BROADCOM SOFTWARE

Exam Study Guide

Administration of Symantec Endpoint Detection and Response 4.2

EXAM CODE: 250-555

Exam Description

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

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

For more information about Broadcom Software's certification program, see

https://www.broadcom.com/support/education/software/certification

Recommended Experience

It is recommended that the candidate has at least 3-6 months experience with Symantec EDR solutions (On Premise and/or Cloud) 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 Symantec EDR planning steps.
- Perform Symantec EDR implementation steps.
- Perform initial Symantec EDR configuration steps.
- Perform basic Symantec EDR administration actions.
- Configure Symantec EDR to integrate and share data with other applications.
- 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

Courses

Symantec Endpoint Detection and Response 4.2 Planning and Implementation

(2 Day Instructor Led with Hands-on Labs)

- Symantec EDR Overview
- Symantec EDR Architecture and Sizing
- Symantec EDR On-Premise Implementation
- Symantec EDR Cloud Implementation

Symantec Endpoint Detection and Response 4.2 Administration

(2 Day Instructor Led with Hands-on Labs)

- Introduction to Symantec EDR
- Increasing the Visibility of Suspicious and Malicious Activity
- Decreasing Security Risk by Responding to Security Threats
- Collecting and Analyzing Forensic Data for the Investigation of Security Incidents

Documentation

- Symantec EDR Help
- https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-4.html
    - Related Documents (Includes the following):
    - Symantec EDR Sizing and Scalability Guide
    - Symantec EDR Installation Guide for Dell 8840 and 8880 Appliances
    - Symantec EDR Installation Guide for Virtual Appliances
    - Symantec EDR Installation Guide for the S550 Appliance
    - Symantec EDR Threat Hunting Guide
    - Symantec EDR App for Splunk Administration Guide
    - Symantec EDR App 1.0 for ServiceNow
- https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-4/Related-Documents.html

Website

- https://support.broadcom.com/security
- https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-4.html
- https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-4/Related-Documents.html
- Symantec Endpoint Detection and Response Product Page
- Symantec Endpoint Detection and Response Help
- https://www.broadcom.com/support/education/software/training-courses
- https://www.broadcom.com/support/education/symantec/elibrary

Exam Objectives

The following tables list the Broadcom Software 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.

It is strongly recommended that all candidates complete all applicable lab exercises in preparation for the exam.

Symantec EDR Overview

Exam Objectives	Applicable Course Content
Describe the Symantec EDR Shared Technologies.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR Overview • *Shared Technologies*
Describe the Symantec EDR product add-ons.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR Overview • *Product Add-Ons*

Symantec EDR Architecture and Sizing

Exam Objectives	Applicable Course Content
Describe the Symantec EDR Architecture.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR Architecture and Sizing • *Symantec EDR Architecture*
Describe sizing a Symantec EDR implementation.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR Architecture and Sizing • *Symantec EDR Sizing*

Symantec EDR On-Premise Implementation

Exam Objectives	Applicable Course Content
Describe the Symantec EDR System Requirements.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR On-Prem Implementation • *System Requirements* •
Describe the Symantec EDR Bootstrapping process.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR On-Prem Implementation • *Bootstrapping*

Exam Objectives	Applicable Course Content
Describe the Symantec EDR Initial Configuration process.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR On-Prem Implementation • *Initial Configuration*
Describe Symantec EDR User-Managed Certificates.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR On-Prem Implementation • *User-Managed Certificates*
Describe the Symantec EDR On-Prem User Accounts and Roles.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR On-Prem Implementation • *User Accounts and Roles*
Describe the process of integration Symantec EDR with Symantec Endpoint Protection.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR On-Prem Implementation • *Symantec Endpoint Protection Integration*

