BROADCOM®
SOFTWARE

250-571
Endpoint Detection and Response 4.x Technical Specialist

Exam Study Guide v. 1.0

Exam Description

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

This exam targets IT Professionals using the Symantec Endpoint Detection and Response (SEDR) product in a Security Operations role. This certification exam tests the candidate's knowledge on how to detect, investigate, remediate, and recover from an incident using Symantec Endpoint Detection and Response in their organizations.

Recommended Experience

It is recommended that the candidate has at least 3-6 months experience with Symantec EDR solutions with at least the ability to complete the following:

- Operational knowledge of Symantec Endpoint Detection and Response.
- Familiarity with Cybersecurity and Threat Protection concepts
- Familiarity with Symantec Endpoint Protection products.
- Perform initial Symantec EDR setup steps.
- Configure Symantec EDR to share data with third-party applications.
- Create Deny and Allow list policies.
- Able to investigate threats in the environment.
- Able to act on threats in the environment.
- Able to recover after threats have been contained.
- Able to report on threats in the environment.

Study References

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

Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1 (3 Day Classroom/Virtual)

- Introduction
- Architecture and Sizing
- Implementation
- Detecting Threats
- Investigating Threats
- Responding to Threats
- Reporting on Threats

Documentation

https://support.broadcom.com/security

- Symantec Endpoint Detection and Response Documentation
  https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-6.html

Symantec Websites

- Symantec Endpoint Security Product Page

Exam Objectives

The following tables list the Broadcom Technical Specialist exam objectives for the exam and how these objectives align to the corresponding Broadcom 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 Detection and Response

Exam Objectives	Applicable Course Content
Describe the challenges faced when threat hunting in the environment and their resultant business objectives.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** • Module: Introduction
Describe how Symantec EDR meets business objectives.	

Architecting and Sizing

Exam Objectives	Applicable Course Content
Given a scenario, demonstrate knowledge of SEDR Architecture and Sizing considerations.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** • Module: Architecture and Sizing
Describe the capabilities and functions of Symantec EDR.	

Implementation

Exam Objectives	Applicable Course Content
Given a scenario, define the discrete components found within SEDR.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** • Module: Implementation
Describe installation prerequisites, minimum solution configuration and installation procedures required to implement SEDR.	
Given a scenario, demonstrate knowledge of the methods used to integrate SEDR with other solutions and services.	

Detecting Threats

Exam Objectives	Applicable Course Content
Describe how SEDR increases the visibility of suspicious and malicious activity in a typical environment.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** • Module: Detecting Threats
Describe installation prerequisites, minimum solution configuration and installation procedures required to identify threats.	

Investigating Threats

Exam Objectives	Applicable Course Content
Describe the various types of suspicious and malicious activity found in a typical environment.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** • Module: Investigating Threats
Describe the methods used to identify evidence of suspicious and malicious activity.	
Describe the various types of Indicators of Compromise (IoC) found in a typical environment.	
Describe the methods used to search for IOCs using SEDR.	

Responding to Threats

Exam Objectives	Applicable Course Content
Describe the benefits of reducing security risks by responding to threats in the environment.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** • Module: Responding to Threats
Describe the methods SEDR uses to respond to threats in a typical environment.	
Describe installation prerequisites, minimum solution configuration and installation procedures required to isolate threats.	
Describe the various methods used to block threats in a typical environment.	
Describe installation prerequisites, minimum solution configuration and installation procedures required to remove threats.	
Given a scenario, determine the appropriate method for removing threats to reduce security risk.	

Reporting on Threats

Exam Objectives	Applicable Course Content
Describe how SEDR can be used to collect and review forensic information for further investigation of security incidents.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** • Module: Reporting on Threats
Describe installation prerequisites, minimum solution configuration and installation procedures required to collect forensic data.	
Describe the methods used to create post incident reports and the benefits to forensic analysis it provides.	
Given a scenario, determine the appropriate method to create a post incident report using SEDR.	

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. What component consists of cross-platform applications that collect artifacts from endpoints and sends them to SEDR Cloud?

A. Collection Service Agent
B. Dissolvable Server Agent
C. SEDR Scan Agent
D. Cloud Service Agent

2. Which statement relates to the challenges faced from Incomplete Endpoint Remediation?

E. Limited granularity in normal activity
F. Reduced ability to detect advanced attack methods
G. Reduction of orchestration across controls
H. Attack objects remain on endpoint

3. What, in addition to Techniques, does the MITRE Att&ck Matrix consists of?

A. Entities
B. Problems
C. Tactics
D. Solutions

4. What is applied to the Collected Data within SEDR Cloud Tasks?

E. Investigation Playbook
F. Collection Service Agent
G. Dissolvable Agent Server
H. Scan Policy

5. What does a Ranged query do?

I. Returns or excludes data matching the exact field names and their values
J. Returns or excludes data falling between two specified values of a given field
K. Returns or excludes data matching a regular expression
L. Returns or excludes data based on specific values for a given field

6. What is the first step in the SEDR Insight proxy process?

M. SEDR checks to see if the file is blacklisted or whitelisted
N. SEDR returns reputation information
O. The Endpoint sends a reputation lookup to SEDR
P. Symantec Insight replies with reputation information to SEDR

7. Which Cybersecurity function would “deleting a file” fall under?

Q. Identify
R. Protect
S. Respond
T. Recover

8. Which Symantec Endpoint Protection (SEP) function is used when isolating a breached endpoint from the SEDR Manager?

U. Quarantine Firewall policy
V. Application and Device Control Policy
W. LiveUpdate policy
X. Centralized Exceptions Policy

9. Which feature of Symantec Endpoint Detection and Response allows for a Process Dump?

Y. Synapse
Z. Cynic
AA. Endpoint Activity Recorder
BB. Endpoint Communications Channel

10. What does a medium priority incident indicate?

CC. The incident can safely be ignored
DD. The incident can result in a business outage
EE. The incident does not affect critical business operation
FF. The incident may have an impact on the business

Sample Exam Answers:

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