Symantec Control Compliance Suite Vulnerability Manager 12.0 Administration

COURSE DESCRIPTION

The Symantec Control Compliance Suite Vulnerability Manager (CCS-VM) 12.0 Administration Training is designed for the IT security professional tasked with installation, administering, monitoring and reporting on CCS-VM 12.x.
Students learn how to install the products components, run network-based vulnerability scans, create Smart Rules, navigate the CCS-VM interface and examine vulnerability findings, and use CCS-VM Analytics and Reporting.

Delivery Method
Instructor-led and Virtual Academy

Duration
Two Days

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

- Demonstrate how to install CCS-VM
- Understand how to do local and enterprise scanning
- Demonstrate how to optimize configurations
- Understand and execute reports
- Understand the CCS-VM Connector installation process

Who Should Attend
This course is for network managers, system administrators, security administrators, systems professionals, and consultants who are charged with the configuration, and day-to-day management of CCS-VM in a variety of network environments, and who are responsible for administration of this product in the enterprise environment.

Prerequisites
There are no prerequisites for this course, but the student should have hands on experience of general networking environments and operating systems. Student should also have working knowledge of Control Compliance Suite for the Connector Lesson.

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: Overview of Vulnerability Management
- Vulnerability Management Overview

Lesson 2: CCS-VM Architecture and Installation
- Review Installation Prerequisites
- Install the CCS-VM Network Scanner (CVNS)
- Install the CCS-VM console
- Configure CVNS to send data to CCS-VM Console
- Configure Analytics and Reporting

Lesson 3: Performing Localized Scanning
- Run discovery and vulnerability scans
- Generate and review remediation reports
- Configure and run other report types

Lesson 4: Performing Enterprise Vulnerability Scanning

- Configure and run standard vulnerability scans from the CCS-VM console
- Review and navigate vulnerability reports
- Interactively navigate vulnerability findings within the console
- Configure and use Saved Credentials
- Configure, run and review other scan types

Lesson 5: Organizing Asset Scans to Business Needs

- Review and create asset-based Smart Rules
- Create vulnerability based Smart Rules
- Review Smart Rule use cases

Lesson 6: Optimizing CCS-VM for your Business Needs

- Integrate with Active Directory
- Configure role-based access controls
- Configure and utilize Address Groups
- Configure Audit Groups
- Explore Connectors
- Configure Directory Queries

Lesson 7: Understanding How to Customize Reports on the Data You Need

- Explore and execute various reports using your scan data
- Understand how to create and analyze various trending reports
- Gain familiarity with the Audit Viewer, Threat Analyzer and Heat Maps
- Understand Pivot Grids

Lesson 8: Layering Your Vulnerability Data with Your Compliance Data

- Install the CCS-VM Connector
- Configure the CCS-VM Connector
- View the CCS-VM data in CCS