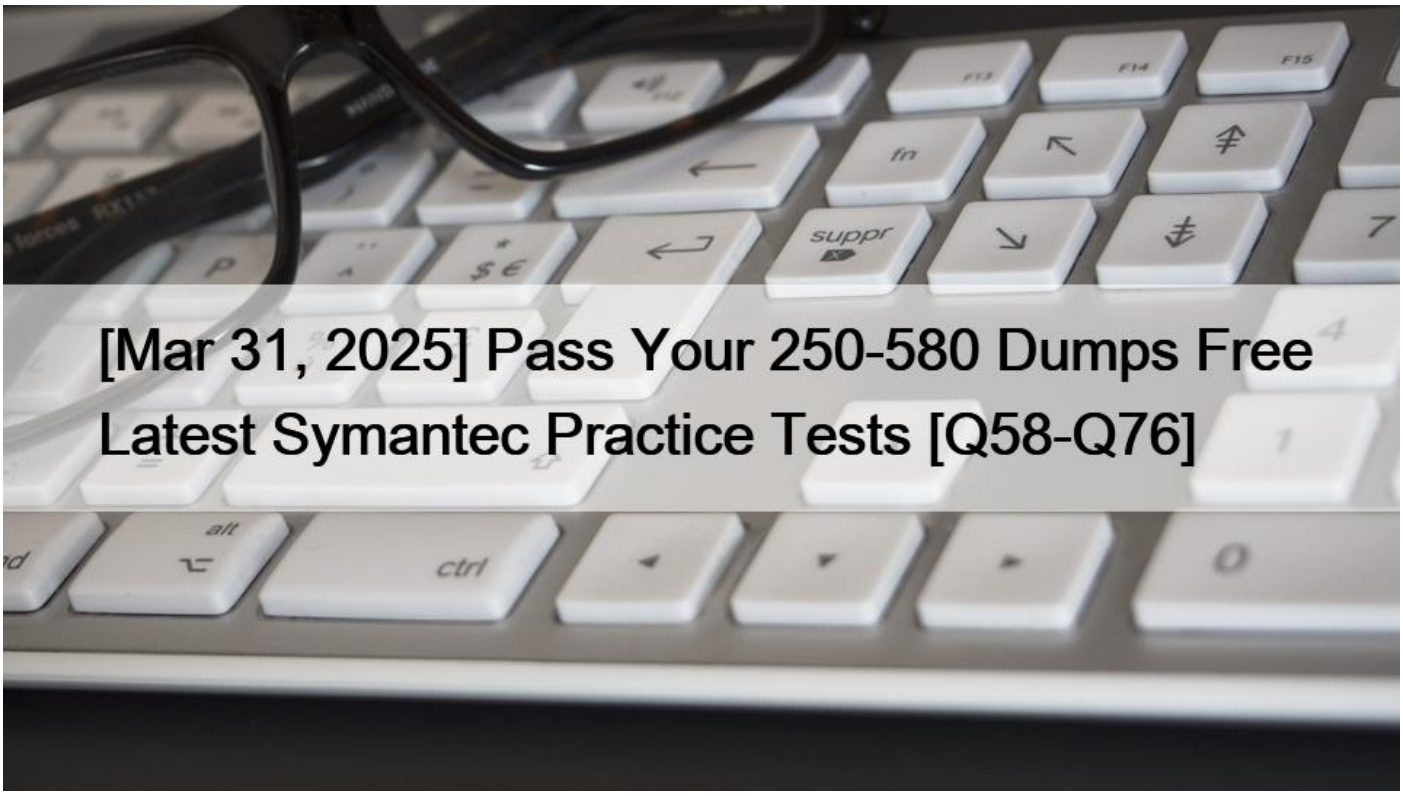
[Mar 31, 2025 Pass Your 250-580 Dumps Free Latest Symantec Practice Tests [Q58-Q76



[Mar 31, 2025] Pass Your 250-580 Dumps Free Latest Symantec Practice Tests
Get Top-Rated Symantec 250-580 Exam Dumps Now

Q58. Which security control runs at the packet level to inspect traffic for malicious communication patterns?
* Network Protection
* Intrusion Prevention
* Exploit Mitigation
* Firewall
TheIntrusion Prevention System (IPS)operates at thepacket levelto inspect traffic for malicious communication patterns. IPS analyzes network packets in real-time, identifying and blocking potentially harmful traffic based on predefined signatures and behavioral rules.

