



Enterprise Computing Solutions - Education Services

## TRAINING OFFERING

---

**Sie erreichen uns unter**

Arrow ECS GmbH, Elsenheimerstraße 1, 80687 München

Email: [training.ecs.de@arrow.com](mailto:training.ecs.de@arrow.com)

Phone: +49 (0)89 930 99 168

# Symantec Endpoint Security Complete Administration R1.3

<b>CODE:</b>	<b>LÄNGE:</b>	<b>PREIS:</b>
SYM_000248	40 Hours (5 Tage)	€4,000.00

## Description

The Symantec Endpoint Security Complete Administration R1.3 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 a SESC endpoint security environment. The course focuses on SES Complete cloud-based management using the ICDm management console.

## Lernziel

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

- Describe the benefits of using a multi-layered cloudbased environment for endpoint security.
- Secure endpoints against network, file based, and emerging threats.
- Control endpoint integrity and compliance.
- Respond to security threats using SESC monitoring and reporting.
- Enforce adaptive security compliance.
- Protect Active Directory
- Use SES

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

## Voraussetzungen

This course assumes that students have a basic understanding of advanced computer terminology, an administrator-level knowledge of Microsoft Windows operating systems, and have viewed the “Symantec Endpoint Security Complete – Basic Administration” eLearning content prior to attending this course.

## Inhalt

Module 1: Introduction to Endpoint Security Complete

- Introduction
- SES Complete Architecture
- SES Complete Cloud-Based Management
- SES Complete in a Hybrid Environment
- SES Complete Device Group Management
- SES Complete Client Deployment
- SES Device Management

Module 2: Configuring SES Complete Security Controls

- Policy Overview
- Threat Overview and the MITRE ATT&CK Framework
- Preventing Initial Access
- Preventing Execution
- Preventing Persistence
- Preventing Privilege Escalation
- Preventing Defense Evasion
- Preventing Discovery
- Blocking Command & Control
- Blocking Exfiltration
- Blocking the Impact Phase
- Managing Content Updates
- Policy Versioning and History

#### Module 3: Responding to Threats with ICDm

- The ICDm Home Page
- Searching SES Data
- Using SES Reports
- Configuring Alerts
- Managing Mitigation
- Acting on Events

#### Module 4: Endpoint Detection and Response

- Introduction to EDR
- Detecting Threats
- Investigating Threats
- Responding to Threats

#### Module 5: Attack Surface Reduction

- Reduce the Attack Surface with Adaptive Protection
- Reduce the Attack Surface with Application Control
- Reduce the Attack Surface with Custom Application Behavior
- Reduce the Attack Surface with Host Integrity

#### Module 6: Mobile and Modern Device Security

- Definition of Modern and Mobile Devices
- Modern and Mobile Threats
- Introducing Network Integrity
- Network Integrity Policy Configuration
- Network Integrity for Windows 10 Modern Devices
- Network Integrity for Mobile Devices
- Exploring Generated Alerts

#### Module 7: Threat Defense for Active Directory

- Active Directory Security Challenges
- Introducing Threat Defense for Active Directory
- TDAD Configuration
- Threat Scenarios and Remediation

#### Module 8: Working with a Hybrid Environment

- Reasons for Moving to the Cloud
- SES / SEP Hybrid Architecture
- Moving to Hybrid Managed
- Policies and Device Management from the Cloud
- Migrating to the Cloud

### **Test und Zertifizierung**

250-580: Symantec Endpoint Security Complete Administration R2

### **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.](#)