



## 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](mailto:educationteam.ecs.uk@arrow.com)  
Phone: 0870 251 1000



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

CODE:	LENGTH:	PRICE:
SYM_000200	24 Hours (3 days)	£2,025.00

## 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.

## 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

## 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
- 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

### **Session Dates**

On request. Please [Contact Us](#)

### **Additional Information**

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