* How IPS Functions at the Packet Level:

* IPS inspects packets as they enter the network, comparing them against known attack signatures or patterns of suspicious behavior. This packet-level inspection helps prevent various attacks, such as SQL injection or cross-site scripting.

* Why Other Options Are Incorrect:

* Network Protection(Option A) is a broader category and not necessarily specific to packet inspection.

* Exploit Mitigation(Option C) focuses on preventing application exploits, not packet-level traffic analysis.

* Firewall(Option D) controls traffic flow based on rules but does not inspect packets for malicious patterns as comprehensively as IPS.

References: Intrusion Prevention provides essential packet-level protection in Symantec’s security framework, safeguarding against network-based attacks.

Q59. Administrators at a company share a single terminal for configuring Symantec Endpoint Protection. The administrators want to ensure that each administrator using the console is forced to authenticate using their individual credentials. They are concerned that administrators may forget to log off the terminal, which would easily allow others to gain access to the Symantec Endpoint Protection Manager (SEPM) console.

Which setting should the administrator disable to minimize the risk of non-authorized users logging into the SEPM console?
* Allow users to save credentials when logging on
* Delete clients that have not connected for specified time
* Lock account after the specified number of unsuccessful logon attempts
* Allow administrators to reset passwords
To reduce the risk of unauthorized access when administrators forget to log off, the setting”Allow users to save credentials when logging on”should be disabled in Symantec Endpoint Protection Manager (SEPM).

Disabling this option ensures that administrators are required to enter their credentials each time they access the SEPM console, preventing automatic logins and reducing the chance of someone else gaining access without permission.

* Purpose of Disabling Saved Credentials:

* By preventing credential saving, SEPM forces each administrator to authenticate manually on every session, thus improving security.

* This setting is particularly useful in shared environments, as it prevents the console from retaining login information when an administrator fails to log out.

* Why Other Options Are Less Relevant:

* Delete clients that have not connected(Option B) pertains to endpoint clients, not administrator logins.

* Lock account after unsuccessful attempts(Option C) protects against brute-force attempts but does not address saved credentials.

* Allow administrators to reset passwords(Option D) is related to password management rather than login persistence.

References: Disabling saved credentials is a best practice to enforce unique logins for each session, enhancing security in shared console environments.

Q60. A Symantec Endpoint Protection (SEP) client uses a management server list with three management servers in the priority 1 list.

Which mechanism does the SEP client use to select an alternate management server if the currently selected management server is unavailable?
* The client chooses another server in the list randomly.
* The client chooses a server based on the lowest server load.

* The client chooses a server with the next highest IP address.
* The client chooses the next server alphabetically by server name.

When aSymantec Endpoint Protection (SEP) clienthas multiplemanagement serverslisted in its priority 1 list and the currently selected management server becomes unavailable, the SEP clientrandomly selects another serverfrom the list. This randomized selection helps distribute load among the available servers and ensures continuity of management services.

* Mechanism of Random Selection:

* By choosing the next server randomly, SEP clients help balance the load across available servers, avoiding potential bottlenecks.

* This method also ensures that the client can quickly connect to an alternative server without requiring additional logic for server selection.

* Why Other Options Are Incorrect:

* SEP clients do not evaluateserver load(Option B), IP addresses (Option C), oralphabetical order (Option D) when selecting an alternate server.

References: The SEP client’s randomized approach to selecting management servers ensures efficient load distribution and server availability.

Q61. Which SES security control protects a user against data leakage if they encounter a man-in-the-middle attack?

