VirtuLearn

TRUSTED, ACCURATE AND RELIABLE!

The most comprehensive IT certification preparation materials in the industry!

https://www.virtulearner.com
support@virtulearner.com

Broadcom

250-586

Endpoint Security Complete Implementation - Technical Specialist Exam

QUESTION: 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(s): 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.

QUESTION: 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(s): C

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

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

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

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

Explanation of Why Other Options Are Less Likely:

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

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

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

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

QUESTION: 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