



**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

CODE:	LÄNGE:	PREIS:
SYM_000218	40 Hours (5 Tage)	€4,000.00

## Description

The Symantec Endpoint Security Complete Administration R1.2 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 cloud-based 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 SESC in a Hybrid Environment / Migrate to the Cloud

## 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 - Getting Started" 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  
Managing Devices and Policies with ICDm SES Complete Client Deployment  
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  
Managing Mitigation Acting on Events Module 4: Endpoint Detection and Response  
Enabling Endpoint Detection and Response Understanding Suspicious & Malicious Activity Investigating Threats  
Capturing Endpoint Data LiveShell Retrieving and Submitting Files for Analysis Quarantining Devices  
Blocking and Quarantining Files 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 Configuration  
Threat Scenarios and Remediation Module 8: Working with a Hybrid Environment  
Reasons for Choosing a Hybrid Environment SES Hybrid Architecture SEPM Enrollment Process in ICDm  
Policies and Device Management from the Cloud Migrating to the Cloud

## Test und Zertifizierung

250-561 ENU: Symantec Endpoint Security Complete Administration R1

## **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.