Course Outline

Symantec Endpoint Security Complete Administration R1

Course Summary

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.

Objectives

At the end of this course, students 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.

Topics

- Introduction to Endpoint Security Complete
- Configuring SES Complete Security Controls
- Responding to Threats with ICDm
- Endpoint Detection and Response
- Attack Surface Reduction
- Mobile and Modern Device Security
- Threat Defense for Active Directory
- Working with a Hybrid Environment

Audience

This course is designed for the network, IT security, and systems administration professional in a Security Operations position tasked with the day-to-dayoperation of a SESC endpoint security 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

Duration

Five days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Course Outline

Symantec Endpoint Security Complete Administration R1

Course Outline

I. *Introduction to Endpoint Security Complete*
   A. Introduction to the basic components required to get up and running with the solution including
   B. Licensing
   C. Architecture
   D. Client deployment

II. *Configuring SES Complete Security Controls*
   A. The comprehensive set of security controls with SES Complete including
   B. Policy use and configuration
   C. Versioning
   D. Allow and deny lists

III. *Responding to Threats with ICDm*
   A. Incident response from the perspective of the ICDm anagement platform utilizing features such as
   B. Dashboards
   C. Events
   D. Reports

IV. *Endpoint Detection and Response*
   A. Focus on the Endpoint Detection and Response feature set covering
   B. Configuration
   C. Administration
   D. Incident Investigation
   E. It is specifically focused on EDR on ICDm only

V. *Attack Surface Reduction*
   A. SESC features that work to reduce overall attack surface including product features such as
   B. App Control
   C. Adaptive Protection

VI. *Mobile and Modern Device Security*
   A. Focus on additional endpoint device protection areas
   B. Mobile
   C. Point of sale
   D. Other specific use devices
   E. Device enrolment
   F. Specific policies
   G. Configuration and administration

VII. *Threat Defense for Active Directory*
   A. Threat Defense for Active Directory
   B. Assessment
   C. Implementation
   D. Use

VIII. *Working with a Hybrid Environment*
   A. Hybrid deployment architecture
   B. Differences
   C. Policy Migration
   D. Best practices when using a hybrid deployment configuration of SESC

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically