**Broadcom.Premium.250-586.75q - DEMO**

Number: 250-586
Passing Score: 800
Time Limit: 120
File Version: 1.7

## Exam Code: 250-586

## Exam Name: Endpoint Security Complete Implementation - Technical Specialist

**Website: www.Vdumps.com**

**Exam A**

**QUESTION 1**
Which technology is designed to prevent security breaches from happening in the first place?

A. Network Firewall and Intrusion Prevention
B. Host Integrity Prevention
C. Endpoint Detection and Response
D. Threat Hunter

**Correct Answer: A**
**Section:**
**Explanation:**
Network Firewall and Intrusion Prevention technologies are designed to prevent security breaches from happening in the first place by creating a protective barrier and actively monitoring network traffic for potential threats. Firewalls restrict unauthorized access, while Intrusion Prevention Systems (IPS) detect and block malicious activities in real-time. Together, they form a proactive defense to stop attacks before they penetrate the network.
Symantec Endpoint Security Documentation supports the role of firewalls and IPS as front-line defenses that prevent many types of security breaches, providing crucial protection at the network level.

**QUESTION 2**
What should be checked to ensure proper distribution and mapping for LUAs or GUPs in the Manage phase?

A. Content Delivery configuration
B. Replication between sites
C. Security Roles
D. Default or custom Device/Policy Groups

**Correct Answer: A**
**Section:**
**Explanation:**
To ensure proper distribution and mapping for LiveUpdate Administrators (LUAs) or Group Update Providers (GUPs) in the Manage phase, checking the Content Delivery configuration is essential. This configuration ensures that updates are correctly distributed to all endpoints and that LUAs or GUPs are properly positioned to reduce bandwidth usage and improve update efficiency across the network.
Symantec Endpoint Protection Documentation highlights the importance of verifying Content Delivery configuration to maintain effective update distribution and optimal performance, particularly in large or distributed environments.

**QUESTION 3**
Which EDR feature is used to search for real-time indicators of compromise?

A. Cloud Database search
B. Endpoint search
C. Domain search
D. Device Group search

**Correct Answer: B**
**Section:**
**Explanation:**
In Endpoint Detection and Response (EDR), the Endpoint search feature is used to search for real-time indicators of compromise (IoCs) across managed devices. This feature allows security teams to investigate suspicious

activities by querying endpoints directly for evidence of threats, helping to detect and respond to potential compromises swiftly.
SES Complete Documentation describes Endpoint search as a crucial tool for threat hunting within EDR, enabling real-time investigation and response to security incidents.

**QUESTION 4**
What is the purpose of the project close-out meeting in the Implement phase?

A. To retain and transfer knowledge

B. To develop and review the project plan

C. To obtain the customer's official acceptance of the engagement deliverables

D. To ensure that any potential outstanding activities and tasks are dismissed

**Correct Answer: C**
**Section:**
**Explanation:**
The purpose of the project close-out meeting in the Implement phase is to obtain the customer's official acceptance of the engagement deliverables. This meeting marks the formal conclusion of the project, where the consulting team presents the completed deliverables to the customer for approval. This step ensures that all agreed-upon goals have been met and provides an opportunity for the client to confirm satisfaction with the results, thereby formally closing the project.
SES Complete Implementation Curriculum notes that securing official acceptance is a crucial step to finalize the project, ensuring transparency and mutual agreement on the outcomes achieved.

**QUESTION 5**
What permissions does the Security Analyst Role have?

A. Search endpoints, trigger dumps, create policies

B. Trigger dumps, get and quarantine files, enroll new sites

C. Search endpoints, trigger dumps, get and quarantine files

D. Trigger dumps, get and quarantine files, create device groups

**Correct Answer: C**
**Section:**
**Explanation:**
In Endpoint Security Complete implementations, the Security Analyst Role generally has permissions that focus on monitoring, investigating, and responding to security threats rather than administrative functions like policy creation or device group management. Here's a breakdown of why Option C aligns with best practices:
Search Endpoints: Security Analysts are often tasked with investigating security alerts or anomalies. To support this, they typically need access to endpoint search functionalities to locate specific devices affected by potential threats.
Trigger Dumps: Triggering memory or system dumps on endpoints can be crucial for in-depth forensic analysis. This helps analysts capture a snapshot of the system's state during or after a security incident, aiding in a comprehensive investigation.
Get and Quarantine Files: Security Analysts are often allowed to isolate or quarantine files that are identified as suspicious or malicious. This action helps contain potential threats and prevent the spread of malware or other harmful activities within the network. This permission aligns with their role in mitigating threats as quickly as possible.
Explanation of Why Other Options Are Less Likely:
Option A (Create Policies): Creating policies typically requires higher administrative privileges, such as those assigned to security administrators or endpoint managers, rather than Security Analysts. Analysts primarily focus on threat detection and response rather than policy design.
Option B (Enroll New Sites): Enrolling new sites is typically an administrative task related to infrastructure setup and expansion, which falls outside the responsibilities of a Security Analyst.
Option D (Create Device Groups): Creating and managing device groups is usually within the purview of a system administrator or endpoint administrator role, as this involves configuring the organizational structure of the endpoint management system.
In summary, Option C aligns with the core responsibilities of a Security Analyst focused on threat investigation and response. Their permissions emphasize actions that directly support these objectives, without extending into administrative configuration or setup tasks.

**QUESTION 6**
What is the purpose of the Test Plan in the implementation phase?

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

**Correct Answer: C**
**Section:**
**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 7**
Which policy should an administrator edit to utilize the Symantec LiveUpdate server for pre-release content?

A. The System Policy

B. The LiveUpdate Policy

C. The System Schedule Policy

D. The Firewall Policy

**Correct Answer: B**
**Section:**
**Explanation:**
To use the Symantec LiveUpdate server for pre-release content, the administrator should edit the LiveUpdate Policy. This policy controls how endpoints receive updates from Symantec, including options for pre-release content.
Purpose of the LiveUpdate Policy: The LiveUpdate Policy is specifically designed to manage update settings, including source servers, scheduling, and content types. By adjusting this policy, administrators can configure endpoints to access pre-release content from Symantec's servers.
Pre-Release Content Access: Enabling pre-release content within the LiveUpdate Policy allows endpoints to test new security definitions and updates before they are generally available. This can be beneficial for organizations that want to evaluate updates in advance.
Policy Configuration for Symantec Server Access: The LiveUpdate Policy can be set to point to the Symantec LiveUpdate server, allowing endpoints to fetch content directly from Symantec, including any available beta or pre-release updates.
Explanation of Why Other Options Are Less Likely:
Option A (System Policy) and Option C (System Schedule Policy) do not govern update settings.
Option D (Firewall Policy) controls network access rules and would not manage LiveUpdate configurations.
Therefore, to configure access to the Symantec LiveUpdate server for pre-release content, the LiveUpdate Policy is the correct policy to edit.

**QUESTION 8**
What is purpose of the Solution Configuration Design in the Implement phase?

A. To provide a brief functional overview of the component placement in the environment
B. To outline the hardware requirements for on-premise components
C. To guide the implementation of features and functions
D. To detail the storage estimates and hardware configuration

**Correct Answer: C**
**Section:**
**Explanation:**
The Solution Configuration Design in the Implement phase serves to guide the implementation of features and functions within the deployment. It provides specific details on how to configure the solution to meet the organization's security requirements.
Purpose in Implementation: This document provides detailed instructions for configuring each feature and function that the solution requires. It helps ensure that all components are set up according to the design specifications.
Guidance for Administrators: The Solution Configuration Design outlines precise configurations, enabling administrators to implement necessary controls, settings, and policies.
Consistency in Deployment: By following this document, the implementation team can maintain a consistent approach across the environment, ensuring that all features operate as intended and that security measures align with the intended use case.
Explanation of Why Other Options Are Less Likely:
Option A (brief functional overview) is typically part of the initial design phase.
Option B (hardware requirements) would be part of the Infrastructure Design.
Option D (storage and hardware configuration) is more relevant to system sizing rather than feature configuration.
Thus, the Solution Configuration Design is key to guiding the implementation of features and functions.

