Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

Symantec Endpoint Protection 14.2 Configure and Protect

CODE:	LENGTH:	PRICE:
SYM_00034658	24 Hours (3 days)	£1,785.00

Description

The *Symantec Endpoint Protection 14.2 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 Endpoint Protection 14.2. This class brings context and examples of attacks and tools used by cybercriminals.

Objectives

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

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.

Programme

Module 1: Introducing Network Threats

- Describing how Endpoint Protection protects each layer of the network stack
- Discovering the tools and methods used by attackers
- Describing the stages of an attack

Module 2: Protecting against Network Attacks and Enforcing Corporate Policies using the Firewall Policy

- Preventing network attacks
- Examining Firewall Policy elements
- Creating custom firewall rules
- Enforcing corporate security policy with firewall rules
- Configuring advanced firewall feature

Module 3: Blocking Threats with Intrusion Prevention

- Introducing Intrusion Prevention technologies
- Configuring the Memory Exploit Mitigation policy
- Configuring the Intrusion Prevention policy
- Managing custom signatures
- Monitoring Intrusion Prevention events

Module 4: Introducing File-Based Threats

- Describing threat types
- Discovering how attackers disguise their malicious applications
- Describing threat vectors
- Describing Advanced Persistent Threats and a typical attack scenario
- Following security best practices to reduce risks

Module 5: Preventing Attacks with SEP Layered Security

- Virus and Spyware protection needs and solutions
- Examining file reputation scoring
- Describing how endpoints are protected with the Intelligent Threat Cloud Service
- Describing how the emulator executes a file in a sandbox and the machine learning engine's role and function
- Describing download protection with Download Insight.
- Describing file system and Email Auto-Protect and various Auto-Protect considerations.
- Describing SONAR real-time protection.
- Describing the different scan types and scan considerations.

Module 6: Securing Windows Clients

- Platform and Virus and Spyware Protection policy overview
- Tailoring scans to meet an environment's needs
- Ensuring real-time protection for clients
- Detecting and remediating risks in downloaded files
- Identifying zero-day and unknown threats
- Preventing email from downloading malware
- Configuring advanced options
- Monitoring virus and spyware activity

Module 7: Securing Linux Clients

- Navigating the Linux client
- Tailoring Virus and Spyware settings for Linux clients
- Monitoring Linux clients
- SEP for Linux Logs

Module 8: Securing Mac Clients

- Touring the SEP for Mac client
- Securing Mac clients
- Monitoring Mac clients
- SEP Logs on Mac clients

Module 9: Providing Granular Control with

- Host Integrity
- Ensuring client compliance with Host Integrity
- Host Integrity concepts

- Configuring Host Integrity
- Troubleshooting Host Integrity
- Monitoring Host Integrity

Module 10: Controlling Application and File Access

- Application Control overview
- Describing Application Control and concepts
- Creating application rulesets to restrict how applications run
- Monitoring Application Control events

Module 11: Restricting Device Access for Windows and Mac Clients

Module 12: Hardening Clients with System Lockdown

- What is System Lockdown?
- Creating and managing the file fingerprint list
- System Lockdown use cases

Module 13: Customizing Policies based on Location

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

Module 14: Managing Security Exceptions

- Describing security exceptions
- Describing the automatic exclusion created during installation
- Managing Windows and Mac exclusions
- Monitoring security exceptions
- Introducing Device Control
- Describing Device Control features and concepts for Windows
- Describing Device Control features and concepts for Mac clients
- Discovering hardware access policy violations with reports, logs, and notifications

Test and Certification

250-428 Administration of Symantec Endpoint 14

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.