Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

Symantec Endpoint Protection 14.x: Configure and Protect

CODE:	LENGTH:	PRICE:
SYM_SEP-CP	24 Hours (3 days)	€2,350.00

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 completion of this course, you will be able to:
Secure endpoints against network and filebase threats
Control endpoint integrity and compliance
Enforce adaptive security posture

Audience

Network, IT security, and systems administratio professionals in a Security Operations position who are tasked with configuring optimum security settings for endpoints protected by Symantec Endpoint Protection 14

Prerequisites

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.

Programme

Introduction
Course environment
Lab environment
Securing Endpoints against Network-Based Attacks
Introducing Network Threats
Describing how Symantec Endpoint Protection protects each layer of the network stack
Discovering the tools and methods used by attackers
Describing the stages of an attack

Protecting against Network Attacks and Enforcing Corporate Policies using the Firewall Policy
Preventing network attacks
Examining Firewall Policy elements
Evaluating built-in rules
Creating custom firewall rules
Enforcing corporate security policy with firewall rules
Blocking network attacks using protection and stealth settings
Configuring advanced firewall feature

Blocking Threats with Intrusion Prevention
Introducing Intrusion Prevention technologies

Configuring the Intrusion Prevention policy
Managing custom signatures
Monitoring Intrusion Prevention events

Securing Endpoints against File-Based Threats

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

Preventing Attacks with SEP Layered Security

Virus and Spyware protection needs and solutions
Describing how Symantec Endpoint Protection protects each layer of the network stack
Examining file reputation scoring
Describing how SEP protects against zero-day threats and threats downloaded through files and email
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 engineâ€™s role and function

Securing Windows Clients

Platform and Virus and Spyware Protection policy overview
Tailoring scans to meet an environmentâ€™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

Securing Mac Clients

Touring the SEP for Mac client
Securing Mac clients
Monitoring Mac clients

Securing Linux Clients

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

Controlling endpoint integrity and compliance

Providing Granular Control with Host Integrity

Ensuring client compliance with Host Integrity
Configuring Host Integrity
Troubleshooting Host Integrity
Monitoring Host Integrity

Controlling Application and File Access

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

Restricting Device Access for Windows and Mac Clients

Describing Device Control features and concepts for Windows and Mac clients
Enforcing access to hardware using Device Control
Discovering hardware access policy violations with reports, logs, and notifications

Hardening Clients with System Lockdown

What is System Lockdown?
Determining to use System Lockdown in Whitelist or Blacklist mode
Creating whitelists for blacklists
Protecting clients by testing and Implementing System Lockdown.

Enforcing Adaptive Security Posture

Customizing Policies based on Location

Creating locations to ensure the appropriate level of security when logging on remotely

Determining the criteria and order of assessment before assigning policies
Assigning policies to location
Monitoring locations on the SEPM and SEP client
Managing Security Exceptions
Creating file and folder exceptions for different scan types
Describing the automatic exclusion created during installation
Managing Windows and Mac exclusions
Monitoring security exceptions

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

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