**QUESTION 9**
What is the recommended setup to ensure clients automatically fallback to their Priority 1 server(s) in case of a faulty SEP Manager?

A. Configure all SEP Managers with equal priority
B. Configure all SEP Managers with different priorities
C. Do not configure any priority for SEP Managers
D. Use a separate fallback server

**Correct Answer: A**
**Section:**
**Explanation:**
To ensure clients can automatically fall back to their Priority 1 server(s) if a SEP Manager fails, it is recommended to configure all SEP Managers with equal priority.
Fallback Mechanism: When SEP Managers are set with equal priority, clients can automatically reconnect to any available server in their priority group. This setup offers a high-availability solution, allowing clients to quickly fall back to another server if their primary SEP Manager becomes unavailable.
Ensuring Continuity: Equal priority settings enable seamless client-server communication, ensuring clients do not experience interruptions in receiving policy updates or security content.
High Availability: This configuration supports a robust failover system where clients are not dependent on a single manager, thus enhancing resilience against server outages.
Explanation of Why Other Options Are Less Likely:
Option B (different priorities) could cause delays in failover as clients would have to exhaust Priority 1 servers before attempting Priority 2 servers.
Option C (no priority configuration) would lead to inconsistent fallback behavior.
Option D (separate fallback server) adds complexity and is not required for effective client fallback.
Therefore, setting all SEP Managers with equal priority is the recommended setup.

**QUESTION 10**
Where can you submit evidence of malware not detected by Symantec products?

A. SymProtect Cases Page

B. Virus Definitions and Security Update Page
C. SymSubmit Page
D. Symantec Vulnerability Response page

**Correct Answer: C**
**Section:**
**Explanation:**
The SymSubmit Page is the designated platform for submitting evidence of malware not detected by Symantec products. This process allows Symantec to analyze the submission and potentially update its definitions or detection techniques.
Purpose of SymSubmit: This page is specifically set up to handle customer-submitted files that may represent new or undetected threats, enabling Symantec to improve its malware detection capabilities.
Process of Submission: Users can submit files, URLs, or detailed descriptions of the suspected malware, and Symantec's security team will review these submissions for potential inclusion in future updates.
Improving Detection: By submitting undetected malware, organizations help Symantec maintain up-to-date threat intelligence, which enhances protection for all users.
Explanation of Why Other Options Are Less Likely:
Option A (SymProtect Cases Page) is not intended for malware submissions.
Option B (Virus Definitions and Security Update Page) provides updates, not a submission platform.
Option D (Symantec Vulnerability Response page) is focused on reporting software vulnerabilities, not malware.
The correct location for submitting undetected malware is the SymSubmit Page.

**QUESTION 11**
What is the primary purpose of the Pilot Deployment in the Implementation phase?

A. To validate the effectiveness of the solution design in the customer's environment
B. To ensure that the communication paths between major components have been established
C. To ensure that any potential outstanding activities and tasks are assigned to the right people
D. To ensure that all accounts are set with their allocated permissions and assignments

**Correct Answer: A**
**Section:**
**Explanation:**
The primary purpose of the Pilot Deployment in the Implementation phase is to validate the effectiveness of the solution design in the customer's environment. This stage is crucial for testing the solution in a real-world setting, allowing the implementation team to verify that the deployment meets the planned objectives.
Validation in Real-World Conditions: The Pilot Deployment tests how the solution performs under actual operating conditions, identifying any gaps or adjustments needed before full deployment.
Fine-Tuning the Solution: Feedback and performance metrics from the pilot help refine settings, policies, and configurations to ensure optimal security and usability.
User Acceptance Testing: This phase also allows end users and administrators to interact with the system, providing insights on usability and any necessary training or adjustments.
Explanation of Why Other Options Are Less Likely:
Option B (establishing communication paths) and Option D (setting account permissions) are preliminary tasks.
Option C (assigning tasks) is an administrative step that doesn't align with the primary testing purpose of the Pilot Deployment.
Thus, validating the effectiveness of the solution design is the primary goal of the Pilot Deployment.

**QUESTION 12**
Which two options are available when configuring DNS change detected for SONAR? (Select two.)

A. Block
B. Active Response
C. Quarantine
D. Log
E. Trace

**Correct Answer: A, D**
**Section:**
**Explanation:**
When configuring DNS change detection for SONAR, two available options are Block and Log. These options allow administrators to define how SONAR should respond to unexpected or suspicious DNS changes.
Block: This option enables SONAR to immediately block DNS changes that it detects as potentially malicious, preventing suspicious DNS redirections that could expose endpoints to threats like phishing or malware sites.
Log: Selecting Log allows SONAR to record DNS changes without taking direct action. This option is useful for monitoring purposes, providing a record of changes for further analysis.
Explanation of Why Other Options Are Less Likely:
Option B (Active Response) and Option C (Quarantine) are generally associated with threat responses but are not specific to DNS change detection.
Option E (Trace) is not an available response option for DNS changes in SONAR.
Therefore, the correct options for configuring DNS change detected for SONAR are Block and Log.

**QUESTION 13**
What should be done with the gathered business and technical objectives in the Assess phase?

A. List them and rank them by priority
B. Document them and proceed with the assessment of the solution
C. Discuss them with the IT staff only
D. Create a separate report for each objective

**Correct Answer: B**
**Section:**
**Explanation:**
In the Assess phase, the gathered business and technical objectives should be documented as they provide the foundation for assessing the solution's effectiveness and alignment with organizational goals.
Documenting Objectives: Proper documentation ensures that the objectives are clearly understood and preserved for reference throughout the implementation process, aligning all stakeholders on the expected outcomes.
Proceeding with the Assessment: Once documented, these objectives guide the evaluation of the solution's performance, identifying any areas that may require adjustments to meet the organization's needs.
Ensuring Traceability: Documented objectives offer traceability, allowing each stage of the implementation to reference back to these goals for consistent alignment.
Explanation of Why Other Options Are Less Likely:
Option A (ranking them) is useful but does not substitute the documentation and assessment process.
Option C (discussing only with IT staff) limits stakeholder involvement.
Option D (creating separate reports) is redundant and not typically required at this stage.
The correct approach is to document the objectives and proceed with the assessment of the solution's alignment with these goals.

**QUESTION 14**
What is the role of the Cloud Bridge Connector in the SES Complete Hybrid Architecture?

A. To manage all on-premise clients that connect to a SQL Server database through TCP Port 1443.
B. To synchronize communications between an on premise SEP Manager and the Integrated Cyber Security Manager securely over TCP port 443.
C. To offload the updating of agent and security content that communicate on TCP ports 7070 for HTTP traffic or 7078 for SSL traffic.
D. To provide content update to all engines building the protection stack on the SEP client.

**Correct Answer: B**
**Section:**
**Explanation:**
In the SES Complete Hybrid Architecture, the Cloud Bridge Connector serves a critical role in enabling secure communication between on-premise and cloud components:
Synchronization Role: The Cloud Bridge Connector allows the on-premise Symantec Endpoint Protection (SEP) Manager to securely communicate and synchronize data with the Integrated Cyber Security Manager in the cloud environment.
Secure Communication over TCP Port 443: The connector uses TCP port 443 for secure HTTPS communication, which is crucial for transmitting sensitive security data and maintaining synchronization between the on-premise and cloud environments.
Hybrid Architecture Support: This synchronization capability is essential in hybrid architectures, where a mix of on-premise and cloud resources work together to provide a cohesive security solution.

Explanation of Why Other Options Are Less Likely:
Option A (managing on-premise clients through SQL Server) is unrelated to the Cloud Bridge Connector's function.
Option C (offloading updates via TCP ports 7070 and 7078) pertains to update distribution, not synchronization.
Option D (providing content updates on the SEP client) is also outside the primary role of the Cloud Bridge Connector.
The correct answer is that the Cloud Bridge Connector is used to synchronize communications between the on-premise SEP Manager and the Integrated Cyber Security Manager over TCP port 443.

**QUESTION 15**
What does the Configuration Design section in the SES Complete Solution Design provide?

A. A summary of the features and functions to be implemented
B. A sequential list of testing scenarios in production environments
C. The validation of the SES complete solution
D. To review the base architecture and infrastructure requirements

**Correct Answer: A**
**Section:**
**Explanation:**
The Configuration Design section in the SES Complete Solution Design provides a summary of the features and functions that will be implemented in the deployment. This section outlines the specific elements that make up the security solution, detailing what will be configured to meet the customer's requirements.
Summary of Features and Functions: This section acts as a blueprint, summarizing the specific features (e.g., malware protection, firewall settings, intrusion prevention) and configurations that need to be deployed.
Guidance for Implementation: By listing the features and functions, the Configuration Design serves as a reference for administrators, guiding the deployment and ensuring all necessary components are included.
Ensuring Solution Completeness: The summary helps verify that the solution covers all planned security aspects, reducing the risk of missing critical configurations during deployment.
Explanation of Why Other Options Are Less Likely:
Option B (testing scenarios) is part of the Test Plan, not the Configuration Design.
Option C (solution validation) is conducted after configuration and is typically part of testing.
Option D (base architecture and infrastructure requirements) would be found in the Infrastructure Design section.
Therefore, the Configuration Design section provides a summary of the features and functions to be implemented.

**QUESTION 16**
Which two actions are completed in the Implement phase of the SES Complete Implementation framework? (Select two)

A. Presentation of the SES Complete Solution Proposal
B. Execution of a Pilot Deployment
C. Implementation of the Solution Configuration Design
D. Preparing a customized high-level project plan
E. Gathering of business drivers and technical requirements

**Correct Answer: B, C**
**Section:**
**Explanation:**
In the Implement phase of the SES Complete Implementation framework, two key actions are typically executed:
Execution of a Pilot Deployment: This action is crucial to test the solution in a controlled subset of the customer environment, ensuring that the solution design meets functional and security requirements before a full-scale rollout. The Pilot Deployment validates configurations and allows adjustments as needed based on real-world performance.
Implementation of the Solution Configuration Design: This involves setting up and configuring all aspects of the solution according to the predefined Solution Configuration Design. This step ensures that all features and functionalities are properly implemented, configured, and aligned with the solution's objectives.
Explanation of Why Other Options Are Less Likely:
Option A (presentation of the SES Complete Solution Proposal) and Option D (preparing a project plan) are tasks completed earlier in the planning phase.
Option E (gathering of business drivers and technical requirements) is part of the Assess phase, where requirements are collected and documented.

Thus, Pilot Deployment and Solution Configuration Design implementation are the correct actions for the Implement phase.

**QUESTION 17**
What is a reason to choose a single site design for a SEP on-premise architecture?

A. Geographic coverage
B. Legal constraints on log retention
C. Centralized reporting with no delay
D. Control over WAN usage

**Correct Answer: C**
**Section:**
**Explanation:**
A single site design in a SEP on-premise architecture is often chosen when centralized reporting without delay is a primary requirement. This design allows for real-time access to data and reports, as all data processing occurs within a single, centralized server environment.
Centralized Data Access: A single site design ensures that data is readily available without the delays that might occur with multi-site replication or distributed environments.
Efficient Reporting: With all logs, alerts, and reports centralized, administrators can quickly access real-time information, which is crucial for rapid response and monitoring.
Explanation of Why Other Options Are Less Likely:
Option A (geographic coverage) would typically favor a multi-site setup.
Option B (legal constraints on log retention) does not specifically benefit from a single site design.
Option D (control over WAN usage) is more relevant to distributed environments where WAN traffic management is necessary.
Therefore, centralized reporting with no delay is a key reason for opting for a single site design.

**QUESTION 18**
An organization has several remote locations with minimum bandwidth and would like to use a content distribution method that does NOT involve configuring an internal LiveUpdate server. What content distribution method should be utilized?

A. External LiveUpdate
B. Management Server
C. Intelligent Updater
D. Group Update Provider

**Correct Answer: D**
**Section:**
**Explanation:**
For an organization with remote locations and minimal bandwidth that wants a content distribution solution without configuring an internal LiveUpdate server, using a Group Update Provider (GUP) is the best choice.
Efficient Content Distribution: The GUP serves as a local distribution point within each remote location, reducing the need for each client to connect directly to the central management server for updates. This minimizes WAN bandwidth usage.
No Need for Internal LiveUpdate Server: The GUP can pull updates from the central SEP Manager and then distribute them to local clients, eliminating the need for a dedicated internal LiveUpdate server and optimizing bandwidth usage in remote locations.
Explanation of Why Other Options Are Less Likely:
Option A (External LiveUpdate) would involve each client connecting to Symantec's servers, which could strain bandwidth.
Option B (Management Server) directly distributing updates is less efficient for remote locations with limited bandwidth.
Option C (Intelligent Updater) is typically used for manual updates and is not practical for ongoing, automated content distribution.
Thus, the Group Update Provider is the optimal solution for remote locations with limited bandwidth that do not want to set up an internal LiveUpdate server.

**QUESTION 19**
What happens if a SEP Manager replication partner fails in a multi-site SEP Manager implementation?

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

**Correct Answer: A**
**Section:**
**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 20**
Why is it important to research the customer prior to arriving onsite?

A. To review the supporting documentation
B. To understand recent challenges
C. To align client expectations with consultant expectations
D. To understand the customer and connect their needs to the technology

**Correct Answer: D**
**Section:**
**Explanation:**
Researching the customer before arriving onsite is important to understand the customer's specific needs and how the technology can address those needs. This preparation enables the consultant to make relevant connections between the customer's unique environment and the capabilities of the SES solution.
Understanding Customer Needs: By researching the customer, consultants can gain insight into specific security challenges, organizational goals, and any unique requirements.
Tailoring the Approach: This understanding allows consultants to tailor their approach, present the technology in a way that aligns with the customer's needs, and ensure the solution is relevant to the customer's environment.
Building a Collaborative Relationship: Demonstrating knowledge of the customer's challenges and goals helps establish trust and shows that the consultant is invested in providing value.
Explanation of Why Other Options Are Less Likely:
Option A (reviewing documentation) and Option B (understanding recent challenges) are steps in preparation but do not encompass the full reason.
Option C (aligning expectations) is a part of understanding customer needs but is not the primary purpose.
The best answer is to understand the customer and connect their needs to the technology.

**QUESTION 21**
Which type of infrastructure does the analysis of SES Complete Infrastructure mostly apply to?

A. Cloud-based infrastructure
B. On-premise or Hybrid infrastructure
C. Virtual infrastructure
D. Mobile infrastructure

**Correct Answer: B**

**Section:**
**Explanation:**
The analysis of SES Complete Infrastructure primarily applies to on-premise or hybrid infrastructures. This is because SES Complete often integrates both on-premise SEP Managers and cloud components, particularly in hybrid setups.
On-Premise and Hybrid Complexity: These types of infrastructures involve both on-premise SEP Managers and cloud components, which require careful analysis to ensure proper configuration, security policies, and seamless integration.
Integration with Cloud Services: Hybrid infrastructures particularly benefit from SES Complete's capability to bridge on-premise and cloud environments, necessitating detailed analysis to optimize communication, security, and functionality.
Applicability to SES Complete's Architecture: The SES Complete solution is designed with flexibility to support both on-premise and cloud environments, with hybrid setups being common for organizations transitioning to cloud-based services.
Explanation of Why Other Options Are Less Likely:
Option A (Cloud-based) does not fully apply as SES Complete includes significant on-premise components in hybrid setups.
Option C (Virtual infrastructure) and Option D (Mobile infrastructure) may involve endpoint protection but do not specifically align with the full SES Complete infrastructure requirements.
Thus, the correct answer is on-premise or hybrid infrastructure.

**QUESTION 22**
Which feature is designed to reduce the attack surface by managing suspicious behaviors performed by trusted applications?

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

**Correct Answer: C**
**Section:**
**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 23**
What is the first phase of the SES Complete Implementation Framework?

A. Assess
B. Design
C. Operate
D. Transform

**Correct Answer: A**
**Section:**
**Explanation:**
The first phase of the SES Complete Implementation Framework is the Assess phase. This phase involves gathering information about the customer's environment, identifying business and technical requirements, and understanding the customer's security objectives.

