Symantec Endpoint Protection 14.x: Configure and Protect

Course Summary

Description

The Symantec Endpoint Protection 14.x: Configure and Protect course is designed for the network, IT security, and systems administration professionals in a Security Operations position who are tasked with configuring optimum security settings for endpoints protected by Symantec Endpoint Protection 14. This class brings context and examples of attacks and tools used by cybercriminals.

Objectives

By the end of this course, students will be able to:

- Secure endpoints against network and file-based threats
- Control endpoint integrity and compliance
- Enforce adaptive security posture

Topics

- Introduction
- Securing Endpoints against Network-Based Attacks
- Securing Endpoints against File-Based Threats
- Introducing File-Based Threats
- Controlling endpoint integrity and compliance
- Enforcing Adaptive Security Posture

Audience

This course is designed for Network, IT security, and systems administration professionals in a Security Operations position who are tasked with configuring optimum security settings for endpoints protected by Symantec Endpoint Protection 14.

Prerequisites

Before taking this course, you must have a working knowledge of advanced computer terminology, including TCP/IP networking terms, Internet terms, and an administrator-level knowledge of Microsoft Windows operating systems.

Duration

Three days

ProTech "Charting the Course ...
protechtraining.com

... to Your Success!"

Symantec Endpoint Protection 14.x: Configure and Protect

Course Outline

I. Introduction
- A. Course environment
- B. Lab environment

II. Securing Endpoints against Network-Based Attacks
- A. Introducing Network Threats
  1. Describing how Symantec Endpoint Protection protects each layer of the network stack
  2. Discovering the tools and methods used by attackers
  3. Describing the stages of an attack
- B. Protecting against Network Attacks and Enforcing Corporate Policies using the Firewall Policy
  1. Preventing network attacks
  2. Examining Firewall Policy elements
  3. Evaluating built-in rules
  4. Creating custom firewall rules
  5. Enforcing corporate security policy with firewall rules
  6. Blocking network attacks using protection and stealth settings
  7. Configuring advanced firewall feature
- C. Blocking Threats with Intrusion Prevention
  1. Introducing Intrusion Prevention technologies
  2. Configuring the Intrusion Prevention policy
  3. Managing custom signatures
  4. Monitoring Intrusion Prevention events

III. Securing Endpoints against File-Based Threats
- A. Introducing File-Based Threats
  1. Describing threat types
  2. Discovering how attackers disguise their malicious applications
  3. Describing threat vectors
  4. Describing Advanced Persistent Threats and a typical attack scenario
  5. Following security best practices to reduce risks
- B. Preventing Attacks with SEP Layered Security
  1. Virus and Spyware protection needs and solutions
  2. Describing how Symantec Endpoint Protection protects each layer of the network stack
  3. Examining file reputation scoring
  4. Describing how SEP protects against zero-day threats and threats downloaded through files and email
  5. Describing how endpoints are protected with the Intelligent Threat Cloud Service
  6. Describing how the emulator executes a file in a sandbox and the machine learning engine's role and function
- C. Securing Windows Clients
  1. Platform and Virus and Spyware Protection policy overview
  2. Tailoring scans to meet an environment's needs
  3. Ensuring real-time protection for clients
  4. Detecting and remediating risks in downloaded files
  5. Identifying zero-day and unknown threats
  6. Preventing email from downloading malware
  7. Configuring advanced options
  8. Monitoring virus and spyware activity
- D. Securing Mac Clients
  1. Touring the SEP for Mac client
  2. Securing Mac clients
  3. Monitoring Mac clients

Symantec Endpoint Protection 14.x: Configure and Protect

Course Outline (cont'd)

E. Securing Linux Clients
   1. Navigating the Linux client
   2. Tailoring Virus and Spyware settings for Linux clients
   3. Monitoring Linux clients

IV. Controlling endpoint integrity and compliance

A. Providing Granular Control with Host Integrity
   1. Ensuring client compliance with Host Integrity
   2. Configuring Host Integrity
   3. Troubleshooting Host Integrity
   4. Monitoring Host Integrity

B. Controlling Application and File Access
   1. Describing Application Control and concepts
   2. Creating application rulesets to restrict how applications run
   3. Monitoring Application Control events

C. Restricting Device Access for Windows and Mac
   1. Clients
   2. Describing Device Control features and concepts for Windows and Mac clients
   3. Enforcing access to hardware using Device Control
   4. Discovering hardware access policy violations with reports, logs, and notifications

D. Hardening Clients with System Lockdown
   1. What is System Lockdown?
   2. Determining to use System Lockdown in Whitelist or Blacklist mode
   3. Creating whitelists for blacklists
   4. Protecting clients by testing and Implementing
   5. System Lockdown.

V. Enforcing Adaptive Security Posture

A. Customizing Policies based on Location
   1. Creating locations to ensure the appropriate level of security when logging on remotely
   2. Determining the criteria and order of assessment before assigning policies
   3. Assigning policies to locations
   4. Monitoring locations on the SEPM and SEP client

B. Managing Security Exceptions
   1. Creating file and folder exceptions for different scan types
   2. Describing the automatic exclusion created during installation
   3. Managing Windows and Mac exclusions
   4. Monitoring security exceptions