



**Enterprise Computing Solutions - Education Services**

## **TRAINING OFFERING**

---

**Sie erreichen uns hier**

Freistädterstraße 236, A-4040 Linz

Email: [education.ecs.at@arrow.com](mailto:education.ecs.at@arrow.com)

Phone: +43 1 370 94 40 - 34

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

| CODE:      | LÄNGE:            | PREIS:    |
|------------|-------------------|-----------|
| SYM_000200 | 24 Hours (3 Tage) | €2,400.00 |

## 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.

## Lernziel

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

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

## Voraussetzungen

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

## Inhalt

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

|   |  |  |
|---|--|--|
|   |  | System Requirements                      |
|   |  | Installing and Bootstrapping             |
|   |  | Setup Wizard                             |
|   |  | Management Console Overview              |
| Architecture and Sizing Overview          |  | Managing Certificates                    |
| Architecture                              |  | User Accounts and Roles                  |
| Sizing                                    | Module 3: Implementation   | Symantec Endpoint Protection Integration |
|   | Understanding Suspicious & Malicious Activity                            |  |
|   | Prerequisite configuration or considerations                             |  |
|   | Identifying evidence of suspicious/malicious activity                    |  |
| Module 4: Detecting Threats               | with Symantec EDR  | Module 5: Investigating Threats          |
| General Stages of an Advanced Attack      |  | Cybersecurity Framework                  |
| Understanding Indicators of Compromise    |  | Isolating Threats in The Environment     |
| Searching for Indicators of Compromise    |  | Blocking Threats in The Environment      |
| Analyzing Endpoint Activity Recorder Data |  | Removing Threats in The Environment      |
| Additional Investigation Tools            | Module 6: Responding to Threats  | Tuning the Environment                   |
|   | Recovery Overview  |  |
|   | Notifications and Reporting  |  |
|   | Collecting forensic data for further investigation of security incidents |  |
|   | Using Symantec EDR to create a Post Incident Report                      |  |
| Module 7: Reporting on Threats            |  |  |

## 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.](#)