Purpose of the Assess Phase: The goal is to fully understand the customer's needs, which guides the entire implementation process.
Foundation for Solution Design: This phase provides essential insights that shape the subsequent design and implementation stages, ensuring that the solution aligns with the customer's requirements.
Explanation of Why Other Options Are Less Likely:
Option B (Design) follows the Assess phase, where the gathered information is used to develop the solution.
Option C (Operate) and Option D (Transform) are later phases focusing on managing and evolving the solution post-deployment.
Thus, the Assess phase is the correct starting point in the SES Complete Implementation Framework.

**QUESTION 24**
Where can information about the validation of in-use features/functions be found during the Manage phase?

A. Solution Infrastructure Design
B. Solution Configuration Design
C. Test Plan
D. Business or Technical Objectives

**Correct Answer: C**
**Section:**
**Explanation:**
In the Manage phase, information about the validation of in-use features/functions can be found in the Test Plan. This document outlines the specific tests, criteria, and methods for verifying that the solution's features and functions are operating as expected.
Validation Purpose of the Test Plan: The Test Plan specifies the steps to validate that each configured feature is performing correctly and meeting the intended objectives.
Documentation of Test Results: It also includes documentation of results, which helps ensure that all features remain functional and aligned with requirements in the production environment.
Explanation of Why Other Options Are Less Likely:
Option A (Solution Infrastructure Design) and Option B (Solution Configuration Design) focus on setup and configuration rather than validation.
Option D (Business or Technical Objectives) are used for setting goals, not validating functionality.
The Test Plan is thus the correct source for information on validating in-use features/functions during the Manage phase.

**QUESTION 25**
Which two are policy types within the Symantec Endpoint Protection Manager? (Select two.)

A. Exceptions
B. Host Protection
C. Shared Insight
D. Intrusion Prevention
E. Process Control

**Correct Answer: A, D**
**Section:**
**Explanation:**
Within Symantec Endpoint Protection Manager (SEPM), Exceptions and Intrusion Prevention are two policy types that can be configured to manage endpoint security. Here's why these two are included:
Exceptions Policy: This policy type allows administrators to set exclusions for certain files, folders, or processes from being scanned or monitored, which is essential for optimizing performance and avoiding conflicts with trusted applications.
Intrusion Prevention Policy: This policy protects against network-based threats by detecting and blocking malicious traffic, playing a critical role in network security for endpoints.
Explanation of Why Other Options Are Less Likely:
Option B (Host Protection) and Option E (Process Control) are not recognized policy types in SEPM.
Option C (Shared Insight) refers to a technology within SEP that reduces scanning load, but it is not a policy type.
Thus, Exceptions and Intrusion Prevention are valid policy types within Symantec Endpoint Protection Manager.

**QUESTION 26**
What is the main focus when defining the adoption levels required for features in SE5 Complete?

A. Customer requirements
B. Technical specifications
C. Regulatory compliance
D. Competitor analysis

**Correct Answer: A**
**Section:**
**Explanation:**
The main focus when defining adoption levels required for features in SES Complete is on Customer requirements. This approach ensures that the deployment of security features aligns with the customer's specific needs and priorities.
Aligning with Business Needs: By focusing on customer requirements, adoption levels are set based on the security goals, operational needs, and the specific environment of the customer.
Tailored Implementation: Adoption levels vary depending on the organization's risk tolerance, technical landscape, and strategic goals. Meeting these unique requirements ensures maximum value from the solution.
Explanation of Why Other Options Are Less Likely:
Option B (Technical specifications) and Option C (Regulatory compliance) are considerations, but they support rather than define adoption levels.
Option D (Competitor analysis) is not typically relevant to adoption level decisions within an implementation framework.
Therefore, Customer requirements are the primary focus for defining adoption levels in SES Complete.

**QUESTION 27**
What is the final task during the project close-out meeting?

A. Acknowledge the team's achievements
B. Hand over final documentation
C. Obtain a formal sign-off of the engagement
D. Discuss outstanding support activity and incident details

**Correct Answer: C**
**Section:**
**Explanation:**
The final task during the project close-out meeting is to obtain a formal sign-off of the engagement. This step officially marks the completion of the project, confirming that all deliverables have been met to the customer's satisfaction.
Formal Closure: Obtaining sign-off provides a documented confirmation that the project has been delivered as agreed, closing the engagement formally and signifying mutual agreement on completion.
Transition to Support: Once sign-off is received, the customer is transitioned to standard support services, and the project team's responsibilities officially conclude.
Explanation of Why Other Options Are Less Likely:
Option A (acknowledging achievements) and Option D (discussing support activities) are valuable but do not finalize the project.
Option B (handing over documentation) is part of the wrap-up but does not formally close the engagement.
Therefore, obtaining a formal sign-off is the final and essential task to conclude the project close-out meeting.

**QUESTION 28**
Which term or expression is utilized when adversaries leverage existing tools in the environment?

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

**Correct Answer: A**
**Section:**
**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 29**
What are the two stages found in the Assess Phase?

A. Planning and Testing
B. Data Gathering and Implementation
C. Planning and Data Gathering
D. Execution and Review

**Correct Answer: C**
**Section:**
**Explanation:**
In the Assess Phase of the Symantec Endpoint Security Complete (SESC) Implementation Framework, two key stages are critical to establishing a thorough understanding of the environment and defining requirements. These stages are:
Planning: This initial stage involves creating a strategic approach to assess the organization's current security posture, defining objectives, and setting the scope for data collection. Planning is essential to ensure the following steps are organized and targeted to capture the necessary details about the current environment.
Data Gathering: This stage follows planning and includes actively collecting detailed information about the organization's infrastructure, endpoint configurations, network topology, and existing security policies. This information provides a foundational view of the environment, allowing for accurate identification of requirements and potential areas of improvement.
Reference in SES Complete Documentation highlight that successful execution of these stages results in a tailored security assessment that aligns with the specific needs and objectives of the organization. Detailed instructions and best practices for conducting these stages are covered in the Assessing the Customer Environment and Objectives section of the SES Complete Implementation Curriculum.

**QUESTION 30**
Which two criteria should an administrator use when defining Location Awareness for the Symantec Endpoint Protection (SEP) client? (Select two.)

A. NIC description
B. SEP domain
C. Geographic location
D. WINS server
E. Network Speed

**Correct Answer: A, D**
**Section:**
**Explanation:**

When defining Location Awareness for the Symantec Endpoint Protection (SEP) client, administrators should focus on criteria that can uniquely identify a network or environment characteristic to trigger specific policies. Two important criteria are:
NIC Description: This criterion allows SEP to detect which Network Interface Card (NIC) is in use, helping to determine whether the endpoint is connected to a trusted internal network or an external/untrusted network. NIC description is a straightforward attribute SEP can monitor to determine location.
WINS Server: By detecting the WINS (Windows Internet Name Service) server, SEP can identify whether the endpoint is within a specific network environment. WINS server settings are often unique to particular locations within an organization, aiding in policy application based on network location.
Reference in Symantec Endpoint Protection Documentation outline using such network and connection-specific criteria to optimize Location Awareness policies effectively. The Location Awareness Configuration Guide provides best practices for configuring SEP clients to adapt behavior based on network characteristics, ensuring enhanced security and appropriate access controls across different environments.

**QUESTION 31**
When a SEPM is enrolled in ICDm which policy can only be managed from the cloud?

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

**Correct Answer: B**
**Section:**
**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 32**
What is the purpose of using multiple domains in the Symantec Security cloud console?

A. To combine data across multiple domains
B. To prevent administrators from viewing or managing data in other domains
C. To manage multiple independent entities while keeping the data physically separate
D. To provide a common group of users with access to one or more Symantec cloud products

**Correct Answer: C**
**Section:**
**Explanation:**
In the Symantec Security Cloud Console, using multiple domains enables organizations to manage separate entities within a single environment while ensuring data isolation and independence. This structure is beneficial for organizations with distinct operational divisions, subsidiaries, or independent departments that require separate administrative controls and data boundaries.
Symantec Endpoint Security Documentation outlines how multiple domains help maintain data privacy and secure access management across entities, allowing each domain to operate independently without crossover, which ensures compliance with data segregation policies.