Symantec EDR Cloud Implementation

Exam Objectives	Applicable Course Content
Describe the Symantec EDR Cloud User Accounts and Roles.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR Cloud Implementation • *User Accounts and Roles*
Describe Symantec EDR Cloud Network Ranges.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR Cloud Implementation • *Network Ranges*
Describe Symantec EDR Cloud Dissolvable Agent Servers.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR Cloud Implementation • *Dissolvable Agent Servers*
Describe Symantec EDR Cloud Dissolvable Agent Server Configurations.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR Cloud Implementation • *Dissolvable Agent Server Configurations*
Describe Symantec EDR Cloud Collection Service Agents.	**Symantec EDR 4.2 Planning and Implementation Course** • Symantec EDR Cloud Implementation • *Collection Service Agents*

Symantec EDR and the Evolving Threat Landscape

Exam Objectives	Applicable Course Content
Describe the capabilities and functions of Symantec EDR.	**Symantec EDR 4.2 Administration Course** • Evolving Threat Landscape • *Introduction*
Describe the challenges faced when threat hunting in the environment and their resultant business objectives.	**Symantec EDR 4.2 Administration Course** • Evolving Threat Landscape • *Introduction* • *Challenges of Endpoint Detection & Response in the environment*
Describe how Symantec EDR meets business objectives.	**Symantec EDR 4.2 Administration Course** • Evolving Threat Landscape • *Introduction* • *How Symantec Endpoint Detection and Response meets objectives*

Increasing the Visibility of Suspicious and Malicious Activity

Exam Objectives	Applicable Course Content
Describe the benefits and outcomes of increasing the visibility of suspicious and malicious activity in the environment.	**Symantec EDR 4.2 Administration Course** • Evolving Threat Landscape • *How Symantec Endpoint Detection and Response meets objectives* • Increase the Visibility of Suspicious and Malicious Activity • *Introduction*
Describe how SEDR increases the visibility of suspicious and malicious activity in a typical environment.	**Symantec EDR 4.2 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Introduction*
Describe the various types of suspicious and malicious activity found in a typical environment.	**Symantec EDR 4.2 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Introduction* • *Identifying evidence of suspicious & malicious activity*
Describe installation prerequisites, minimum solution configuration and installation procedures required to identify threats.	**Symantec EDR 4.2 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Introduction* • *Identifying evidence of suspicious & malicious activity*

Exam Objectives	Applicable Course Content
Describe the methods used to identify evidence of suspicious and malicious activity.	**Symantec EDR 4.2 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Identifying evidence of suspicious & malicious activity*
Describe the methods used to enable automated security incident notifications with SEDR.	**Symantec EDR 4.2 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Identifying evidence of suspicious & malicious activity*

Describe the various types of Indicators of Compromise (IoC) found in a typical environment.	**Symantec EDR 4.2 Administration Course**
	• Increase the Visibility of Suspicious and Malicious Activity
	  • *Introduction*
	  • *Searching for Indicators of Compromise*

Describe installation prerequisites, minimum solution configuration and installation procedures required before identifying IOCs.	**Symantec EDR 4.2 Administration Course** • Increase the Visibility of Suspicious and Malicious Activity • *Searching for Indicators of Compromise*

Describe the methods used to search for IOCs using SEDR.	**Symantec EDR 4.2 Administration Course**
	• Increase the Visibility of Suspicious and Malicious Activity
	  • *Introduction*
	  • *Searching for Indicators of Compromise*

Decreasing Security Risk by Responding to Threats

Exam Objectives	Applicable Course Content
Describe the benefits of reducing security risks by responding to threats in the environment.	**Symantec EDR 4.2 Administration Course** • Decreasing Security Risk by Responding to Threats • *Introduction*
Describe the methods SEDR uses to respond to threats in a typical environment.	**Symantec EDR 4.2 Administration Course** • Decreasing Security Risk by Responding to Threats • *Introduction*

Describe the various methods used to isolate threats in a typical environment.	**Symantec EDR 4.2 Administration Course**
	• Decreasing Security Risk by Responding to Threats
	  • *Introduction*
	  • *Isolating Threats in the Environment*

Describe installation prerequisites, minimum solution configuration and installation procedures required to isolate threats.	**Symantec EDR 4.2 Administration Course** • Decreasing Security Risk by Responding to Threats • *Isolating Threats in the Environment*

