Symantec™
A Division of Broadcom

250-550: Symantec Endpoint Security Planning, Implementation, and Administration R1

Exam Study Guide v. 1.0

Exam Description

Candidates can validate technical knowledge and competency by becoming a Symantec Certified Specialist (SCS) based on your specific area of Symantec technology expertise. To achieve this level of certification, candidates must pass this proctored SCS 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 product in a Security Operations role. This certification exam tests the candidate's knowledge on how Symantec Endpoint Security provides cloud-delivered 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 in a production or lab environment.

Study References

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

Symantec Endpoint Security Planning, Implementation, and Administration R1 (3 Day Classroom/Virtual)

- Control endpoint protection from the cloud
- Maintain Security on all endpoints
- Protect endpoints against each phase of the attack chain
- Respond to security threats
- Provide a recommended response for evolving and emerging threats
- Identify threats and systems involved in a Security Incident
- Monitor change management for security controls

Self-Paced https://brocade.csod.com/ui/lms-learning-details/app/video/4e21bbfa-

SES: Basic Planning, Implementation and Administration*

- Symantec Endpoint Security Environment
- SES Policy Management
- Incident Response

* This self-paced course is a prerequisite to the instructor led version of the Symantec Endpoint Security Planning, Implementation and 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 Symantec Certification Program, visit https://www.broadcom.com/support/symantec/services/education/certification.

Control endpoint protection from the cloud

Exam Objectives	Applicable Course Content
Describe the benefits of adopting a cloud-based endpoint security solution.	**Symantec Endpoint Security Planning, Implementation, and Administration** • Module: Control endpoint protection from the cloud
Describe the account access and authentication methods available in SES.	
Describe the network requirements needed for connecting endpoints to the cloud management platform.	
Describe the client communication model and how to verify client connectivity.	
Describe the requirements and process for SEPM integration with the Cyber Defense Manager platform used in SES.	
Describe how content updates can be modified for various network configurations.	

Exam Objectives	Applicable Course Content
Describe LiveUpdate functionality and configuration options.	

Maintain Security on all endpoints

Exam Objectives	Applicable Course Content
Describe the various methods SES uses to identify unmanaged endpoints.	**Symantec Endpoint Security Planning, Implementation, and Administration** • Module: Maintain Security on all endpoints
Describe the methods for enrolling SES endpoint agents.	
Describe the SES system requirements and supported operating systems.	
Describe how to utilize console data to identify and endpoints security status.	

Protect endpoints against each phase of the attack chain

Exam Objectives	Applicable Course Content
Describe the various types of threats that threaten endpoint devices.	**Symantec Endpoint Security Planning, Implementation, and Administration** • Module: Protect endpoints against each phase of the attack chain
Describe how SES can be used to protect endpoints against zero-day attacks.	
Describe how to use SES to block unauthorized applications from running.	
Describe device control and how SES can be used to control device access.	
Describe IPS and how it is used in detecting and preventing unwanted network traffic.	
Describe the signature-based protection model, it's uses, advantages, and disadvantages.	
Describe various Memory Exploit Mitigation techniques and how SES protects against them.	

Exam Objectives	Applicable Course Content
Describe the benefits of controlling network traffic on the endpoint and how SES uses firewall rules to fulfill these requirements.	
Describe SES content update types and how they are distributed to endpoints.	

Respond to security threats

Exam Objectives	Applicable Course Content
Describe incident response stages for threat detections in an enterprise.	**Symantec Endpoint Security Planning, Implementation, and Administration** • Module: Respond to security threats
Describe how the Cyber Defense Manager is used to identify threats in an environment.	
Describe the various types of device commands that can be sent to an endpoint agent and their use.	
Describe the steps that can be taken to remediate threats locally on an endpoint.	
Describe false positives, their impact, and how SES can be used to mitigate them.	
Describe the tools and techniques included in SES to adapt security policies based upon threat detections.	
Describe threat artifacts and the best practices to follow after a major endpoint security event.	

Provide a recommended response for evolving and emerging threats

Exam Objectives	Applicable Course Content
Describe emerging threats and their impact in the current threat landscape.	**Symantec Endpoint Security Planning, Implementation, and Administration**
Describe Advanced Machine Learning and how SES employs this protection to protect endpoints against unknown threats.	

Exam Objectives	Applicable Course Content
Describe the Cyber Defense Manager detection workflow, it's operation and use.	• Module: Provide a recommended response for evolving and emerging threats

Identify threats and systems involved in a Security Incident

Exam Objectives	Applicable Course Content
Describe how to use the SES management console to configure administrative notifications.	**Symantec Endpoint Security Planning, Implementation, and Administration** • Module: Identify threats and systems involved in a Security Incident
Describe how to use the SES management console to configure administrative reports.	
Describe the Cyber Defense Manager security control dashboards and their use.	
Describe the advanced search and filtering capabilities of the Cyber Defense Manager.	
Describe how Virus Total Lookup can be used to gather detailed threat information SES.	

Monitor change management for security controls

Exam Objectives	Applicable Course Content
Describe how an administrator can use SES policy versioning to help minimize unwanted system changes.	**Symantec Endpoint Security Planning, Implementation, and Administration** • Module: Monitor change management for security controls
Describe the SES policy and device groups and how they are used.	

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