**QUESTION 33**
What is the purpose of the Pilot Deployment?

A. To assess the solution infrastructure design
B. To validate the proper implementation and operation of the SES Complete solution
C. To finalize the engagement

D. To obtain customer feedback

**Correct Answer: B**
**Section:**
**Explanation:**
The Pilot Deployment phase in Symantec Endpoint Security Complete (SES Complete) serves a critical purpose: it allows administrators to confirm that the solution is implemented correctly and operates as expected within a controlled environment. This phase is essential for testing policies, configurations, and real-world performance before a full-scale rollout, ensuring any adjustments needed are addressed in advance.
Reference in the SES Complete Implementation Curriculum discuss the Pilot Deployment as a vital validation step to ensure functionality aligns with design objectives, offering an opportunity to refine configurations and mitigate issues that could affect broader deployment success.

**QUESTION 34**
What does the Base Architecture section of the Infrastructure Design provide?

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

**Correct Answer: D**
**Section:**
**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 35**
Where can you validate the Cloud Enrollment configuration in the SEP manager?

A. Advanced Security page
B. Cloud Enrollment Screen
C. Heat map
D. Settings

**Correct Answer: B**
**Section:**
**Explanation:**
The Cloud Enrollment Screen within the SEP Manager is where administrators can validate the Cloud Enrollment configuration. This screen provides details about the current cloud enrollment status and any associated settings, allowing administrators to verify that the enrollment aligns with organizational policies and to troubleshoot any connectivity or setup issues.
Symantec Endpoint Protection Documentation notes that accessing the Cloud Enrollment Screen provides essential information to ensure proper integration between the SEP Manager and the cloud, facilitating a smooth transition to a cloud-managed environment.

**QUESTION 36**
What may be a compelling reason to go against technology best-practices in the SES Complete architecture?

A. To implement a decentralized management model
B. To observe SES Complete Component constraints

C. To understand the IT management team's distribution and their policies

D. To meet a compelling business requirement

**Correct Answer: D**
**Section:**
**Explanation:**
In certain situations, deviating from technology best practices in the SES Complete architecture may be justified to satisfy a compelling business requirement. These requirements could include specific compliance mandates, unique operational needs, or regulatory obligations that necessitate custom configurations or an unconventional approach to implementation. While best practices provide a robust foundation, they may need adjustment when critical business needs outweigh standard technology recommendations.
SES Complete Implementation Curriculum emphasizes the importance of aligning technology solutions with business goals, even if this occasionally requires tailored adjustments to the recommended architecture to fulfill essential business objectives.

**QUESTION 37**
What must be done immediately after the Microsoft SQL Database is restored for a SEP Manager?

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

**Correct Answer: A**
**Section:**
**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 38**
Which SES Complete Solution Design section contains information about the topology of SE5 components, SQL databases, network communications, and management roles?

A. Solution Infrastructure Design

B. Solution Configuration Design

C. Test Plan

D. Business or Technical Objectives

**Correct Answer: A**
**Section:**
**Explanation:**
The Solution Infrastructure Design section in the SES Complete Solution Design encompasses critical details about the topology of SE5 components, SQL databases, network communications, and management roles. This section provides an in-depth architectural overview, specifying how components are interconnected, the placement and configuration of SQL databases, and the roles involved in managing and maintaining the infrastructure. This comprehensive outline supports a robust design that meets both operational and security needs.
Reference in SES Complete Documentation outline Solution Infrastructure Design as a foundational section for defining the technical infrastructure and communications setup, ensuring that each component is optimally placed and configured.

**QUESTION 39**
Who should be consulted to uncover the current corporate objectives and requirements in the Manage phase?

A. Security Operations
B. Technical Leadership
C. Business Leads
D. Network Operations

**Correct Answer: C**
**Section:**
**Explanation:**
In the Manage phase of the SES Complete implementation, consulting Business Leads is crucial to uncover and align with the current corporate objectives and requirements. Business Leads provide insight into organizational goals, compliance needs, and strategic priorities, which help inform the ongoing management and potential adjustments of the SES solution. Engaging with Business Leads ensures that security measures support the broader business framework and objectives.
SES Complete Implementation Curriculum highlights the importance of involving Business Leads during the Manage phase to ensure that the security solution continues to align with evolving business needs and strategic directions.

**QUESTION 40**
What happens when a device fails a Host Integrity check?

A. An antimalware scan is initiated
B. An administrative notification is logged
C. The device is restarted
D. The device is quarantined

**Correct Answer: D**
**Section:**
**Explanation:**

When a device fails a Host Integrity check in SES Complete, it is typically quarantined. Quarantine actions are designed to isolate non-compliant or potentially compromised devices to prevent them from interacting with the broader network. This isolation allows administrators to address and remediate the device's compliance issues before it regains full access. The quarantine process is a fundamental security measure within SES to enforce policy compliance and protect network integrity.
Reference in Symantec Endpoint Protection Documentation emphasize quarantine as a primary response to failed Host Integrity checks, helping to contain potential security risks effectively.

**QUESTION 41**
What is the first step taken when defining the core security/protection requirements in the Assess phase?

A. Start with the high-level questions and pain points
B. Immediately propose a solution
C. Archive data from the Pre-Engagement Questionnaire
D. Avoid understanding the customer's needs

**Correct Answer: A**
**Section:**
**Explanation:**
The first step in defining core security and protection requirements during the Assess phase is to start with high-level questions and pain points. This approach helps clarify the customer's key concerns, primary risks, and specific protection needs, providing a foundation to tailor the security solution effectively. By focusing on these high-level issues, the assessment can be aligned with the customer's unique environment and strategic objectives.
SES Complete Implementation Curriculum outlines this initial step as critical for gathering relevant information that shapes the direction of the security solution, ensuring it addresses the customer's main pain points and requirements comprehensively.

**QUESTION 42**

What is the purpose of LiveUpdate Administrator (LUA) Servers in Symantec Endpoint Security implementations?

A. To download content directly to the clients from the cloud console
B. To offload the updating of agent and security content
C. To distribute policy content to other peers in the network
D. To provide failover support for event updates

**Correct Answer: B**
**Section:**
**Explanation:**
The purpose of LiveUpdate Administrator (LUA) Servers in Symantec Endpoint Security implementations is to offload the updating of agent and security content from the primary management servers. LUA servers download updates and content (such as virus definitions and security patches) from Symantec's cloud, then distribute them to endpoints within the network. This approach reduces bandwidth and load on the management server, improving overall efficiency in environments with large or distributed endpoint populations.
Symantec Endpoint Protection Documentation describes LUA as an essential component for managing content updates in complex network environments, particularly those requiring optimized bandwidth and centralized update control.

**QUESTION 43**
What is the purpose of the Internal Planning Call in the Planning Stage of the Assess phase?

A. To review recent challenges
B. To discuss critical items
C. To gather customer information
D. To align client expectations with consultant expectations

**Correct Answer: D**
**Section:**
**Explanation:**
The purpose of the Internal Planning Call in the Planning Stage of the Assess phase is to align client expectations with consultant expectations. This alignment is essential to ensure that both the consulting team and the client have a mutual understanding of project goals, deliverables, timelines, and potential constraints. Setting clear expectations minimizes misunderstandings and provides a foundation for a successful engagement by confirming that the scope and objectives are fully understood by all parties.
SES Complete Implementation Curriculum highlights the importance of this step for establishing a collaborative and transparent working relationship, thereby enhancing the effectiveness of the subsequent phases of the implementation.

**QUESTION 44**
What should an administrator know regarding the differences between a Domain and a Tenant in ICDm?

A. A domain can contain multiple tenants
B. A tenant can contain multiple domains
C. Each customer can have one tenant and no domains
D. Each customer can have one domain and many tenants

**Correct Answer: B**
**Section:**
**Explanation:**
In the context of Integrated Cyber Defense Manager (ICDm), a tenant is the overarching container that can include multiple domains within it. Each tenant represents a unique customer or organization within ICDm, while domains allow for further subdivision within that tenant. This structure enables large organizations to segregate data, policies, and management within a single tenant based on different operational or geographical needs, while still keeping everything organized under one tenant entity.
Symantec Endpoint Security Documentation describes tenants as the primary unit of organizational hierarchy in ICDm, with domains serving as subdivisions within each tenant for flexible management.

