Broadcom 250-580

Broadcom Endpoint Security Complete - R2 Technical Specialist Certification Questions & Answers

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

250-580

Technical Specialist of Endpoint Security Complete - R2
150 Questions Exam – 70% Cut Score – Duration of 180 minutes

Table of Contents:

Discover More about the Broadcom 250-580 Certification

Are you interested in passing the Broadcom 250-580 exam? First discover, who benefits from the 250-580 certification. The 250-580 is suitable for a candidate if he wants to learn about Endpoint Security. Passing the 250-580 exam earns you the Technical Specialist of Endpoint Security Complete - R2 title.

While preparing for the 250-580 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The 250-580 PDF contains some of the most valuable preparation tips and the details and instant access to useful **250-580 study materials just at one click.**

Broadcom 250-580 Endpoint Security Complete - R2 Technical Specialist Certification Details:

Exam Name	Technical Specialist of Endpoint Security Complete - R2
Exam Code	250-580
Exam Price	$250 (USD)
Duration	180 mins
Number of Questions	150
Passing Score	70%
Books / Training	**Endpoint Protection 14.x Administration R1** **Endpoint Protection 14.2 Maintain and Troubleshoot** **Endpoint Detection and Response 4.x Planning, Implementation and Administration R1**
Schedule Exam	**Pearson VUE**
Sample Questions	**Broadcom Endpoint Security Complete - R2 Technical Specialist Sample Questions**
Practice Exam	**Broadcom 250-580 Certification Practice Exam**

Broadcom 250-580 Syllabus:

Topic	Details
Introduction to Symantec Endpoint Security Complete	- Understand SES Complete Architecture. - Describe the benefits of SES Complete Cloud-based management.

Topic	Details
	- Describe the various methods for enrolling SES endpoint agents.
Configuring SES Complete Security Controls	- Understand how policies are used to protect endpoint devices. - Understand the Threat landscape and the MITRE ATT&CK Framework. - Describe how SES Complete can be used in preventing an attacker from accessing the environment. - 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	- Describe the ICDm security control dashboards and their use. - 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	- Describe the requirements to enable Endpoint Detection and Response in the ICDm management console. - Describe how EDR assists in identifying suspicious and malicious activity. - Describe how EDR aids in investigating potential threats.

Topic	Details
	- 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	- Describe Behavior Prevalence the use of the SES Complete Behavioral Insights and Policy Tuning Widget. - 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. - Describe the process of monitoring drift to further tune App Control policies.
Mobile and Modern Device Security	- Describe the requirements to enable Network Integrity in the ICDm management console. - Describe Network Integrity Policy Configuration and its 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	- Describe the requirements for Threat Defense for Active Directory Installation and Configuration. - Describe the Threat Defense Active Directory policy and its use. - Describe how Threat Defense for Active Directory is used to identify threats. - Describe how Threat Defense for Active Directory protects against misconfigurations and vulnerabilities in an environment.

Topic	Details
Working with a Hybrid Environment	- Describe the process for policy migration from SEPM to the ICDm console. - 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.
Architecting and Sizing the SEP Implementation	- Describe the Symantec Endpoint Protection components. - Determine proper placement for GUP, SEPM, and LUA for communication and content deployment.
Preventing File-Based Attacks with SEP Layered Security	- Explain common threats and security risks to the endpoint.
Managing Client Architecture and Active Directory Integration	- Explain how policies and concepts relate to the Symantec Endpoint Protection architecture. - Describe how to configure communication, general, and security settings.
Managing Client-to-Server Communication	- Identify how to verify client connectivity and find clients in the console.
Introducing Content Updates Using LiveUpdate	- Describe how to configure LiveUpdate policies.
Managing Security Exceptions	- Describe when and how to configure exceptions. - Explain the remediation actions for infected files.
Preventing Attacks with SEP Layered Security	- Describe how protection technologies interact and their dependencies. - Describe how to customize Firewall, Intrusion Prevention and Application and Device Control policies.
Securing Windows Clients	- Describe how to configure scheduled and ondemand scans. - Describe how to configure Auto-Protect for file systems/email clients. - Describe how to configure Insight and Download Insight. - Describe how to configure SONAR.
Protecting Against Network Attacks and Enforcing Corporate	- Describe how to configure the Firewall policy.

Topic	Details
Policies using the Firewall Policy	
Blocking Network Threats with Intrusion Prevention	- Describe how to configure Intrusion Prevention policies.
Controlling Application and File Access and Restricting Device Access for Windows and Mac Clients	- Describe how to configure Application and Device Control policies.
Installing the Symantec Endpoint Protection Manager	- Explain when to install additional Symantec Endpoint Protection Managers and sites.
Managing Replication and Failover	- Describe how to edit server and site properties.
Benefiting from a SEPM Disaster Recovery Plan	- Explain the procedures for Symantec Endpoint Protection database management, backup, restore and Symantec Endpoint Protection disaster recovery.
Monitoring the Environment and Responding to Threats	- Describe how to create, view, and manage notifications.
Managing Console Access and Delegating Authority	- Describe how to manage administrator accounts and delegation of roles.
Endpoint Detection and Response – 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 identify threats.
Detecting Threats	- Describe installation prerequisites, minimum solution configuration and installation procedures required to identify threats. - Describe the challenges faced when threat hunting in the environment and their resultant business objectives.
Investigating Threats	- Describe the methods used to identify evidence of suspicious and malicious activity. - Describe the various types of Indicators of

Topic	Details
	Compromise (IoC) found in a typical environment. - Describe the methods used to search for IOCs using SEDR.
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.
Reporting on Threats	- 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 250-580 Sample Questions:

Question: 1

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

Answer: d

Question: 2

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

Answer: b

Question: 3

Which report format is supported in Symantec Endpoint Security?

a) Text
b) HTML
c) XML
d) PDF

Answer: d

Question: 4

Which SES Policy controls port scan detection?

a) IPS
b) Firewall
c) Device Control
d) Exploit Mitigation

Answer: b

Question: 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

Answer: c

Question: 6

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

a) Rampage
b) Kill Chain
c) Exfiltration
d) Impact

Answer: d

Question: 7

Which antimalware engine detects attacks coded in JavaScript?

a) Emulator
b) Sapient
c) Core3
d) SONAR

Answer: a

Question: 8

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

a) 4G
b) Wifi
c) Satellite
d) VPN

Answer: c

Question: 9

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

a) Deny list file
b) Allow list file
c) Enable IPS audit
d) Quarantine file

Answer: a

Question: 10

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

a) User Access Control
b) Windows Firewall
c) Group Policies
d) Local Policies

Answer: a

Avail the Study Guide to Pass Broadcom 250-580 Endpoint Security Complete - R2 Technical Specialist Exam:

- Find out about the 250-580 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 250-580 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 Security Complete - R2 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 250-580 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. 250-580 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 250-580 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.

Here Is the Trusted Practice Test for the Broadcom 250-580 Certification

CertFun.Com is here with all the necessary details regarding the 250-580 exam. We provide authentic practice tests for the 250-580 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on CertFun.Com for rigorous, unlimited two-month attempts on the **250-580 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the Technical Specialist of Endpoint Security Complete - R2.

Start Online practice of Broadcom 250-580 Exam by visiting URL
https://www.certfun.com/broadcom/250-580-symantec-endpoint-security-complete-r2-technical-specialist