

Symantec Enterprise Security Manager 6.5

COURSE DESCRIPTION

The Symantec Enterprise Security Manager 6.5 course trains students to install, configure, and manage Symantec Enterprise Security Manager (ESM) 6.0 through 6.5—using advanced management techniques—across a Windows environment. The course also examines the strong reporting features.

Delivery Method

Instructor-led

Duration

Three days

Course Objectives

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

- Describe the role of Symantec Enterprise Security Manager as a security management tool.
- Select appropriate vulnerability checks that meet a given corporate policy guideline.
- Select the appropriate modules to install so as to comply with a given corporate policy statement.
- Install and configure an ESM agent, Manager, and Console to meet specific network topology requirements.
- Create custom policies and run built-in and custom policies that identify host vulnerabilities determined by a corporate policy statement.
- Plan the installation and configuration of the reporting components.
- Describe the report and query analysis that can be done with Symantec Enterprise Reporting.
- Analyze how and when to change an existing query or report.
- Understand the method of modifying an existing query or report.
- Determine steps necessary to create new queries and reports.
- Implement a Symantec Enterprise Security Architecture (SESA) bridge for a given network and ESM topology.
- Create a Malicious File Watch template and policy.
- Use ESM tools such as the Integrated Command Engine and the Command-Line Interface.

Who Should Attend

This course is for security officers, systems administrators, network engineers, design consultants, and resellers who install, configure, and maintain Symantec Enterprise Security Manager (ESM). Typically, class participants are those charged with the management of corporate policy compliance within their enterprise.

Prerequisites

You should have working knowledge of network security, TCP/IP internetworking, Windows 2000/XP/2003 administration, and a conceptual understanding of corporate policy design and compliance.

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

Policy Management

- Security Overview
- Security Policy Process and Model
- Symantec ESM and Security Management
- Symantec ESM Architecture

Installation and Configuration

- Installation Planning
- Installing Symantec ESM Core Components
- Installing Network Assessment
- Platform-Specific Challenges
- Navigating the Console
- Post-Installation Configuration
- Command Line

Security Policies

- Policy Overview
- Managing Policies
- Managing Modules
- Templates and Word Files
- Running Custom Policies

Reporting

- Reports Overview
- Report Utilities
- Database Conversion
- Generating Reports

Templates

- Creating Templates
- File Watch
- Malicious File Watch
- Template Update Process

Advanced Policy Management

- Symantec ESM Internals
- Automating Policy Runs
- Updating Symantec ESM
- Change Management
- Symantec ESM Policy Tool

Symantec ESM Best Practice Policies

- Best Practice Policies Overview
- Operating System Best Practice Policies
- Application-Based Best Practice Policies
- Industry Standards-Based Best Practice Policies
- Updated Policies and Modules

Integrate Command Engine

- Integrated Command Engine Overview
- Capabilities and Options
- Create an ICE Module

Maintenance

- Data Maintenance
- Configuration and Communication
- Upgrading Symantec ESM
- Troubleshooting
- Database Conversion

Command-Line Interface

- Symantec ESM Command Line Interface Overview
- Using the CLI for Common Tasks
- Running Batch Jobs

Symantec ESM SESA Bridge

- SESA Overview
- SESA Bridge Overview
- Installing the Bridge
- Configuring the Bridge
- Resolving Reporting Problems
- Uninstalling the Bridge

Overview of Enterprise Reporting

- Report Basics
- Report Components

Installing Enterprise Reporting

- Deploying Symantec ESM Reporting
- Confirming Component Installation

Reporting Reports

- Reporting Interface
- Default Reports
- Running Reports

Using Query Studio

- Query Studio Overview
- Metadata Model
- Creating Queries

Using Report Studio

- Planning Reports
- Report Components
- Modifying and Creating Reports

Administering Enterprise Reporting

- Administration Tools
- User Accounts
- Scheduling
- Custom Reports