**QUESTION 45**
What is the purpose of a Threat Defense for Active Directory Deceptive Account?

A. It exposes attackers as they seek to gather credential information from workstation memory
B. It acts as a honeypot to expose attackers as they attempt build their AD treasure map
C. It prevents attackers from reading the contents of the Domain Admins Group
D. It assigns a fake NTLM password hash value for users with an assigned AdminCount attribute.

**Correct Answer: A**
**Section:**
**Explanation:**
The purpose of a Threat Defense for Active Directory Deceptive Account is to expose attackers as they attempt to gather credential information from workstation memory. These deceptive accounts are crafted to resemble legitimate credentials but are, in fact, traps that alert administrators to malicious activity. When an attacker attempts to access these deceptive credentials, it indicates potential unauthorized efforts to harvest credentials, allowing security teams to detect and respond to these intrusions proactively.
SES Complete Documentation explains the use of deceptive accounts as part of a proactive defense strategy, where false credentials are seeded in vulnerable areas to catch and track attacker movements within the network.

**QUESTION 46**
What is the next step after implementing the SES Complete Base architecture in the Implement phase?

A. Implement the Logical Design
B. Sign into Symantec Security Cloud page
C. Create administrative accounts
D. Endpoint Enrollment and Distribution

**Correct Answer: D**
**Section:**
**Explanation:**
After implementing the SES Complete Base Architecture in the Implement phase, the next crucial step is Endpoint Enrollment and Distribution. This step involves enrolling endpoint devices into the security environment and distributing the necessary security agents across the devices. Proper enrollment and distribution ensure that endpoints are registered, policies are applied, and they begin receiving protection under the SES Complete solution.
SES Complete Implementation Curriculum explains this as a structured process following the base architecture setup to bring endpoints under management, enabling full policy enforcement and threat protection capabilities.

**QUESTION 47**
What is the purpose of evaluating default or custom Device/Policy Groups in the Manage Phase?

A. To understand how resources are managed and assigned
B. To validate replication between sites
C. To analyze the Solution Test Plan
D. To validate Content Delivery configuration

**Correct Answer: A**
**Section:**
**Explanation:**
In the Manage Phase, evaluating default or custom Device/Policy Groups is critical to understand how resources are managed and assigned. This evaluation helps administrators verify that resources and policies are properly aligned with organizational structures and that devices are correctly grouped according to policy needs and security requirements. This understanding ensures optimal management, resource allocation, and policy application across different groups.
Symantec Endpoint Security Documentation suggests regularly reviewing and adjusting these groups to keep the solution aligned with any organizational changes or new security needs, ensuring efficient management of endpoints and policies.

**QUESTION 48**
What does the Design phase of the SESC Implementation Framework include?

A. Creation of a SES Complete Solution Design
B. Creation of a SES Complete Solution Proposal
C. Assessing the base architecture and infrastructure requirements
D. Implementation of the pilot deployment of the Solution

**Correct Answer: A**
**Section:**
**Explanation:**
The Design phase in the SESC Implementation Framework includes the creation of a SES Complete Solution Design. This design document details the architectural plan for deploying SES Complete, including component layout, communication flows, security policies, and configurations. The Solution Design serves as a blueprint that guides the subsequent phases of implementation, ensuring that the deployment aligns with both technical requirements and business objectives.
SES Complete Implementation Curriculum outlines the Solution Design as a critical deliverable of the Design phase, providing a comprehensive, structured plan that directs the implementation and ensures all security and operational needs are met.

**QUESTION 49**
What is the first step that must be executed before creating the base architecture for a cloud-based implementation?

A. Create administrative accounts
B. Sign into Symantec Security Cloud page
C. Create new production domains
D. Review both cloud and on-premise architectures

**Correct Answer: B**
**Section:**
**Explanation:**
Before creating the base architecture for a cloud-based implementation of SES Complete, the first step is to sign into the Symantec Security Cloud page. Accessing this page is essential as it serves as the central hub for managing and configuring cloud-based elements of the solution, allowing administrators to set up the required environment and configurations for the base architecture.
Symantec Endpoint Security Documentation outlines this step as foundational for initiating a cloud-based implementation, enabling the administrator to access and configure the necessary cloud resources.

**QUESTION 50**
What is one of the objectives of the Design phase in the SES Complete Implementation Framework?

A. Develop the Solution Configuration Design
B. Gather customer requirements
C. Create the SES Complete Solution Proposal
D. Conduct customer training sessions

**Correct Answer: A**
**Section:**
**Explanation:**
One of the primary objectives of the Design phase in the SES Complete Implementation Framework is to develop the Solution Configuration Design. This design includes specific configurations, policy settings, and parameters that customize the SES Complete solution to meet the unique security needs and operational requirements of the organization. The Solution Configuration Design complements the Solution Infrastructure Design, providing a detailed plan for implementation.
SES Complete Implementation Curriculum emphasizes that creating the Solution Configuration Design is integral to the Design phase, as it ensures that all configuration aspects are thoroughly planned before deployment.

**QUESTION 51**
What is the main focus of the 'Lessons' agenda item in a project close-out meeting?

A. Gathering insights and deriving practical lessons from the project
B. Discussing the next steps and any possible outstanding project actions
C. Confirming project closure with all stakeholders
D. Acknowledging the team's achievements

**Correct Answer: A**
**Section:**
**Explanation:**
In the project close-out meeting, the main focus of the 'Lessons' agenda item is to gather insights and derive practical lessons from the project. This discussion helps the team identify what went well, what challenges were faced, and how similar projects might be improved in the future. Documenting these lessons is valuable for continuous improvement and knowledge-sharing within the organization.
SES Complete Implementation Framework suggests that capturing lessons learned during the close-out is essential for refining processes and enhancing the success of future implementations, reinforcing best practices and avoiding previous pitfalls.

**QUESTION 52**
What is the Integrated Cyber Defense Manager (ICDm) used for?

A. To manage cloud-based endpoints only
B. To manage on-premises endpoints only
C. To manage cloud-based and hybrid endpoints
D. To manage network-based security controls

**Correct Answer: C**
**Section:**
**Explanation:**
The Integrated Cyber Defense Manager (ICDm) is used to manage both cloud-based and hybrid endpoints within the Symantec Endpoint Security environment. ICDm serves as a unified console, enabling administrators to oversee endpoint security configurations, policies, and events across both fully cloud-hosted and hybrid environments, where on-premises and cloud components coexist. This integrated approach enhances visibility and simplifies management across diverse deployment types.
Symantec Endpoint Security Documentation highlights ICDm's role in providing centralized management for comprehensive endpoint security, whether the endpoints are cloud-based or part of a hybrid architecture.

**QUESTION 53**
What is the first step to permanently convert SEP Manager-managed groups and policies to cloud-managed groups and policies?

A. Run the Switch Group to Cloud Managed command from the cloud console
B. Verify that the groups moved from under the My Company parent group to the Default parent group
C. Recreate device groups based on how you organize your endpoints
D. Install a package from Symantec Endpoint Security

**Correct Answer: A**
**Section:**
**Explanation:**
The first step to permanently convert SEP Manager-managed groups and policies to cloud-managed ones is to run the Switch Group to Cloud Managed command from the cloud console. This command initiates the transfer process, allowing groups and policies previously managed on-premises by the SEP Manager to be controlled through the cloud interface. This step is crucial for migrating management responsibilities to the cloud, aligning with cloud-managed infrastructure practices.
Reference in SES Complete Documentation emphasize the importance of this command as the initial action in transitioning groups and policies to cloud management, facilitating a smooth migration to a fully cloud-based management approach.

