Broadcom 250-580 Practice Questions

Shared by Cortez on 03-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which security control is complementary to IPS, providing a second layer of protection against network attacks?

Options:

A- Host Integrity
B- Network Protection
C- Antimalware
D- Firewall

Answer:

D

Explanation:

The Firewall provides a complementary layer of protection to Intrusion Prevention System (IPS) in Symantec Endpoint Protection.

Firewall vs. IPS:

While IPS detects and blocks network-based attacks by inspecting traffic for known malicious patterns, the firewall controls network access by monitoring and filtering inbound and outbound traffic based on policy rules.

Together, these tools protect against a broader range of network threats. IPS is proactive in identifying malicious traffic, while the firewall prevents unauthorized access.

Two-Layer Defense Mechanism:

The firewall provides control over which ports, protocols, and applications can access the network, reducing the attack surface.

When combined with IPS, the firewall blocks unauthorized connections, while IPS actively inspects and prevents malicious content within allowed traffic.

Why Other Options Are Not Complementary:

Host Integrity focuses on compliance and configuration validation rather than direct network traffic protection.

Network Protection and Antimalware are essential but do not function as second-layer defenses for IPS within network contexts.

Question 2

Question Type: MultipleChoice

What version number is assigned to a duplicated policy?

Options:

A- The original policy's version number
B- Zero
C- The original policy's number plus one
D- One

Answer:

D

Explanation:

When a policy is duplicated in Symantec Endpoint Protection (SEP), the duplicated policy is assigned a version number of 'One'. This means that the new policy starts fresh with a version number of 1, separate from the original policy's version history. The SEP system uses this new version number to track any subsequent changes to the duplicated policy independently of the original.

Question 3

Question Type: MultipleChoice

Which Firewall rule components should an administrator configure to block facebook.com use during business hours?

Options:

A- Host(s), Network Interface, and Network Service
B- Application, Host(s), and Network Service
C- Action, Hosts(s), and Schedule

D- Action, Application, and Schedule

Answer:

C

Explanation:

To block facebook.com use during business hours, the SEP administrator should configure the Action, Hosts(s), and Schedule components within the Firewall rule.

Explanation of Each Component:

Action: Set to 'Block' to deny access to the specified site.

Hosts(s): Specify facebook.com as the target host, ensuring that all traffic to this domain is blocked.

Schedule: Define the rule to apply only during business hours, ensuring that access is restricted within the designated time frame.

Why Other Options Are Incorrect:

Network Interface and Network Service (Options A and B) are not specific to blocking domain access.

Application (Options B and D) is unnecessary if the goal is to block access based on domain and schedule.

Question 4

Question Type: MultipleChoice

What methods should an administrator utilize to restore communication on a client running SEP for Mac?

Options:

A- Use Client Deployment Wizard to push out a communications package.
B- Use the Sylink Drop Tool on the SEPM.
C- Use SSH and run the command:
D- sudo launchct1 load /Library/LaunchDaemons/eom.Symantec.symdaemon.'plist
E- Use Third Party Deployment to push out a communications package.

Answer:

A

Explanation:

To restore communication on a client running Symantec Endpoint Protection (SEP) for Mac, an administrator should use the Client Deployment Wizard to push out a communications package. This package re-establishes communication settings with the Symantec Endpoint Protection Manager (SEPM), ensuring the client can connect to the management server.

Why Use Client Deployment Wizard:

The Client Deployment Wizard allows administrators to deploy the communication settings (Sylink.xml) needed for the SEP client to reconnect to SEPM, re-establishing proper communication channels.

Why Other Options Are Less Suitable:

Sylink Drop Tool (Option B) is primarily used on Windows, not macOS.

SSH command (Option C) is not relevant for restoring SEPM communication settings.

Third-Party Deployment (Option D) is unnecessary when the Client Deployment Wizard is available.

Question 5

Question Type: MultipleChoice

What does a medium-priority incident indicate?

Options:

A- The incident may have an impact on the business
B- The incident can result in a business outage
C- The incident does not affect critical business operation
D- The incident can safely be ignored

Answer:

A

Explanation:

A medium-priority incident in Symantec's framework indicates that the incident may have an impact on the business. This priority level suggests that while the incident is not immediately critical, it still poses a potential risk to business operations and should be addressed.

Understanding Medium-Priority Impact:

Medium-priority incidents are not severe enough to cause immediate operational disruption but may still affect business processes or data security if left unresolved.

Prompt action is recommended to prevent escalation or downstream effects on business functions.

Why Other Options Are Incorrect:

Business outage (Option B) would likely be classified as high priority.

No impact on critical operations (Option C) would suggest a lower priority.

Safe to ignore (Option D) does not reflect the importance of addressing medium-priority incidents.

Question 6

Question Type: MultipleChoice

What EDR function minimizes the risk of an endpoint infecting other resources in the environment?

Options:

A- Quarantine
B- Block
C- Deny List
D- Firewall

Answer:

A

Explanation:

The function of 'Quarantine' in Endpoint Detection and Response (EDR) minimizes the risk of an infected endpoint spreading malware or malicious activities to other systems within the network environment. This is accomplished by isolating or restricting access of the infected endpoint to contain any threat within that specific machine. Here's how Quarantine functions as a protective measure:

Detection and Isolation: When EDR detects potential malicious behavior or files on an endpoint, it can automatically place the infected file or process in a 'quarantine' area. This means the threat is separated from the rest of the system, restricting its ability to execute or interact with other resources.

Minimizing Spread: By isolating compromised files or applications, Quarantine ensures that malware or suspicious activities do not propagate to other endpoints, reducing the risk of a widespread infection.

