BROADCOM®
SOFTWARE

Exam 250-561: Endpoint Security Complete R1 Technical Specialist

Exam Study Guide v. 1.2

Exam Description

Candidates can validate technical knowledge and competency by becoming a Broadcom Certified Specialist (BTS) based on your specific area of Symantec technology expertise. To achieve this level of certification, candidates must pass this proctored BTS exam that is based on a combination of Symantec training material, commonly referenced product documentation, and real-world job scenarios.

This exam targets IT Professionals using the Symantec Endpoint Security Complete product in a Security Operations role. This certification exam tests the candidate's knowledge on how Symantec Endpoint Security Complete provides comprehensive endpoint security with multilayered defense and single agent/single console management with AI-guided policy updates.

Recommended Experience

It is recommended that the candidate has at least 3-6 months experience working with Symantec Endpoint Security Complete in a production or lab environment.

Study References

Instructor Led https://www.broadcom.com/support/symantec/services/education

Symantec Endpoint Security Complete Administration R1.2

(5 Day Classroom/Virtual)

- Introduction to Symantec Endpoint Security Complete
- Configuring SES Complete Security Controls
- Responding to Threats with ICDm
- Endpoint Detection and Response
- Attack Surface Reduction
- Mobile and Modern device security
- Threat Defense for Active Directory
- Working with a Hybrid Environment

Self-Paced https://brocade.csod.com/ui/lms-learning-details/app/video/e595bd09-

Symantec Endpoint Security Complete – Getting Started*

- Understanding Suspicious and Malicious activity using the MITRE ATT&CK Framework
- Integrated Cyber Defense Manager console tour
- Default Policies
- Role-based Access

* This self-paced course is a prerequisite to the instructor led version of the Symantec Endpoint Security Complete Administration course and is recommended study by the exam candidate as some of the questions were derived from this courseware.

Documentation

https://support.broadcom.com/security

- Symantec Endpoint Security Documentation https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud.html

Symantec Websites

- Symantec Endpoint Security Product Page
- Symantec Endpoint Security Cloud Help

Exam Objectives

The following tables list the Symantec SCS Certification exam objectives for the exam and how these objectives align to the corresponding Symantec course topics and their associated lab exercises as well as the referenced product documentation.

Candidates are encouraged to complete applicable lab exercises as part of their preparation for the exam.

For more information on the Broadcom Certification Program, visit https://www.broadcom.com/support/education/software/certification/all-exams

Introduction to Symantec Endpoint Security Complete

Exam Objectives	Applicable Course Content
Understand SES Complete Architecture.	**Symantec Endpoint Security Complete Administration R1.2** • Module: Introduction to Symantec Endpoint Security Complete
Describe the benefits of SES Complete Cloud-based management.	
Describe the various methods for enrolling SES endpoint agents.	

Configuring SES Complete Security Controls

Exam Objectives	Applicable Course Content
Understand how policies are used to protect endpoint devices.	**Symantec Endpoint Security Complete Administration R1.2**
Understand the Threat landscape and the MITRE ATT&CK Framework.	

Exam Objectives	Applicable Course Content
Describe how SES Complete can be used in preventing an attacker from accessing the environment.	• Module: Configuring SES Complete Security Controls
Describe how SES Complete prevents threat execution.	
Describe how SES Complete prevents threat persistence.	
Describe how SES Complete prevents privilege escalation.	
Describe how SES Complete prevents defense evasion.	
Describe how SES Complete prevents device discovery.	
Describe how SES Complete blocks Command & Control communication.	
Describe how SES Complete works to block data exfiltration.	
Describe SES Complete content update types and how they are distributed to endpoints.	
Describe SES Complete policy versioning and its use.	

Responding to Threats with ICDm

Exam Objectives	Applicable Course Content
Describe the ICDm security control dashboards and their use.	**Symantec Endpoint Security Complete Administration R1.2** • Module: Responding to Threats with ICDm
Understand how ICDm is used to identify threats in the environment.	
Describe the incident lifecycle and steps required to identify a threat.	
Describe the ways in which ICDm can be used to remediate threats.	
Describe how to use ICDm to configure administrative reports.	

