Broadcom 250-586 Practice Questions

Shared by Ray on 03-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What must be done immediately after the Microsoft SQL Database is restored for a SEP Manager?

Options:

A- Restart Symantec services on the SEP Managers
B- Purge the SQL database
C- Trigger failover for the managed clients
D- Replicate the SQL database

Answer:

A

Explanation:

After restoring the Microsoft SQL Database for a Symantec Endpoint Protection (SEP) Manager, it is essential to restart the Symantec services on the SEP Managers immediately. This step ensures that the SEP Manager re-establishes a connection to the database and resumes normal operations. Restarting the services is critical to enable the SEP Manager to recognize and use the newly restored database, ensuring that all endpoints continue to function correctly and maintain their protection status.

Symantec Endpoint Protection Documentation specifies restarting services as a necessary action following any database restoration to avoid potential data synchronization issues and ensure seamless operation continuity.

Question 2

Question Type: MultipleChoice

What happens if a SEP Manager replication partner fails in a multi-site SEP Manager implementation?

Options:

A- Clients for that site connect to the remaining SEP Managers
B- Replication continues and reporting is delayed
C- Replication is stopped and managed devices discontinue protection
D- Clients for that site do not connect to remaining SEP Managers but date is retained locally

Answer:

A

Explanation:

In a multi-site SEP Manager implementation, if one SEP Manager replication partner fails, the clients for that site automatically connect to the remaining SEP Managers. This setup provides redundancy, ensuring that client devices maintain protection and receive policy updates even if one manager becomes unavailable.

Redundancy in Multi-Site Setup: Multi-site SEP Manager deployments are designed with redundancy, allowing clients to failover to alternative SEP Managers within the environment if their primary replication partner fails.

Continuous Client Protection: With this failover, managed devices continue to be protected and can still receive updates and policies from other SEP Managers.

Explanation of Why Other Options Are Less Likely:

Option B (delayed replication) and Option C (discontinued protection) are incorrect as replication stops only for the failed manager, and client protection continues through other managers.

Option D suggests data retention locally without failover, which is not the standard approach in a multi-site setup.

Therefore, the correct answer is that clients for the affected site connect to the remaining SEP Managers, ensuring ongoing protection.

Question 3

Question Type: MultipleChoice

Which term or expression is utilized when adversaries leverage existing tools in the environment?

Options:

A- Living off the land
B- Opportunistic attack
C- File-less attack
D- Script kiddies

Answer:

A

Explanation:

In cybersecurity, the term 'Living off the land' (LOTL) refers to adversaries using legitimate tools and software that are already present within a target's environment to conduct malicious activity. This approach allows attackers to avoid detection by using trusted applications instead of bringing in new, suspicious files that might be flagged by endpoint security solutions.

Definition and Usage Context 'Living off the land' is a method that leverages tools, utilities, and scripting environments typically installed for administrative or legitimate purposes. Attackers prefer this approach to minimize their visibility and avoid triggering endpoint detection mechanisms that rely on recognizing foreign or malicious executables. Tools like PowerShell, Windows Management Instrumentation (WMI), and command-line utilities (e.g., cmd.exe) are frequently employed by attackers using this strategy.

Tactics in Endpoint Security Complete Implementation Within an Endpoint Security Complete implementation framework, LOTL is specifically recognized in contexts where endpoint solutions need to monitor and distinguish between legitimate use and misuse of standard administrative tools. This approach is often documented in the Detection and Prevention phases of Endpoint Security Implementation, where specific focus is given to monitoring command-line activities, auditing PowerShell usage, and identifying anomalous behavior tied to these tools.

Impact and Mitigation LOTL can complicate detection efforts because security solutions must discern between legitimate and malicious uses of pre-existing tools. Symantec Endpoint Security Complete counters this by using behavior-based analysis, anomaly detection, and machine learning models to flag unusual patterns, even when no new files are introduced.

Relevant Reference in SES Complete Documentation Detailed guidance on addressing LOTL tactics within Symantec Endpoint Security Complete is often found in the documentation sections covering Threat Hunting and Behavior Analytics. These resources outline how the platform is designed to flag suspicious usage patterns within native OS tools, leveraging telemetry data and known indicators of compromise (IoCs) for early detection.

Question 4

Question Type: MultipleChoice

Which feature is designed to reduce the attack surface by managing suspicious behaviors performed by trusted applications?

Options:

A- Malware Prevention Configuration
B- Host Integrity Configuration
C- Adaptive Protection
D- Network Integrity Configuration

Answer:

C

Explanation:

Adaptive Protection is designed to reduce the attack surface by managing suspicious behaviors performed by trusted applications. This feature provides dynamic, behavior-based protection that allows trusted applications to operate normally while monitoring and controlling any suspicious actions they might perform.

Purpose of Adaptive Protection: It monitors and restricts potentially harmful behaviors in applications that are generally trusted, thus reducing the risk of misuse or exploitation.

Attack Surface Reduction: By focusing on behavior rather than solely on known malicious files, Adaptive Protection effectively minimizes the risk of attacks that exploit legitimate applications.

Explanation of Why Other Options Are Less Likely:

Option A (Malware Prevention Configuration) targets malware but does not specifically control trusted applications' behaviors.

Option B (Host Integrity Configuration) focuses on policy compliance rather than behavioral monitoring.

Option D (Network Integrity Configuration) deals with network-level threats, not application behaviors.

Therefore, Adaptive Protection is the feature best suited to reduce the attack surface by managing suspicious behaviors in trusted applications.

Question 5

Question Type: MultipleChoice

What do technical objectives represent in the general IT environment?

