Course Outline

ProTech Professional Technical Services, Inc.

Symantec Endpoint Protection 14.2: Configure and Protect

Course Summary

Description

This 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 14.2. This class brings context and examples of attacks and tools used by cyber criminals.

Objectives

By the end of thise course, you will be able to:

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

Topics

- Introducing Network Threats
- Protecting against Network Attacks and Enforcing corporate Policies using the Firewall Policy
- Blocking Threats with Intrusion Prevention
- Introducing File-Based Threats
- Preventing Attacks with SEP Layered Security
- Securing Windows clients
- Securing Linux Clients
- Securing Mac Clients
- Providing Granular Control with Host Integrity
- Controlling Application and File Access
- Restricting Device Access for Windows and Mac Clients
- Hardening Clients with System Lockdown
- Customizing Policies based on Location
- Managing Security Exceptions

Audience

This course is for Network, IT security, and systems administration professionals in a Security Operations position who are tasked with configuring optimum security settings with endpoints protected by Symantec Endpoint Protection 14.2.

Prerequisites

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

Duration

Three 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 Protection 14.2: Configure and Protect

Course Outline

I. Introducing Network Threats
- A. Describing how Symantec Endpoint Protection protects each layer of the network stack
- B. Discovering the tools and methods used by attackers
- C. Describing the states of an attack

II. Protecting against Network Attacks and Enforcing Corporate Policies using the Firewall Policy
- A. Preventing network attacks
- B. Examining Firewall Policy elements
- C. Creating custom firewall rules
- D. Enforcing corporate security policy with firewall rules
- E. Configuring advanced firewall feature

III. Blocking Threats with Intrusion Prevention
- A. Introducing Intrusion Prevention technologies
- B. Configuring the Memory Exploit Mitigation policy
- C. Configuring the Intrusion Prevention policy
- D. Managing custom signatures
- E. Monitoring Intrusion Prevention events

IV. Introducing File-Based threats
- A. Describing threat types
- B. Desicovering how attackers disguise their malicious applications
- C. Describing threat vectors
- D. Describing Advanced Persistent Threats and a typical attack scenario
- E. Following security best practices to reduce risks

V. Preventing Attacks with SEP Layered Security
- A. Virus and Spyware protection needs and solutions
- B. Examining file reputation scoring
- C. Describing how endpoints are protected with the Intelligent Threat Cloud Service
- D. Describing how the emulator executes a file in a sandbox and the machine learning engine's role and function
- E. Describing download protection with Download Insight
- F. Describing file system and Email Auto-Protect and various Auto-Protect considerations
- G. Describing SONAR real-time protection
- H. Describing the different scan types and scan considerations

VI. Securing Windows Clients
- A. Platform and Virus and Spyware Protection policy overview
- B. Tailoring scans to meet an environment's needs
- C. Ensuring real-time protection for clients
- D. Detecting and remediating risks in downloaded files
- E. Identifying zero-day and unknown threats
- F. Preventing email from downloading malware
- G. Configuring advanced options
- H. Monitoring virus and spyware activity

VII. Securing Linux Clients
- A. Navigating the Linux client
- B. Tailoring Virus and Spyware settings for Linux clients
- C. Monitoring Linux clients
- D. SEP for Linux Logs

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 (cont)

VIII. Securing Mac Clients

A. Touring the SEP for Mac client
B. Securing Mac clients
C. Monitoring Mac clients
D. SEP Logs on Mac clients

IX. Providing Granular Control with Host Integrity

A. Ensuring client compliance with Host Integrity
B. Host Integrity concepts
C. Configuring Host Integrity
D. Troubleshooting Host Integrity
E. Monitoring Host Integrity

X. Controlling Application and File Access

A. Application Control overview
B. Describing Application Control and concepts
C. Creating application r ulesets to restrict how applications run
D. Monitoring Application Control events

XI. Restricting Device Access for Windows and Mac Clients

A. Introducing Device Control
B. Describing Device Control features and concepts for Windows clients
C. Describing Device Control features and concepts for Mac clients
D. Discovering hardware access policy violations with reports, logs, and notifications

XII. Hardening Clients with System Lockdown

A. What is System Lockdown?
B. Creating and managing the file fingerprint list
C. System Lockdown use cases

XIII. Customizing Policies based on Location

A. Creating locations to ensure the appropriate level of security when logging on remotely
B. Assigning policies to locations
C. Monitoring locations on the SEPM and SEP client

XIV. Managing Security Exceptions

A. Describing security exceptions
B. Describing the automatic exclusion created during installation
C. Managing Windows and Mac exclusions Mointoring security exceptions

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