* IPv6 Tunneling
* IPS
* Firewall
* VPN

TheIntrusion Prevention System (IPS)in Symantec Endpoint Security (SES) plays a crucial role in defending against data leakage during a man-in-the-middle (MITM) attack. Here’s how IPS protects in such scenarios:

* Threat Detection:IPS monitors network traffic in real-time, identifying and blocking suspicious patterns that could indicate an MITM attack, such as unauthorized access attempts or abnormal packet patterns.

* Prevention of Data Interception:By blocking these threats, IPS prevents malicious actors from intercepting or redirecting user data, thus safeguarding against data leakage.

* Automatic Response:IPS is designed to respond immediately, ensuring that attacks are detected and mitigated before sensitive data can be compromised.

By providing proactive protection, IPS ensures that data remains secure even in the face of potential MITM threats.

Q62. A company deploys Symantec Endpoint Protection (SEP) to 50 virtual machines running on a single ESXi host.

Which configuration change can the administrator make to minimize sudden IOPS impact on the ESXi server while each SEP endpoint communicates with the Symantec Endpoint Protection Manager?

* Increase the download Insight sensitivity level
* Reduce the heartbeat interval
* Increase the download randomization window
* Reduce the number of content revisions to keep

To minimize sudden IOPS impact on the ESXi server due toSEP endpoint communication, the administrator shouldincrease the download randomization window. This configuration change helps spread out the timing of SEP updates across virtual machines,

reducing the simultaneous I/O load on the server.

* Effect of Download Randomization:

* By increasing the randomization window, updates are downloaded at staggered intervals rather than all at once, lowering the burst IOPS demand.

* This is especially beneficial in virtualized environments where multiple VMs are hosted on a single ESXi server, as it prevents performance degradation from high IOPS activity.

* Why Other Options Are Less Effective:

* Increasing Download Insight sensitivity(Option A) has no impact on IOPS.

* Reducing the heartbeat interval(Option B) could increase communication frequency, potentially raising IOPS.

* Reducing content revisions(Option D) affects storage size but does not control update IOPS.

References: Increasing the download randomization window is a recommended practice in virtual environments to manage IOPS demands during SEP update cycles.

Q63. What version number is assigned to a duplicated policy?
* The original policy’s version number
* Zero
* The original policy’s number plus one
* One

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

References: This is consistent with SEP’s policy management approach, where versioning for duplicated policies starts anew at 1 to ensure clarity in tracking policy versions.

Q64. An administrator changes the Virus and Spyware Protection policy for a specific group that disables Auto- Protect. The administrator assigns the policy and the client systems apply the corresponding policy serial number. Upon visual inspection of a physical client system, the policy serial number is correct. However, Auto-Protect is still enabled on the client system.

Which action should the administrator take to ensure that the desired setting is in place for the client?
* Restart the client system
* Run a command on the computer to Update Content
* Enable the padlock next to the setting in the policy
* Withdraw the Virus and Spyware Protection policy

If an administrator modifies theVirus and Spyware Protection policyto disable Auto-Protect, but finds it still enabled on the client, the likely cause is that the setting was not locked. In Symantec EndpointProtection policies, enabling thepadlock iconnext to a setting ensures that the policy is enforced strictly, overriding local client configurations. Without this lock, clients may retain previous settings despite the new policy. Locking the setting guarantees that the desired configuration is applied consistently across all clients within the specified group.

Q65. What Symantec Best Practice is recommended when setting up Active Directory integration with the Symantec Endpoint

Protection Manager?
* Ensure there is more than one Active Directory Server listed in the Server Properties.
* Link the built-in Admin account to an Active Directory account.
* Import the existing AD structure to organize clients in user mode.
* Secure the management console by denying access to certain computers.
When setting up Active Directory (AD) integration with Symantec Endpoint Protection Manager (SEPM), Symantec’s best practice is toimport the existing AD structureto manage clients in user mode. This approach offers several benefits:

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

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

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

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

Q66. Which Symantec Endpoint Protection technology blocks a downloaded program from installing browser plugins?
* Intrusion Prevention
* SONAR
* Application and Device Control
* Tamper Protection
TheApplication and Device Controltechnology within Symantec Endpoint Protection (SEP) is responsible for blocking unauthorized software behaviors, such as preventing a downloaded program from installing browser plugins. This feature is designed to enforce policies that restrict specific actions by applications, which includes controlling program installation behaviors, access to certain system components, and interactions with browser settings. Application and Device Control effectively safeguards endpoints by stopping potentially unwanted or malicious modifications to the browser, thus protecting users from threats that may arise from unverified or harmful plugins.

