Symantec Endpoint Security Complete Administration R1

Course Code:000185

Course Description

The *Symantec Endpoint Security Complete (SESC) Administration R1* course is designed for the network, IT security, and systems administration professional in a Security Operations position tasked with the day-to-day operation of a SESC endpoint security environment. The course focuses on SES Complete cloud-based management using the ICDm management console.

Delivery Method

Instructor-Led

Duration

Five Days

Course Objectives

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

- Describe the benefits of using a multi-layered cloud-based environment for endpoint security.
- Secure endpoints against network, file based, and emerging threats.
- Control endpoint integrity and compliance.
- Respond to security threats using SESC monitoring and reporting.
- Enforce adaptive security compliance.

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

This course assumes that

- students have a basic understanding of advanced computer terminology
- an administrator-level knowledge of Microsoft Windows operating systems
- Reviewed the “Getting Started with SES Complete” eLearning content prior to attending this course.

For further information, please contact your regional education team:

Americas.Education@Broadcom.com | APJ.Education@Broadcom.com | EMEA.Education@Broadcom.com

COURSE OUTLINE

Module 1: Introduction to Endpoint Security Complete

- Introduction to the basic components required to get up and running with the solution including
  - Licensing
  - Architecture
  - Client deployment

Module 2: Configuring SES Complete Security Controls

- The comprehensive set of security controls with SES Complete including
  - Policy use and configuration
  - Versioning
  - Allow and deny lists

Module 3: Responding to Threats with ICDm

- Incident response from the perspective of the ICDm management platform utilizing features such as
  - Dashboards
  - Events
  - Reports

Module 4: Endpoint Detection and Response

- Focus on the Endpoint Detection and Response feature set covering
  - Configuration
  - Administration
  - Incident Investigation
- It is specifically focused on EDR on ICDm only

Module 5: Attack Surface Reduction

- SESC features that work to reduce overall attack surface including product features such as
  - App Control
  - Adaptive Protection

Module 6: Mobile and Modern Device Security

- Focus on additional endpoint device protection areas
  - Mobile
  - Point of sale
- Other specific use devices
  - Device enrolment
  - Specific policies
  - Configuration and administration

Module 7: Threat Defense for Active Directory

- Threat Defense for Active Directory
- Assessment
- Implementation
- Use

Module 8: Working with a Hybrid Environment

- Hybrid deployment architecture
- Differences
- Policy Migration
- Best practices when using a hybrid deployment configuration of SESC

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.