Endpoint Detection and Response

Exam Objectives	Applicable Course Content
Describe the requirements to enable Endpoint Detection and Response in the ICDm management console.	**Symantec Endpoint Security Complete Administration R1.2** • Module: Endpoint Detection and Response
Describe how EDR assists in identifying suspicious and malicious activity.	
Describe how EDR aids in investigating potential threats.	
Describe the configuration and use of the Endpoint Activity Recorder.	
Understand the use of LiveShell for incident response.	
Describe how to use EDR to retrieve and submit files for analysis.	
Describe how EDR can be used to quarantine endpoint devices.	
Describe how EDR can be used to block and quarantine suspicious files.	

Attack Surface Reduction

Exam Objectives	Applicable Course Content
Describe Behavior Prevalence the use of the SES Complete Behavioral Insights and Policy Tuning Widget.	**Symantec Endpoint Security Complete Administration R1.2** • Module: Attack Surface Reduction
Describe how the SES Complete Heatmap can be used to prevent unwanted application behaviors.	
Describe SES Complete policy adaptations and behavioral tuning.	
Describe the SES Complete policy and device groups and how they are used.	
Describe the requirements to enable App Control in the ICDm management console.	

Exam Objectives	Applicable Course Content
Describe the process of monitoring drift to further tune App Control policies.	

Mobile and Modern Device Security

Exam Objectives	Applicable Course Content
Describe the requirements to enable Network Integrity in the ICDm management console.	**Symantec Endpoint Security Complete Administration R1.2** • Module: Mobile and Modern Device Security
Describe Network Integrity Policy Configuration and it's use.	
Describe how Network Integrity works to remediate threats.	
Describe how SES Complete's mobile technologies protection against malicious apps.	
Describe how SES Complete's mobile technologies protection against malicious networks.	

Threat Defense for Active Directory

Exam Objectives	Applicable Course Content
Describe the requirements for Threat Defense for Active Directory Installation and Configuration.	**Symantec Endpoint Security Complete Administration R1.2** • Module: Threat Defense for Active Directory
Describe the Threat Defense Active Directory policy and it's use.	
Describe how Threat Defense for Active Directory is used to identify threats.	
Describe how Threat Defense for Active Directory protects against misconfigurations and vulnerabilites in an environment.	

Working with a Hybrid Environment

Exam Objectives	Applicable Course Content
Describe the process for policy migration from SEPM to the ICDm console.	**Symantec Endpoint Security Complete Administration R1.2** • Module: Working with a Hybrid Environment
Describe policy precedence in a hybrid configuration.	
Understand how Sites and Replication are impacted in a Hybrid environment.	
Describe the requirements and process for SEPM integration with the ICDm platform used in a SES Complete Hybrid architecture.	

Sample Exam Questions

Review the following sample questions prior to taking an exam to gain a better understanding of the types of questions asked.

1. **Which Windows component needs to be tuned using a registry key change to enable SES remote push?**

   A. Windows Firewall
   B. User Access Control
   C. Group Policies
   D. Local Policies

2. **Which MITRE ATT&CK framework step includes destroying data and rendering an endpoint inoperable?**

   A. Rampage
   B. Kill Chain
   C. Exfiltration
   D. Impact

3. **Which SES Policy controls port scan detection?**

   A. IPS
   B. Firewall
   C. Device Control
   D. Exploit Mitigation

4. **Which type of endpoint connectivity requires low bandwidth mode for LiveUpdate?**

   A. 4G
   B. Wifi
   C. VPN
   D. Satellite

5. **Using the ICDm console, a SES administrator issues a device command. When will the command be executed on the endpoint?**

   A. At the next heartbeat
   B. When the user is idle
   C. Immediately
   D. When the endpoint reboots

6. **Which antimalware engine detects attacks coded in JavaScript?**

   A. Emulator
   B. Sapient
   C. Core3
   D. SONAR

7. **When an endpoint is compromised and quarantined, which online resource is available to remediate the infection?**

   A. Windows Update
   B. LiveUpdate
   C. Security Response
   D. SymDiag

8. **Which auto management task is created when a malicious file generates malicious outbound traffic?**

   A. Blacklist file
   B. Whitelist file
   C. Enable IPS audit
   D. Quarantine file

9. **Which report format is supported in Symantec Endpoint Security?**

   A. Text
   B. MHTML
   C. XML
   D. PDF

10. **What is the recommended first step for an administrator to perform when beginning a discover and deploy campaign?**

    A. Configure the registry
    B. Configure the SES policies and Groups
    C. Disable the Windows firewall
    D. Install the first SES agent in the subnet

Sample Exam Answers:

1.	B
2.	D
3.	B
4.	D
5.	C
6.	A
7.	B
8.	A
9.	D
10.	D