IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **250-586**

Title : Endpoint Security Complete Implementation - Technical Specialist

Version : DEMO

1.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
Answer: C
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.

2.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
Answer: C
Explanation:
In the implementation phase of Symantec Endpoint Security Complete (SESC), the Test Plan is primarily designed to provide structured guidance on adopting and verifying the deployment of SES Complete within the customer's environment.

Here’s a step-by-step reasoning:
Purpose of the Test Plan: The Test Plan ensures that all security features and configurations are functioning as expected after deployment. It lays out testing procedures that verify that the solution meets the intended security objectives and is properly integrated with the customer’s infrastructure.
Adoption of SES Complete: This phase often includes evaluating how well SES Complete integrates into the customer's existing environment, addressing any issues, and making sure users and stakeholders are prepared for the transition.
Structured Testing During Implementation: The Test Plan is essential for testing and validating the solution’s capabilities before fully operationalizing it. This involves configuring, testing, and fine-tuning the solution to align with the customer’s security requirements and ensuring readiness for the next phase.
Explanation of Why Other Options Are Less Likely:
Option A refers to the broader solution design assessment, typically done during the design phase rather than in the implementation phase.
Option B is more aligned with post-implementation monitoring rather than guiding testing.
Option D (seeking approval for the next phase) relates to project management tasks outside the primary function of the Test Plan in this phase.
The purpose of the Test Plan is to act as a roadmap for adoption and testing, ensuring the SES Complete solution performs as required.

3.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
Answer: C
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.

4.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
Answer: A
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.

5.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
Answer: B
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.