Q67. What is the maximum number of SEPMs a single Management Platform is able to connect to?
* 50
* 10
* 5,000
* 500
Themaximum number of Symantec Endpoint Protection Managers (SEPMs)that a single Management Platform can connect to is50. This limit ensures that the management platform can handlecommunication, policy distribution, and reporting across connected SEPMs without overloading the system.

* Significance of the 50 SEPM Limit:

* This limitation is in place to ensure stable performance and effective management, especially in large-scale deployments where multiple SEPMs are required to support extensive environments.

* Relevance in Large Enterprises:

* Organizations managing endpoints across multiple locations often use several SEPMs, and the platform’s 50-manager limit allows scalability while maintaining centralized management.

References: The SEPM connection limits are documented as part of the architecture specifications for Symantec Endpoint Protection.

Q68. What account type must the AD Gateway Service Account be assigned to the AD Gateway device for AD Synchronization to function correctly?
* Local Standard
* Local Administrator
* Domain Administrator
* Domain User

ForAD Synchronizationto function correctly, theAD Gateway Service Accounton the AD Gateway device must be assigned as aDomain User. This role provides sufficient permissions to read Active Directory information for synchronization without requiring elevated privileges.

* Role of the Domain User Account:

* Domain User permissions allow the service account to access and synchronize necessary AD data, ensuring that the integration functions without unnecessary security risks associated with higher-level permissions.

* Why Other Account Types Are Not Suitable:

* Local StandardandLocal Administrator(Options A and B) do not have the required permissions for domain-wide AD access.

* Domain Administrator(Option C) provides excessive permissions, which are not needed for basic synchronization and could introduce unnecessary security risks.

References: Assigning the AD Gateway Service Account as a Domain User is a best practice for secure and functional AD synchronization in Symantec environments.

Q69. Which alert rule category includes events that are generated about the cloud console?
* Security
* System
* Diagnostic
* Application Activity

TheSystemalert rule category includesevents generated about the cloud console. These alerts relate to system-level activities within the management console, such as administrative actions, system health checks, and other essential notifications related to console operations.

* Types of Alerts in System Category:

* System alerts cover activities directly associated with the console and infrastructure, ensuring that administrators are informed of significant changes or issues affecting the management platform itself.

* Why Other Options Are Incorrect:

* Security(Option A) focuses on potential threats and security events.

* Diagnostic(Option C) involves troubleshooting information but does not specifically cover console events.

* Application Activity(Option D) pertains to application-specific events rather than console-level notifications.

References: System alerts provide visibility into cloud console-related events, crucial for managing and maintaining the console’s operational integrity.

Q70. The Behavioral Heat Map indicates that a specific application and a specific behavior are never used together.

What action can be safely set for the application behavior in a Behavioral Isolation policy?
* Deny
* Allow
* Delete
* Monitor

In Symantec EDR’s Behavioral Isolation policy, if theBehavioral Heat Mapindicates that a specific application and a particular behavior are never used together, setting the action toDenyfor that application behavior is a safe response. This prevents potential misuse by blocking the unusual behavior, which could indicate a security risk.

* Rationale for Denying the Behavior:

* If historical data shows that this behavior does not normally occur with the application, it suggests that any attempt to initiate it could be anomalous or malicious. Blocking this behavior helps prevent unexpected activities that could be exploited by threats.

* Why Other Actions Are Less Appropriate:

* Allow(Option B) would permit potentially risky behavior.

* Delete(Option C) does not apply in this context, as it is not an action for behavior control.

* Monitor(Option D) would only log the behavior but does not provide active protection, which is critical when the behavior is atypical.