Exam Objectives	Applicable Course Content
Given a scenario, determine the appropriate method for isolating threats to reduce security risk.	**Symantec EDR 4.2 Administration Course** • Decreasing Security Risk by Responding to Threats • *Isolating Threats in the Environment*
Describe the various methods used to block threats in a typical environment.	**Symantec EDR 4.2 Administration Course** • Decreasing Security Risk by Responding to Threats • *Blocking Threats in the Environment*
Describe installation prerequisites, minimum solution configuration and installation procedures required to block threats.	**Symantec EDR 4.2 Administration Course** • Decreasing Security Risk by Responding to Threats • *Blocking Threats in the Environment*
Given a scenario, determine the appropriate method for blocking threats to reduce security risk.	**Symantec EDR 4.2 Administration Course** • Decreasing Security Risk by Responding to Threats • *Blocking Threats in the Environment*

Describe the various methods used to remove threats in a typical environment.	**Symantec EDR 4.2 Administration Course**
	• Decreasing Security Risk by Responding to Threats
	  • *Introduction*
	  • *Removing Threats in the Environment*

Describe installation prerequisites, minimum solution configuration and installation procedures required to remove threats.	**Symantec EDR 4.2 Administration Course** • Decreasing Security Risk by Responding to Threats • *Removing Threats in the Environment*
Given a scenario, determine the appropriate method for removing threats to reduce security risk.	**Symantec EDR 4.2 Administration Course** • Decreasing Security Risk by Responding to Threats • *Removing Threats in the Environment*

Collecting and Reporting Forensic Data

Exam Objectives	Applicable Course Content
Describe the benefits of collecting and reviewing forensic information.	**Symantec EDR 4.2 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Introduction*

Describe how SEDR can be used to collect and review forensic information for further investigation of security incidents.	**Symantec EDR 4.2 Administration Course**
	• Collecting and Reporting Forensic Data for Further Investigation
	  • *Introduction*
	  • *Collecting Forensic Information*

Exam Objectives	Applicable Course Content

Describe the various forms of information collected by SEDR in a typical environment.	**Symantec EDR 4.2 Administration Course**
	• Collecting and Reporting Forensic Data for Further Investigation
	  • *Introduction*
	  • *Collecting Forensic Information*

Describe installation prerequisites, minimum solution configuration and installation procedures required to collect forensic data.	**Symantec EDR 4.2 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Collecting Forensic Information*
Given a scenario, determine the appropriate method for the collection of forensic data using SEDR.	**Symantec EDR 4.2 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Collecting Forensic Information*

Describe the methods used to create post incident reports and the benefits to forensic analysis it provides.	**Symantec EDR 4.2 Administration Course**
	• Collecting and Reporting Forensic Data for Further Investigation
	  • *Introduction*
	  • *Reporting Forensic Information*

Given a scenario, determine the appropriate method to create a post incident report using SEDR.	**Symantec EDR 4.2 Administration Course** • Collecting and Reporting Forensic Data for Further Investigation • *Reporting Forensic Information*

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?

A. Limited granularity in normal activity
B. Reduced ability to detect advanced attack methods
C. Reduction of orchestration across controls
D. 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?

A. Investigation Playbook
B. Collection Service Agent
C. Dissolvable Agent Server
D. Scan Policy

5. What does a Ranged query do?

A. Returns or excludes data matching the exact field names and their values
B. Returns or excludes data falling between two specified values of a given field
C. Returns or excludes data matching a regular expression
D. Returns or excludes data based on specific values for a given field

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

A. SEDR checks to see if the file is blacklisted or whitelisted
B. SEDR returns reputation information
C. The Endpoint sends a reputation lookup to SEDR
D. Symantec Insight replies with reputation information to SEDR

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

A. Identify
B. Protect
C. Respond
D. Recover

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

A. Quarantine Firewall policy
B. Application and Device Control Policy
C. LiveUpdate policy
D. Centralized Exceptions Policy

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

A. Synapse
B. Cynic
C. Endpoint Activity Recorder
D. Endpoint Communications Channel

10. What does a medium priority incident indicate?

A. The incident can safely be ignored
B. The incident can result in a business outage
C. The incident does not affect critical business operation
D. 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