Symantec Data Center Security: Server Advanced 6.7 Administration

COURSE DESCRIPTION

The Symantec Data Center Security: Server Advanced 6.7 Administration course is an introduction to implementing and managing a Symantec Data Center Security: Server Advanced 6.7 deployment. The architecture and individual components of the SDCS:SA 6.7 solution are detailed and explained. Agent installation and configuration are taught along with deployment and management of SDCS:SA agents and policies across the enterprise. The course also covers SDCS:SA Policy creation/modification in detail.

Delivery Method

Instructor-led training (ILT) and Virtual Academy

Duration

3 days

Course Objectives

By the completion of this course, you will be able to:

- Describe the major components of Symantec Data Center Security: Server Advanced and how they communicate.
- Install the management server, consoles, and agent.
- Define, manage and create assets, policies, events and configurations.
- Understand policy creation and editing in depth.

Who Should Attend

This course is for information technology professionals, security professionals, network, system managers and administrators who are charged with the installation, configuration, and day-to-day management of Symantec Data Center Security: Server Advanced.

Prerequisites

You should have working knowledge of TCP/IP protocols and communications concepts. You must have experience with the Windows and UNIX operating systems in general. A basic understanding of key security disciplines (firewalls, intrusion detection/prevention, policy management, vulnerability assessment, antivirus protection and so on) is required.

Hands-On

This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

COURSE OUTLINE

Lesson 1: Introduction to Security Risks and Risk

- Security Risks
- Security Risk Management
- Managing and Protecting Systems
- Corporate Security Policies and Security Assessments
- Host-Based Computer Security Issues

Lesson 2: SDCS:Server Advanced Overview

- SDCS: Server Advanced Component Overview
- How Does SDCS:SA Work?
- Policy Types and Platforms
- Management Console Overview
- Agent User Interface Overview

Lesson 3: Installation and Deployment

- Planning the Installation
- Deployment Planning
- Server Installation
- Installing the Server Management Console
- Installing a Windows Agent
- Installing a Unix Agent

Lesson 4: Configuring Agents

- Assets Defined
- Agent Architecture
- Viewing Agents and Assets
- Managing Agents
- Managing Agents on Assets by Command Line

Lesson 5: Policy Overview

- Policies Defined
- Prevention Policy Overview
- Detection Policy Overview
- Policy Workspace
- Implementing Policies with SDCS:SA
- SDCS:SA Use Cases

Lesson 6: Windows Prevention Policies

- Windows Prevention Policy Structure Overview
- Editing a Windows Prevention Policy—Basic
- Advanced Policy Settings: Global Policy Options
- Advanced Policy Settings: Sandboxes
- Resource Lists

Lesson 7: UNIX and Legacy Prevention Policies

- Global Policy Options
- Daemon and Service Options
- Interactive Program Options
- Resource Lists
- Sandbox Options
- Profile Lists
- Predefined Policies

Lesson 8: Advanced Prevention

- Profile Applications
- Customize Predefined Prevention Policies
- Custom Sandbox
- Prepare for Policy Deployment
- Create New Policies

Lesson 9: Detection Policies

- Detection Policy Details
- Predefined Detection Policies

Lesson 10: Event Management

- Defining Events
- Viewing Events
- Event Handling Best Practices
- Creating Alerts

Lesson 11: Agent Management and Troubleshooting

- Configurations Defined
- Creating and Editing Configurations
- Analyzing Event Log Files
- Agent Logs
- Diagnostic Policies
- Local Agent Tools

Lesson 12: System Management

- Database Management
- Managing Users and Roles
- Server Management
- Server Logs