager 96xx Series appliances and the Information Manager console, including details about the components, architecture, features, and benefits.

Students will learn how to deploy and install the product in an enterprise environment, with emphasis on configuration, rule creation, modification, and management of incidents. This course concentrates on how to use Symantec Security Information Manager to reduce security risk by managing security events emanating from many different Symantec and third-party products.

Delivery Method

Instructor-led

Duration

3 days

Course Objectives

By the end of this course, you should be able to

- Describe the features and benefits of Symantec Security Information Manager.
- Set up the Symantec Security Information Manager appliance.
- Configure Symantec Security Information Manager components for real-world use.
- Create, modify, and manage correlation and event filtering rules.
- Manage incidents, help desk tickets, and reports.

Who Should Attend

This course is for security professionals or IT administrators who are tasked with proactively identifying, prioritizing, and resolving critical security incidents.

Prerequisites

You should have a working knowledge of networking, including typical security components such as firewalls, intrusion detection systems, and antivirus systems. It is beneficial to be familiar with the operation of a help desk in an Information Technology environment.

Hands-On

This course includes practical exercises that enable you to test your new skills and begin to transfer them into your working environment.

COURSE OUTLINE

Introduction to the SSIM Appliances

- Information Security Challenges
- About Symantec Security Information Manager
- Product Specifications
- SSIM Concepts

Deployment Planning and Installation

- SSIM Components and Design Architecture
- Deployment Guidelines in Basic Network Situations
- Installation

Introduction to the SSIM Console

- SSIM Console Installation
- SSIM Console Walkthrough and Features

Configuration

- Basic Configurations of the SSIM System
- Directory Configurations
- Assets

Event System

- Event System Concepts
- Managing Events in the Console
- Event Forwarding

An Incident Life Cycle

- Incident Workflow from Events to Incidents
- Managing Incidents Walkthrough
- Managing Help Desk Tickets

Collectors

- Collectors Basics
- Collectors Configurations
- Examples of Collectors

(Continued)

Rules

- Rules Basics
- Rules Components
- Rules Configurations

Security Monitoring and Reporting

- Security Monitoring Overview
- Reports
- Dashboards

System Maintenance

- Updating SSIM
- Database Maintenance Tasks
- Web Configuration Page Options
- Troubleshooting