Symantec Data Center Security Server Advanced 6.x Planning, Implementation, and Administration R1

Course Code: 000210

Course Description

The Symantec Data Center Security Server Advanced 6.x Planning, Implementation, and Administration R1 course is an introduction to implementing and managing a Data Center Security: Server Advanced deployment. The architecture and individual components of the SDCS:SA 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

Duration

Three Days

Course Objectives

- Describe the major components of 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.

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.

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.

Certification

250-426 Administration of Symantec Data Center Security Server Advanced 6.7

Course Outline

Module 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

Module 2: SDCS: Server Advanced Overview

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

Module 3: Installation and Deployment

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

Module 4: Configuring Agents

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

Module 5: Policy Overview

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

Module 6: Windows Prevention Policies

- Windows Prevention Policy Structure
- Editing Windows Prevention Policy
- Advanced Policy Settings: Global Policy Options
- Advanced Policy Settings: Sandboxes
- Resource Lists
- Custom Sandboxes

Module 7: UNIX and Legacy Prevention Policies

- Unix and Legacy Prevention Policies
- Global Policy Options
- Daemon and Service Options
- Interactive Program Options
- Resource Lists
- Sandbox Options
- Custom Sandboxes
- Trusted Users, Groups, and Applications
- Profile Lists
- Predefined Prevention Policies

Module 8: Advanced Prevention

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

Module 9: Detection Policies

- Detection Policy Details
- Predefined Detection Policies

Module 10: Event Management

- Defining Events
- Viewing Events
- Event Handling and Bulk Logging ▪ Creating Alerts

Module 11: Agent Management and Troubleshooting

- Configurations Defined
- Creating and Editing Configurations
- Bulk Logging Details
- Analyzing Event Log Files and Bulk Loading
- Troubleshooting Agents Using Logs and Configuration Files
- Using Agent Diagnostic Policies
- Using Agent Command-line Interface

Module 12: System Management

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