Broadcom 250-571

Broadcom Endpoint Detection and Response 4.x Technical Specialist Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

250-571

Technical Specialist of Endpoint Detection and Response 4.x
65-70 Questions Exam – 70% Cut Score – Duration of 90 minutes

Table of Contents:

Discover More about the Broadcom 250-571 Certification

Are you interested in passing the Broadcom 250-571 exam? First discover, who benefits from the 250-571 certification. The 250-571 is suitable for a candidate if he wants to learn about Endpoint Security. Passing the 250-571 exam earns you the Technical Specialist of Endpoint Detection and Response 4.x title.

While preparing for the 250-571 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The 250-571 PDF contains some of the most valuable preparation tips and the details and instant access to useful **250-571 study materials just at one click.**

Broadcom 250-571 Endpoint Detection and Response 4.x Technical Specialist Certification Details:

Exam Name	Technical Specialist of Endpoint Detection and Response 4.x
Exam Code	250-571
Exam Price	$250 (USD)
Duration	90 mins
Number of Questions	65-70
Passing Score	70%
Books / Training	**Endpoint Detection and Response 4.x Planning, Implementation and Administration R1**
Schedule Exam	**Pearson VUE**
Sample Questions	**Broadcom Endpoint Detection and Response 4.x Technical Specialist Sample Questions**
Practice Exam	**Broadcom 250-571 Certification Practice Exam**

Broadcom 250-571 Syllabus:

Topic	Details
Introduction to Symantec Endpoint Detection and Response	- Describe the challenges faced when threat hunting in the environment and their resultant business objectives.

Topic	Details
	- Describe how Symantec EDR meets business objectives.
Architecting and Sizing	- Given a scenario, demonstrate knowledge of SEDR Architecture and Sizing considerations. - Describe the capabilities and functions of Symantec EDR.
Implementation	- Given a scenario, define the discrete components found within SEDR. - 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	- Describe how SEDR increases the visibility of suspicious and malicious activity in a typical environment. - Describe installation prerequisites, minimum solution configuration and installation procedures required to identify threats.
Investigating Threats	- Describe the various types of suspicious and malicious activity found in a typical environment. - 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	- Describe the benefits of reducing security risks by responding to threats in the environment. - 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.

Topic	Details
Reporting on Threats	- Describe how SEDR can be used to collect and review forensic information for further investigation of security incidents. - 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.

Broaden Your Knowledge with Broadcom 250-571 Sample Questions:

Question: 1

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

Answer: b

Question: 2

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

a) Endpoint Communications Channel
b) Cynic
c) Synapse
d) Endpoint Activity Recorder

Answer: d

Question: 3

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

a) Entities
b) Problems
c) Tactics
d) Solutions

Answer: c

Question: 4

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

a) Recover
b) Respond
c) Protect
d) Identify

Answer: b

Question: 5

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

Answer: a

Question: 6

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

Answer: c

Question: 7

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

Answer: c

Question: 8

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

Answer: d

Question: 9

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

Answer: a

Question: 10

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

a) Attack objects remain on endpoint
b) Reduced ability to detect advanced attack methods
c) Reduction of orchestration across controls
d) Limited granularity in normal activity

Answer: a

Avail the Study Guide to Pass Broadcom 250-571 Endpoint Detection and Response 4.x Technical Specialist Exam:

- Find out about the 250-571 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **Broadcom 250-571 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk

out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.

- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the **Endpoint Detection and Response 4.x Technical Specialist training.** Joining the Broadcom provided training for this Broadcom certification exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **Broadcom 250-571 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. 250-571 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

Passing the Broadcom 250-571 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.