Symantec Data Center Security: Server Advanced 6.0

COURSE DESCRIPTION

The Symantec Data Center Security: Server Advanced 6.0 course is an introduction to implementing and managing a Symantec Data Center Security: Server Advanced 6.0 deployment. The architecture and individual components of the SDCS:SA 6.0 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)

Duration
Three 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, console 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 tasked with installing, configuring and maintaining 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

Introduction

- Course Overview
- The Classroom Lab Environment

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

SDCS:Server Advanced Overview

- SDCS: Server Advanced Component Overview
- Policy Types and Platforms
- Management Console Overview
- Agent User Interface Overview
  DEMO of Management Console

Installation and Deployment

- Planning the Installation
- Deploying SDCS:SA for High Availability
- Scalability
- Installing the Management Server
- Installing the Management Console
- Installing a Windows Agent
- Installing a UNIX Agent
  LAB
  - Install Manager and Agents

Configuring Assets

- Asset and Agent Overview
- Viewing Agents and Assets
- Managing Agents
- Managing Agents on Assets
  LAB
  - Create Asset Groups
  - Examine Agent Interface

Policy Overview

- Policies Defined
- Prevention Policy Overview
  - Process Sets
  - Resource Access
  - Policy Options
- Detection Policy Overview
  - IDS Capabilities
  - Rules

- Collectors
- Policy Management Workspace
- User Interface on Agent
- Example Use Cases

LAB

Paper Based Scenarios
– what type of security strategy should be used ?

Detailed Prevention Policies

- Policy Editor
- Policy Structure
- Global Policy Options
- Service Options
- Program Options
- Policy Processing Order
- Network Rules
- File Rules
- Registry Rules
- Process Sets
- Predefined Policies

LAB

- Deploy Strict policy
- Examine Functionality

Advanced Prevention

- Profiling Applications
- Customizing Predefined Policies

LAB

- Modify Policy Previously Deployed
- Re-examine Functionality

- Preparing for Policy deployment

LAB

- Best Practice - Covering Basics
- Further Enhance Strict Policy

- Create Custom Process Set

LAB

- Secure an FTP Server
- Troubleshoot Policy/pset Assignment Using CLI

Detection Policies

- Detection Policies Structure
- Collectors
- Rules
- Predefined Detection Policies
- Creating a Detection Policy Using the Template Policy

LAB

- Deploy Baseline Policy
- Create Custom Policy

Event Management

- Events Defined
- Viewing Events
- Reports and Queries Overview
- Creating Queries and Reports
- Creating Alerts

LAB

- View Monitor Types and Search Events
- Create Real Time Monitor
- Create Queries and Reports
- Create Alerts

Agent Management and Troubleshooting

- Configurations Defined
- Creating and Editing Configurations
  - Common Parameters
  - Prevention Settings
  - Detection Settings
- Analyzing Agent Log Files
- Diagnostic Policies
- Local Agent Tool – sisipsconfig

LAB

- Create Custom Configurations
- Implement Bulk Logging
- Disable Prevention on Agent Using CLI
- Use Diagnostic Policy to Gather Logs
- Troubleshoot a Policy

System Management

- Managing Users and Roles
- Server Security
- Viewing and Managing Server Settings
- Viewing and Managing Database Settings
- Viewing and Managing Tomcat Settings

LAB

- Create a New User
- View System Settings

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Specifications and product offerings are subject to change without notice.