Enterprise Computing Solutions - Education Services

# TRAINING OFFERING

**Skontaktuj się z nami**

.

Email: szkolenia.ecs.pl@arrow.com
Phone: 12 616 43 00

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

| Kod: | Czas trwania: | Cena netto: |
|---|---|---|
| SYM_000200 | 24 Hours (3 days) | Request Price |

## 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.

## Cel szkolenia

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

## Wymagania wstępne

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

## Program szkolenia

**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 activitywith 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<br>Notifications and Reporting<br>Collecting forensic data for further investigation of security incidents<br>Using Symantec EDR to create a Post Incident Report |

## Terminy

Na żądanie. Prosimy o kontakt

## Dodatkowe informacje

Jeśli interesują Cię inne szkolenia tego producenta - skontaktuj się z nami.