Endpoint Security
Planning, Implementation, and Administration
R1

COURSE DESCRIPTION

The Symantec Endpoint Security (SES) Planning, Implementation, and Administration 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 SES cloud-based endpoint security environment. This course focuses on the SES enterprise workstation protection capabilities utilizing the new cloud management console.

Delivery Method

Instructor-led and Virtual Academy

Duration

Three days

Course Objectives

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

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

Who Should Attend

The SES Planning, Implementation, and Administration course is intended for IT and system administration professionals who are charged with managing and monitoring Symantec Endpoint Protection endpoints.

Prerequisites

This course assumes that students have a basic understanding of advanced computer terminology, including TCP/IP networking and Internet terms, and an administrator-level knowledge of Microsoft Windows operating systems.

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

Module 1: Control endpoint protection from the cloud

- This module describes the benefits a SES customer achieves using a cloud-based solution for managing endpoint security.

Module 2: Maintain Security on all endpoints

- This module details the tools and methods used to identify unmanaged endpoints and enroll them in the cloud management platform. The module also talks about how to maintain healthy endpoints once enrolled.

Module 3: Protect endpoints against each phase of the attack chain

- This module covers the MITRE ATT&CK model and shows how SES provides security controls for each phase of the attack chain.

Module 4: Respond to security threats

- This module provides tools and methods to investigate and respond to attacks on the endpoint.

Module 5: Provide a recommended response for evolving and emerging threats

- This module discusses the use of machine learning and artificial intelligence (AI) to defend against emerging threats through automated workflows and suggestions.

Module 6: Identify threats and systems involved in a Security Incident

- This module shows how to analyze threats and gain insight on past events to strengthen a security posture.

Module 7: Monitor change management for security controls

- This module describes key features to control and organize policy changes in the environment.