



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com

Phone: +31 20 582 6109



Symantec Endpoint Detection and Response 4.x Planning, Implementation and Administration R1.1

CODE:	LENGTH:	PRICE:
SYM_000265	24 Hours (3 days)	€2,250.00

Description

The Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration course is designed for the IT security and systems administration professional in a Security Operations role. This course covers how to investigate, remediate, and recover from a security incident using Symantec Endpoint Detection and Response, as well as the prerequisite sizing and architecture configurations for implementing Symantec Endpoint Detection and Response On-Prem.

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:

- Plan and implement a Symantec Endpoint Detection and Response deployment
- Configure SEDR to perform endpoint detection and response
- Identify evidence of suspicious and malicious activity
- Search for indicators of compromise
- Block, isolate, and remove threats in the environment
- Collect forensic information
- Manage System Settings

Prerequisites

This course assumes that students are familiar with Symantec Endpoint Detection & Response and Symantec Endpoint Protection.

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
Module 5: Investigating Threats
▪ Identifying evidence of suspicious/malicious activity with Symantec EDR
Module 6: Responding to 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 7: Reporting on Threats ▪ Recovery Overview
▪ Cybersecurity Framework ▪ Isolating Threats in The Environment ▪ Blocking Threats in The Environment
▪ Removing Threats in The Environment ▪ Tuning the Environment
Module 8: Managing System Settings ▪ Managing Certificates
▪ Notifications and Reporting ▪ Collecting forensic data for further investigation of security incidents
▪ Using Symantec EDR to create a Post Incident Report
▪ Importing and Exporting Incident Rules State ▪ Event and Incident Forwarding ▪ Splunk Integration

Follow on courses

Students interested in Administration of Symantec Endpoint Detection and Response utilizing the cloud management interface available as part of Symantec Endpoint Security Complete should take the following course:

- Symantec Endpoint Security Complete Administration R1.x

Session Dates

On request. Please [contact us](#)

Additional Information

[This training is also available as onsite training. Please contact us to find out more.](#)