**QUESTION 54**
What are the main phases within the Symantec SES Complete implementation Framework?

A. Assess, Design, Implement, Manage
B. Plan, Execute, Review, Improve
C. Gather, Analyze, Implement, Evaluate
D. Assess, Plan, Deploy, Monitor

**Correct Answer: A**
**Section:**
**Explanation:**
The main phases within the Symantec SES Complete Implementation Framework are Assess, Design, Implement, and Manage. Each phase represents a critical step in the SES Complete deployment process:
Assess: Understand the current environment, gather requirements, and identify security needs.
Design: Develop the Solution Design and Configuration to address the identified needs.
Implement: Deploy and configure the solution based on the designed plan.
Manage: Ongoing management, monitoring, and optimization of the deployed solution.
These phases provide a structured methodology for implementing SES Complete effectively, ensuring that each step aligns with organizational objectives and security requirements.
SES Complete Implementation Curriculum outlines these phases as core components for a successful deployment and management lifecycle of the SES Complete solution.

**QUESTION 55**
Which section of the SES Complete Solution Design provides a summary of the features and functions to be implemented?

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

**Correct Answer: D**
**Section:**
**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.

**QUESTION 56**
What does the Integrated Cyber Defense Manager (ICDm) create automatically based on the customer's physical address?

A. Sub-workspaces
B. Tenants
C. Domains
D. LiveUpdate servers

**Correct Answer: C**
**Section:**
**Explanation:**
The Integrated Cyber Defense Manager (ICDm) automatically creates domains based on the customer's physical address. This automated domain creation helps organize resources and manage policies according to geographic or operational boundaries, streamlining administrative processes and aligning with the customer's structure. Domains provide a logical division within the ICDm for managing security policies and configurations.
Symantec Endpoint Security Documentation describes this automatic domain setup as part of ICDm's organizational capabilities, enhancing resource management based on physical or regional distinctions.

**QUESTION 57**
What is the importance of utilizing Engagement Management concepts?

A. To review recent challenges
B. To drive success throughout the engagement
C. To align client expectations with consultant expectations
D. To discuss critical items

**Correct Answer: B**
**Section:**
**Explanation:**
Utilizing Engagement Management concepts is crucial to drive success throughout the engagement. These concepts ensure that the project maintains a clear focus on goals, timelines, and deliverables while also fostering strong communication between the consulting team and the client. Engagement Management helps to mitigate risks, handle challenges proactively, and align project activities with the client's objectives, thereby contributing to a successful outcome.
SES Complete Implementation Curriculum emphasizes Engagement Management as a key factor in maintaining project momentum and achieving the desired results through structured and responsive project handling.

**QUESTION 58**
What does SES Complete offer customers in terms of deployment options?

A. Cloud-based only
B. On-premises only
C. Hybrid, cloud-based and on-premises
D. Hybrid or on-premises only

**Correct Answer: C**
**Section:**
**Explanation:**
SES Complete offers customers hybrid, cloud-based, and on-premises deployment options. This flexibility allows organizations to choose the deployment model that best aligns with their infrastructure, security policies, and operational needs. Hybrid deployment enables organizations to leverage both on-premises and cloud resources, while a fully cloud-based or solely on-premises model may be preferred based on specific requirements or regulatory considerations.
Symantec Endpoint Security Documentation details the deployment options to provide adaptability for diverse customer environments, enabling optimized security solutions regardless of the infrastructure.

**QUESTION 59**
What should be reviewed to understand how endpoints are being managed in the Manage phase?

A. Agent implementation and distribution processes
B. Site or Content Distribution Management mapping
C. Failover and Replication implementation
D. Organizational model mapping

**Correct Answer: D**
**Section:**
**Explanation:**
In the Manage phase, reviewing the Organizational model mapping is essential to understand how endpoints are being managed. This mapping provides insight into the hierarchical structure of device groups, policy application, and administrative roles within the SES Complete environment, ensuring that management practices are consistent with organizational policies and security requirements.
SES Complete Implementation Documentation advises reviewing the organizational model to verify that endpoints are organized effectively, which is critical for maintaining structured and compliant endpoint management.

**QUESTION 60**

What protection technologies should an administrator enable to protect against Ransomware attacks?

A. Firewall, Host Integrity, System Lockdown
B. IPS, SONAR, and Download Insight
C. IPS, Firewall, System Lockdown
D. SONAR, Firewall, Download Insight

**Correct Answer: B**
**Section:**
**Explanation:**
To protect against Ransomware attacks, an administrator should enable Intrusion Prevention System (IPS), SONAR (Symantec Online Network for Advanced Response), and Download Insight. These technologies collectively provide layered security against ransomware by blocking known exploits (IPS), detecting suspicious behaviors (SONAR), and analyzing downloaded files for potential threats (Download Insight), significantly reducing the risk of ransomware infections.
Symantec Endpoint Protection Documentation emphasizes the combination of IPS, SONAR, and Download Insight as essential components for ransomware protection due to their proactive and reactive threat detection capabilities.

**QUESTION 61**
What is the first step in implementing the Logical Design of an On-Premise infrastructure?

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

**Correct Answer: D**
**Section:**
**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 62**
What is the purpose of the High Availability and Disaster Recovery testing steps in the Infrastructure Test Plan?

A. To ensure that the communication paths between major components have been established
B. To ensure that the database, agent communication, and overall security protection is always available or can be restored in a failover scenario
C. To decide how the SESC Solution use cases will be available using the production environment
D. To obfuscate AD query results and reconnaissance attempts

**Correct Answer: B**
**Section:**
**Explanation:**
The purpose of High Availability and Disaster Recovery testing steps in the Infrastructure Test Plan is to ensure that the database, agent communication, and overall security protection is always available or can be restored in a failover scenario. This testing verifies that critical components of the SES Complete infrastructure can continue functioning or be rapidly recovered if an outage or failure occurs, thus maintaining continuity of security protections.
Symantec Endpoint Security Documentation emphasizes that High Availability and Disaster Recovery testing is essential for validating the resilience of the infrastructure, ensuring uninterrupted security operations.

**QUESTION 63**

What is the term used to describe the interval between the SEP Manager server and the managed client?

A. Check-ins
B. Heartbeats
C. Updates
D. Syncs

**Correct Answer: B**
**Section:**
**Explanation:**
In Symantec Endpoint Protection (SEP), the term 'Heartbeats' is used to describe the interval at which the SEP Manager server and the managed client communicate. The heartbeat interval dictates how frequently the client checks in with the server for updates, policy changes, and status reporting, making it a critical parameter for maintaining synchronization and timely updates.
Symantec Endpoint Protection Documentation refers to heartbeats as a central mechanism for managing client-server communications effectively, balancing network traffic with update needs.

**QUESTION 64**
What does a Group Update Provider (GUP) minimize?

A. Content requests
B. Content downloads
C. Content updates
D. Content validation

**Correct Answer: B**
**Section:**
**Explanation:**
A Group Update Provider (GUP) is used to minimize content downloads across the network. The GUP serves as a local distribution point for updates, allowing clients within the same group to download necessary content (such as virus definitions) from the GUP rather than directly from the SEP Manager. This reduces bandwidth usage and improves update efficiency, particularly in distributed or bandwidth-constrained environments.
Symantec Endpoint Protection Documentation explains that deploying GUPs helps reduce the load on central servers and minimizes network bandwidth consumption, optimizing content delivery in large networks.

**QUESTION 65**
What do technical objectives represent in the general IT environment?

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

**Correct Answer: A**
**Section:**
**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 66**
What is the focus of Active Directory Defense testing in the Test Plan?

A. Validating the Obfuscation Factor for AD Domain Settings

B. Testing the intensity level for Malware Prevention

C. Ensuring that Application Launch Rules are blocking or allowing application execution and behaviors on endpoints

D. Validating the protection against network threats for Network Integrity Configuration

**Correct Answer: C**
**Section:**
**Explanation:**
The focus of Active Directory Defense testing within the Test Plan involves validating endpoint protection mechanisms, particularly Application Launch Rules. This testing focuses on ensuring that only authorized applications are allowed to execute, and any risky or suspicious application behaviors are blocked, supporting Active Directory (AD) defenses against unauthorized access or malicious software activity. Here's how this is structured:
Application Launch Rules: These rules dictate which applications are permissible on endpoints and prevent unauthorized applications from executing. By configuring and testing these rules, organizations can defend AD resources by limiting attack vectors at the application level.
Endpoint Behavior Controls: Ensuring that endpoints follow AD policies is critical. The testing ensures that AD Defense mechanisms effectively control the behavior of applications and prevent them from deviating into risky operations or violating security policies.
Role in AD Defense: This specific testing supports AD Defense by focusing on application control measures that protect the integrity of the directory services.
Explanation of Why Other Options Are Less Likely:
Option A (Obfuscation Factor for AD Domain Settings) is not typically a focus in endpoint security testing.
Option B (intensity level for Malware Prevention) is relevant to threat prevention but not specifically related to AD defenses.
Option D (network threats for Network Integrity Configuration) focuses on network rather than AD defenses.
The Test Plan's focus in this area is on controlling application execution and behavior to safeguard Active Directory from unauthorized or risky applications.