Options:

A- Operational constraints
B- Business values
C- Service-level agreements
D- Legal and regulatory compliance

Answer:

A

Explanation:

In the general IT environment, technical objectives typically represent operational constraints. These objectives are focused on the technical requirements and limitations of the IT infrastructure, such as system capacity, network performance, and resource availability. They are designed to guide the implementation and management of technology solutions within the practical limits of the organization's operational environment.

Symantec Endpoint Security Complete Implementation Documentation notes that technical objectives align closely with operational constraints to ensure solutions are feasible and sustainable within existing IT resources.

Question 6

Question Type: MultipleChoice

What does the Base Architecture section of the Infrastructure Design provide?

Options:

A- The mapping of the chosen implementation model
B- The methods for consistent and reliable delivery of agent installation packages
C- The approach to endpoint enrollment or agent installation
D- The illustration of the solution topology and component placement

Answer:

D

Explanation:

The Base Architecture section of the Infrastructure Design within SES Complete provides a visual layout of the solution topology and component placement. This section is essential for understanding how various components of the solution are distributed across the environment, detailing where each component resides and how they interconnect. This overview helps ensure that each part of the architecture is aligned with the overall security requirements and deployment model.

Reference in Symantec Endpoint Security Documentation explain that having a clear illustration of component placement and solution topology is crucial for effective deployment, maintenance, and scalability of the endpoint security infrastructure.

Question 7

Question Type: MultipleChoice

When a SEPM is enrolled in ICDm which policy can only be managed from the cloud?

Options:

A- Firewall
B- Network Intrusion Prevention
C- LiveUpdate
D- Intensive Protection

Answer:

B

Explanation:

When the Symantec Endpoint Protection Manager (SEPM) is enrolled in the Integrated Cyber Defense Manager (ICDm), certain policies are exclusively managed from the cloud, with the Network Intrusion Prevention policy as one of them. This arrangement centralizes control over specific security aspects to ensure consistent and unified policy application across cloud-managed endpoints, reinforcing a streamlined and efficient cloud-based administration model.

Reference in Symantec Endpoint Protection Documentation emphasize that Network Intrusion Prevention, once SEPM is integrated with ICDm, is governed centrally from the cloud to leverage real-time threat intelligence updates and broader, managed protection capabilities directly.

Question 8

Question Type: MultipleChoice

What is the first step in implementing the Logical Design of an On-Premise infrastructure?

Options:

A- Create the base management structure
B- Implement Groups and Location definitions
C- Deploy all SEP Manager Servers
D- Ensure the MS SQL servers are installed or procured

Answer:

D

Explanation:

The first step in implementing the Logical Design of an On-Premise infrastructure is to ensure the MS SQL servers are installed or procured. The SQL server is a critical backend component for Symantec Endpoint Protection Manager (SEPM) as it stores configuration, event logs, and other essential data. Securing this database infrastructure is foundational before deploying management structures or additional components.

SES Complete Implementation Documentation outlines this step as the initial action, providing the necessary data storage and management capabilities required for a stable on-premises deployment of the Logical Design.

Question 9

Question Type: MultipleChoice

What is the purpose of the Test Plan in the implementation phase?

Options:

A- To assess the SESC Solution Design in the customer's environment
B- To monitor the Implementation of SES Complete
C- To guide the adoption and testing of SES Complete in the implementation phase
D- To seek approval for the next phase of the SESC Implementation Framework

Answer:

C

Explanation:

In the implementation phase of Symantec Endpoint Security Complete (SESC), the Test Plan is primarily designed to provide structured guidance on adopting and verifying the deployment of SES Complete within the customer's environment. Here's a step-by-step reasoning:

Purpose of the Test Plan: The Test Plan ensures that all security features and configurations are functioning as expected after deployment. It lays out testing procedures that verify that the solution meets the intended security objectives and is properly integrated with the customer's infrastructure.

Adoption of SES Complete: This phase often includes evaluating how well SES Complete integrates into the customer's existing environment, addressing any issues, and making sure users and stakeholders are prepared for the transition.

Structured Testing During Implementation: The Test Plan is essential for testing and validating the solution's capabilities before fully operationalizing it. This involves configuring, testing, and fine-tuning the solution to align with the customer's security requirements and ensuring readiness for the next phase.

Explanation of Why Other Options Are Less Likely:

Option A refers to the broader solution design assessment, typically done during the design phase rather than in the implementation phase.

Option B is more aligned with post-implementation monitoring rather than guiding testing.

Option D (seeking approval for the next phase) relates to project management tasks outside the primary function of the Test Plan in this phase.

The purpose of the Test Plan is to act as a roadmap for adoption and testing, ensuring the SES Complete solution performs as required.

Question 10

Question Type: MultipleChoice

Which section of the SES Complete Solution Design provides a summary of the features and functions to be implemented?

Options:

A- Infrastructure Design
B- Configuration Design
C- Initial Test Plan
D- Executive Summary

P2P exams

Answer:

D

Explanation:

The Executive Summary section of the SES Complete Solution Design provides a summary of the features and functions to be implemented. This summary is tailored for stakeholders and decision-makers, offering a high-level overview of the solution's capabilities, key features, and intended outcomes without going into technical specifics. It helps to convey the value and strategic benefits of the SES Complete solution to the organization.

SES Complete Implementation Documentation highlights the Executive Summary as a crucial section for communicating the solution's scope and anticipated impact to executives and non-technical stakeholders.

P2P exams

To Get Premium Files for 250-586 Visit

https://www.p2pexams.com/products/250-586

For More Free Questions Visit

https://www.p2pexams.com/broadcom/pdf/250-586

