Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss her

Postboks 6562 ETTERSTAD, 0606 Oslo, Norge

Email: kurs.ecs.no@arrow.com
Phone: +47 22 02 81 00

Symantec Endpoint Protection 14.x Administration R2

CODE:	LENGTH:	PRICE:
SYM_000286	32 Hours (4 days)	kr42,000.00

Description

The Symantec Endpoint Protection 14.x Administration R2 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.
Hands-On
This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

Objectives

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
▪ Enforce an adaptive security posture

Prerequisites

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.

Programme

Module 1: Introduction ▪ The Evolving Threat Landscape ▪ Challenges of Endpoint Detection and Response in the environment ▪ How Symantec Endpoint Detection and Response meets objectives ▪ Components of Symantec Endpoint Detection and ▪ Response ▪ Shared Technologies ▪ Symantec Endpoint Detection and Response AddOns and Integrations
Module 2: Architecture and Sizing ▪ Architecture and Sizing Overview ▪ Architecture ▪ Sizing **Module 3: Implementation** ▪ System Requirements ▪ Installing and Bootstrapping ▪ Setup Wizard ▪ Management Console Overview ▪ Managing Certificates ▪ User Accounts and Roles ▪ Symantec Endpoint Protection Integration **Module 4: Detecting Threats** ▪ Understanding Suspicious & Malicious Activity ▪ Prerequisite configuration or considerations ▪ Identifying evidence of suspicious/malicious activity with Symantec EDR **Module 5: Investigating Threats** ▪ General Stages of an Advanced Attack ▪ Understanding Indicators of Compromise ▪ Searching for Indicators of Compromise ▪ Analyzing Endpoint Activity Recorder Data ▪ Additional Investigation Tools **Module 6: Responding to Threats** ▪ Cybersecurity Framework ▪ Isolating Threats in The Environment ▪ Blocking Threats in The Environment ▪ Removing Threats in The Environment ▪ Tuning the Environment **Module 7: Reporting on Threats** ▪ Recovery Overview ▪ Notifications and Reporting ▪ Collecting forensic data for further investigation of security incidents ▪ Using Symantec EDR to create a Post Incident Report **Module 8: Managing System Settings** ▪ Managing Certificates ▪ Importing and Exporting Incident Rules State ▪ Event and Incident Forwarding ▪ Splunk Integration

Follow on courses

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 R1.4

Test and Certification

50-580 Endpoint Security Complete - R2 Technical Specialist

Session Dates

Ved forespørsel. Vennligst kontakt oss

Tilleggsinformasjon

Denne treningen er også tilgjengelig som trening på stedet. Kontakt oss for å finne ut mer.