Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns hier

Freistädterstraße 236, A-4040 Linz

Email: education.ecs.at@arrow.com
Phone: +43 1 370 94 40 - 34

Symantec Endpoint Protection 14.x Administration R1

CODE:	LÄNGE:	PREIS:
SYM_000229	40 Hours (5 Tage)	€4,000.00

Description

The Symantec Endpoint Protection 14.x Administration R1 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 the SEPM on-premise management console and with configuring optimum security settings for endpoints protected by Endpoint Protection.

Lernziel

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

- Describe how the Endpoint Protection Manager (SEPM) communicates with clients and make appropriate changes as necessary.
- Design and create Endpoint Protection group structures to meet the needs of your organization.
- Respond to threats using SEPM monitoring and reporting.
- Analyze the content delivery system (LiveUpdate).
- Configure Group Update Providers.
- Create location aware updates.
- Secure endpoints against network and file-based threats
- Control endpoint integrity and compliance
- Enforce an adaptive security posture

Voraussetzungen

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.

Inhalt

Module 1: Managing Console Access and Delegating Authority
- Creating Administrator Accounts
- Managing Administrator Accounts
- Configuring Directory Server Authentication for an Administrator Account

Module 2: Managing Client-to-Server Communication
- Analyzing Client-to-SEPM Communication
- Restoring Communication Between Clients and SEPM
- Verifying Clients are Online with the SEPM

Module 3: Managing Client Architecture and Active Directory Integration
- Describing the Interaction Between Sites, Domains, and Groups
- Managing Groups, Locations, and Shared Policies

- Importing Active Directory Organizational Units (OUs)
- Controlling Access to Client User Interface Settings

Module 4: Managing Clients and Responding to Threats
- Introducing the Clients View
- Monitoring SEP Clients Using the Clients View
- Responding to Incidents Using the Clients View

Module 5: Monitoring the Environment and Responding to Threats
- Monitoring Critical Log Data Using the Summary page
- Identifying New Incidents Using the Logs Page
- Monitoring Actions Sent to Clients Using the Command Status View
- Configuring Notifications

Module 6: Creating Incident and Health Status Reports
- Monitoring Critical Data Using the Reports Page
- Identifying New Incidents Using Quick Reports and Filters
- Configuring Scheduled Reports

Module 7: Introducing Content Updates Using LiveUpdate
- Describing the LiveUpdate Ecosystem
- Configuring LiveUpdate
- Troubleshooting LiveUpdate
- Examining the Need for an Internal LiveUpdate Administrator Server
- Configuring an Internal LiveUpdate Administrator Server

Module 8: Analyzing the SEPM Content Delivery System
- Describing Content Updates
- Configuring LiveUpdate on the SEPM
- Monitoring a LiveUpdate Session
- Managing Content on the SEPM
- Monitoring Content Distribution for Clients

Module 9: Managing Group Update Providers
- Introducing Group Update Providers
- Adding Group Update Providers
- Adding Multiple Group Update Providers and Configuring Explicit Group Update Providers
- Identifying and Monitoring Group Update Providers

Module 10: Manually Downloading Certified and Rapid Release Definitions
- Downloading Certified SEPM Definitions from Symantec Security Response
- Downloading Certified Windows Client Definitions from Symantec Security Response
- Downloading Rapid Release Definitions from Symantec Security Response
- Downloading Certified and Rapid Release
- Definitions from Symantec Security Response for Mac and Linux Clients
- Locating Statically Named Definitions

Module 11: Protecting Against Network Attacks and Enforcing Corporate Policies using the Firewall Policy
- Preventing Network Attacks
- Examining Firewall Policy Elements
- Creating Custom Firewall Rules
- Enforcing a Corporate Security Policy with Firewall Rules
- Configuring Advanced Firewall Features

Module 12: Blocking Network Threats with Intrusion Prevention
- Introducing Intrusion Prevention Technologies
- Configuring the Intrusion Prevention Policy
- Managing Custom Signatures
- Monitoring Intrusion Prevention Events

Module 13: Protecting Against Memory-Based Attacks
- Memory Exploit Mitigation
- Configuring the Memory Exploit Mitigation Policy
- Preventing Defense Evasion

Module 14: Preventing Attacks with SEP Layered Security
- Virus and Spyware Protection
- File Reputation
- Insight Lookup
- Emulator and Machine Learning Engine
- Download Insight
- Auto-Protect Scans
- SONAR
- Administrator-defined Scans

Module 15: 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 16: Securing Linux Clients
- Navigating the Linux Client
- Configuring Virus and Spyware Settings for Linux Clients
- Monitoring Linux Clients
- SEP for Linux Logs

Module 17: Securing Mac Clients
- Touring SEP for Mac Client
- Securing Mac Clients
- Monitoring Mac Clients
- SEP Logs on Mac Clients

Module 18: Providing Granular Control with Host Integrity
- Introducing Host Integrity
- Host Integrity Concepts
- Configuring Host Integrity
- Troubleshooting Host Integrity
- Monitoring Host Integrity

Module 19: Controlling Application and File Access
- Application Control Overview
- Application Control Concepts
- Configuring Application Control
- Monitor Application Control Events

Module 20: Restricting Device Access for Windows and Mac Clients
- Introducing Device Control
- Windows Device Control Concepts
- Mac Device Control Concepts
- Configuring Device Control
- Monitoring Device Control Events

Module 21: Hardening Clients with System Lockdown
- Describing System Lockdown
- Creating and Managing the File Fingerprint List
- System Lockdown use cases

Module 22: Customizing Protection Based on User Location
- Creating Locations
- Adding Policies to Locations
- Monitoring Location Awareness

Module 23: Managing Security Exceptions
- Describing Security Exceptions
- Describing Automatic Exclusions
- Managing Exceptions
- Monitoring Security Exceptions

Weiterführende Kurse

Students interested in Administration of Symantec endpoints utilizing the cloud management interface available as part of Symantec Endpoint Security Complete should take the following course:
- Symantec Endpoint Security Complete Administration R1

Test und Zertifizierung

250-428: Administration of Symantec Endpoint Protection 14

Kurstermine

Auf Anfrage. Bitte kontaktieren Sie uns

Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.