Administrative Review: After an item is quarantined, administrators can review it to determine if it should be deleted or restored based on a false positive evaluation. This controlled environment allows for further analysis without risking network security.

Endpoint-Specific Control: Quarantine is designed to act at the endpoint level, applying restrictions that affect only the infected system without disrupting other network resources.

Using Quarantine as an EDR response mechanism aligns with best practices outlined in endpoint security documentation, such as Symantec Endpoint Protection, which emphasizes containment as a critical first response to threats. This approach supports the proactive defense strategy of limiting lateral movement of malware across a network, thus preserving the security and stability of the entire system.

Question 7

Question Type: MultipleChoice

Which SES feature helps administrators apply policies based on specific endpoint profiles?

Options:

A- Policy Bundles
B- Device Profiles
C- Policy Groups
D- Device Groups

Answer:

D

Explanation:

In Symantec Endpoint Security (SES), Device Groups enable administrators to apply policies based on specific endpoint profiles. Device Groups categorize endpoints according to characteristics like department, location, or device type, allowing tailored policy application that meets the specific security needs of each group. By using Device Groups, administrators can efficiently manage security policies, ensuring relevant protections are applied based on the endpoint's profile.

Question 8

Question Type: MultipleChoice

How does an administrator view all devices impacted by a suspicious file?

Options:

A- From the Alerts and Events list, select Files; then, from the file list, select Devices.
B- From the Discovered Items list, select Devices.
C- From the Discovered Items list, select the file; then, from the Details page, select Devices.
D- From the Alerts and Event list, select Device.

Answer:

C

Explanation:

To view all devices impacted by a suspicious file, the administrator should go to the Discovered Items list, select the specific file, and then view the impacted devices from the Details page.

Steps to View Impacted Devices:

Navigate to the Discovered Items list within the management console.

Locate and select the suspicious file in question to open its Details page.

On the Details page, a list of devices associated with the file is displayed, providing insights into which endpoints are potentially impacted by the suspicious activity.

Why Other Options Are Less Suitable:

Options A and B do not provide the specific device list for a selected file.

Option D is incorrect as it implies selecting by device first rather than by suspicious file.

Question 9

Question Type: MultipleChoice

Which two (2) instances could cause Symantec Endpoint Protection to be unable to remediate a file? (Choose two.)

Options:

A- Another scan is in progress.
B- The detected file is in use.
C- There are insufficient file permissions.
D- The file is marked for deletion by Windows on restart.
E- The file has good reputation.

Answer:

B, C

Explanation:

Symantec Endpoint Protection (SEP) may be unable to remediate a file in certain situations. Two primary reasons for this failure are:

The detected file is in use (Option B): When a file is actively being used by the system or an application, SEP cannot remediate or delete it until it is no longer in use. Active files are locked by the operating system, preventing modification.

Insufficient file permissions (Option C): SEP needs adequate permissions to access and modify files. If SEP does not have the necessary permissions for the detected file, it cannot perform remediation.

Why Other Options Are Incorrect:

Another scan in progress (Option A) does not directly prevent remediation.

File marked for deletion on restart (Option D) would typically allow SEP to complete the deletion upon reboot.

File with good reputation (Option E) is less likely to be flagged for remediation but would not prevent it if flagged.

Question 10

Question Type: MultipleChoice

An organization is considering a single site for their Symantec Endpoint Protection environment. What are two (2) reasons that the organization should consider? (Select two)

Options:

A- Organizational merger
B- Sufficient WAN bandwidth
C- Delay-free, centralized reporting
D- 24x7 admin availability
E- Legal constraints

Answer:

B, C

Explanation:

When considering a single-site deployment for Symantec Endpoint Protection (SEP), the following two factors support this architecture:

Sufficient WAN Bandwidth (B):

A single-site SEP environment relies on robust WAN bandwidth to support endpoint communication, policy updates, and threat data synchronization across potentially distant locations.

High bandwidth ensures that endpoints remain responsive to management commands and receive updates without significant delays.

Delay-free, Centralized Reporting (C):

A single-site architecture enables all reporting data to be stored and accessed from one location, providing immediate insights into threats and system health across the organization.

Centralized reporting is ideal when administrators need quick access to consolidated data for faster decision-making and incident response.

Why Other Options Are Not As Relevant:

Organizational mergers (A) and legal constraints (E) do not necessarily benefit from a single-site architecture.

24x7 admin availability (D) is more related to staffing requirements rather than a justification for a single-site SEP deployment.

Question 11

Question Type: MultipleChoice

What Symantec Best Practice is recommended when setting up Active Directory integration with the Symantec Endpoint Protection Manager?

Options:

A- Ensure there is more than one Active Directory Server listed in the Server Properties.
B- Link the built-in Admin account to an Active Directory account.
C- Import the existing AD structure to organize clients in user mode.
D- Secure the management console by denying access to certain computers.

Answer:

C

Explanation:

When setting up Active Directory (AD) integration with Symantec Endpoint Protection Manager (SEPM), Symantec's best practice is to import the existing AD structure to manage clients in user mode. This approach offers several benefits:

Simplified Client Management: By importing the AD structure, SEPM can mirror the organizational structure already defined in AD, enabling easier management and assignment of policies to groups or organizational units.

User-Based Policies: Organizing clients in user mode allows policies to follow users across devices, providing consistent protection regardless of where the user logs in.

Streamlined Updates and Permissions: Integration with AD ensures that any changes in user accounts or groups are automatically reflected within SEPM, reducing administrative effort and potential errors in client organization.

This best practice enhances SEPM's functionality by leveraging the established structure in AD.

To Get Premium Files for 250-580 Visit

https://www.p2pexams.com/products/250-580

For More Free Questions Visit

https://www.p2pexams.com/broadcom/pdf/250-580