**QUESTION 67**
What should be documented in the Infrastructure Design section to enable traffic redirection to Symantec servers?

A. Required ports and protocols

B. Hardware recommendations

C. Site Topology description

D. Disaster recovery plan

**Correct Answer: A**
**Section:**
**Explanation:**
In the Infrastructure Design section, documenting the required ports and protocols is essential for enabling traffic redirection to Symantec servers. This setup is necessary for allowing endpoints to communicate with Symantec's servers for updates, threat intelligence, and other cloud-based security services.
Traffic Redirection to Symantec Servers: For endpoints to interact with Symantec servers, specific network configurations must be in place. Listing the required ports (e.g., port 443 for HTTPS) and protocols ensures that traffic can flow seamlessly from the endpoint to the server.
Ensuring Compatibility and Connectivity: Documenting ports and protocols helps administrators verify that network configurations meet the security and operational requirements, facilitating proper communication and content updates.
Infrastructure Design Clarity: This documentation clarifies network requirements, allowing for easier troubleshooting and setup consistency across various sites within an organization.
Explanation of Why Other Options Are Less Likely:
Option B (Hardware recommendations), Option C (Site Topology description), and Option D (Disaster recovery plan) are important elements but do not directly impact traffic redirection to Symantec servers.
Thus, documenting required ports and protocols is critical in the Infrastructure Design for enabling effective traffic redirection.

**QUESTION 68**
In the case of cloud-based architecture, what should be indicated in the Base Architecture section of the SES Complete Solution Design?

A. The Tenant and domain structure

B. The major on-premise components

C. The replication and failover design

D. The Initial Test Plan

**Correct Answer: A**
**Section:**
**Explanation:**
In a cloud-based architecture for SES Complete, the Base Architecture section of the Solution Design should indicate the Tenant and domain structure. This structure outlines the organization of the cloud environment, defining how resources and policies are grouped and managed. Proper tenant and domain structuring is essential for managing user access, resource allocation, and policy enforcement effectively within a cloud deployment.
SES Complete Solution Design Documentation specifies the need to define tenant and domain structures as part of the Base Architecture to ensure clear organization and security policy management.

**QUESTION 69**
What does the Symantec Security Center provide to customers?

A. Security centric Information from Symantec experts

B. Access to instructor-led, virtual, web-based and certification offerings

C. Access to the latest product documentation

D. Access to the Symantec Communities platform

**Correct Answer: A**
**Section:**
**Explanation:**
The Symantec Security Center provides customers with security-centric information from Symantec experts. This platform offers insights, updates, and expert advice on the latest security threats, best practices, and strategies to enhance cybersecurity. It is a resource for organizations seeking guidance on evolving threats and how to manage them effectively using Symantec's solutions.
Symantec Endpoint Security Documentation highlights the Security Center as a valuable resource for receiving up-to-date security information and expert analysis, supporting informed decision-making in security management.

**QUESTION 70**
What does the Symantec Communities platform provide?

A. Access to professionals, experts, and enthusiasts to discuss, collaborate, and share knowledge

B. Access to the latest product documentation, downloads, and support information

C. Access to the My Entitlements list

D. Access to customer support incidents

**Correct Answer: A**
**Section:**
**Explanation:**
The Symantec Communities platform provides access to professionals, experts, and enthusiasts to discuss, collaborate, and share knowledge. This platform allows users to connect with others in the cybersecurity field to exchange insights, best practices, and solutions related to Symantec products. It fosters a collaborative environment where users can gain assistance, share experiences, and stay informed about the latest developments.
Symantec Endpoint Security Documentation describes the Symantec Communities as a collaborative forum beneficial for troubleshooting, networking, and expanding knowledge on cybersecurity topics and Symantec tools.

**QUESTION 71**
Which SES Complete use case represents the Pre-Attack phase in the attack chain sequence?

A. Reducing the Attack Surface

B. Ensuring Endpoints are Secured

C. Preventing Attacks from Reaching Endpoints

D. Hunting for Threats Across an Organization

**Correct Answer: A**
**Section:**
**Explanation:**
In SES Complete, the use case of Reducing the Attack Surface represents the Pre-Attack phase in the attack chain sequence. This phase involves implementing measures to minimize potential vulnerabilities and limit exposure to threats before an attack occurs. By reducing the attack surface, organizations can proactively defend against potential exploitation paths that attackers might leverage.
Symantec Endpoint Security Complete Documentation emphasizes that reducing the attack surface is a proactive strategy in the Pre-Attack phase, aimed at strengthening security posture and preventing attacks from finding entry points in the network.

**QUESTION 72**
Where can information about the adoption of SES Complete use cases and their respective settings be found?

A. Test Plan
B. Solution Infrastructure Design
C. Solution Configuration Design
D. Business or Technical Objectives

**Correct Answer: C**
**Section:**
**Explanation:**
The Solution Configuration Design contains information about the adoption of SES Complete use cases and their respective settings. This section details the configuration choices, policy settings, and operational parameters specific to each use case within SES Complete, tailored to the organization's security objectives and operational environment. It provides administrators with a roadmap for implementing use cases according to best practices and optimized configurations.
SES Complete Implementation Documentation emphasizes the Solution Configuration Design as the primary reference for aligning use case adoption with specific configuration settings, ensuring that security requirements are met efficiently.

**QUESTION 73**
In which two areas can host groups be used in a Symantec Endpoint Protection Manager (SEPM) implementation? (Select two.)

A. Application and Device Control
B. Firewall
C. Locations
D. IPS
E. Download Insight

**Correct Answer: B, D**
**Section:**
**Explanation:**
In a Symantec Endpoint Protection Manager (SEPM) implementation, host groups can be used within the Firewall and Intrusion Prevention System (IPS). Host groups allow administrators to define sets of IP addresses or domains that can be referenced in firewall and IPS policies, making it easier to apply consistent security controls across designated hosts or networks.
Symantec Endpoint Protection Documentation specifies the usage of host groups to streamline policy management, enabling efficient and organized rule application for network security measures within SEPM's Firewall and IPS configurations.

**QUESTION 74**
In addition to performance improvements, which two benefits does Insight provide? (Select two.)

A. Reputation scoring for documents
B. Zero-day threat detection

C. Protects against malicious Java scripts
D. False positive mitigation
E. Blocks malicious websites

**Correct Answer: A, D**
**Section:**
**Explanation:**
Beyond performance improvements, Symantec Insight provides two additional benefits: reputation scoring for documents and false positive mitigation. Insight leverages a vast database of file reputation data to score documents based on their likelihood of being malicious, which aids in accurate threat detection. Additionally, Insight reduces false positives by utilizing reputation information to distinguish between legitimate files and potentially harmful ones, thereby improving the accuracy of threat assessments.
Symantec Endpoint Security Documentation highlights Insight's role in enhancing both detection accuracy and reliability by mitigating false positives and providing reputation-based assessments that support proactive threat identification.

**QUESTION 75**
What is replicated by default when replication between SEP Managers is enabled?

A. Policies only
B. Policies and group structure but not configuration
C. Configuration only
D. Policies, group structure, and configuration

**Correct Answer: D**
**Section:**
**Explanation:**
When replication between SEP Managers is enabled, policies, group structure, and configuration are replicated by default. This replication ensures that multiple SEP Managers within an organization maintain consistent security policies, group setups, and management configurations, facilitating a unified security posture across different sites or geographic locations.
Symantec Endpoint Protection Documentation confirms that these elements are critical components of replication to maintain alignment across all SEP Managers, allowing for seamless policy enforcement and efficient administrative control.