References: Setting aDenyaction based on Behavioral Heat Map insights aligns with best practices for proactive threat prevention in Symantec EDR.

Q71. What prevention technique does Threat Defense for Active Directory use to expose attackers?
* Process Monitoring
* Obfuscation
* Honeypot Traps
* Packet Tracing

Threat Defense for Active Directory (TDAD) employsHoneypot Trapsas a primary prevention technique to detect and expose attackers. These honeypot traps act as decoys within the network, mimicking legitimate Active Directory (AD) objects or data that would attract attackers aiming to gather AD information or exploit AD weaknesses.

* Honeypot Trap Functionality:

* Honeypot traps are strategically placed to appear as appealing targets, such as privileged accounts or critical directories, without being part of the actual AD infrastructure.

* When attackers interact with these traps, TDAD records their actions, which can then trigger alerts, allowing administrators to identify and monitor suspicious activities.

* Exposure and Mitigation:

* By enticing attackers to interact with fake assets, honeypot traps help expose malicious intentions and techniques. This information can be used for forensic analysis and to enhance future defenses.

* This technique allows organizations to expose potential threats proactively, before any real AD resources are compromised.

References: This approach is part of Symantec’s Active Directory security strategies and utilizes honeypot mechanisms to deter and identify intruders in real-time.

Q72. What protection technology should an administrator enable to prevent double executable file names of ransomware variants like Cryptolocker from running?
* Download Insight
* Intrusion Prevention System
* SONAR
* Memory Exploit Mitigation

To prevent ransomware variants, such as Cryptolocker, from executing withdouble executable file names, an administrator should enableSONAR (Symantec Online Network for Advanced Response). SONAR detects and blocks suspicious behaviors based on file characteristics and real-time monitoring,which is effective in identifying malicious patterns associated with ransomware. By analyzing unusual behaviors, such as double executable file names, SONAR provides proactive protection against ransomware threats before they can cause harm to the system.

Q73. Which two (2) criteria are used by Symantec Insight to evaluate binary executables? (Select two.)
* Sensitivity
* Prevalence
* Confidentiality
* Content
* Age

Symantec Insight usesPrevalenceandAgeas two primary criteria to evaluate binary executables. These metrics help determine the likelihood that a file is either benign or malicious based on its behavior across a broad user base:

* Prevalence:This metric assesses how widely a file is used across Symantec’s global community. Files with higher prevalence are generally more likely to be safe, while rare files may pose higher risks.

* Age:The age of a file is also considered. Older files with a stable reputation are less likely to be malicious, whereas newer, unverified files are scrutinized more closely.

Using these criteria, Symantec Insight provides reliable reputation ratings for binary files, enhancing endpoint security by preemptively identifying potential threats.

Q74. Which two (2) considerations must an administrator make when enabling Application Learning in an environment? (Select two.)
* Application Learning can generate increased false positives.
* Application Learning should be deployed on a small group of systems in the enterprise.
* Application Learning can generate significant CPU or memory use on a Symantec Endpoint Protection Manager.
* Application Learning requires a file fingerprint list to be created in advance.
* E.Application Learning is dependent on Insight.

When enablingApplication Learningin Symantec Endpoint Protection (SEP), an administrator should consider the following:

* Increased False Positives:Application Learning may lead to increased false positives, as it identifies unfamiliar or rare applications that might not necessarily pose a threat.

* Pilot Deployment Recommended:To mitigate potential disruptions, Application Learning should initially be deployed on a small subset of systems. This approach allows administrators to observe its impact, refine policies, and control the learning data gathered before extending it across the entire enterprise.

These considerations help manage the resource impact and ensure the accuracy of Application Learning.

Q75. Which SEP feature is required for using the SEDR Isolate function?
* Host Isolation Policy
* Application Control
* Host Integrity Policy
* Application Detection

TheHost Integrity Policyin Symantec Endpoint Protection (SEP) is required for using theIsolate functionin Symantec Endpoint Detection and Response (SEDR). Host Integrity enables administrators to enforce security compliance on endpoints and is essential for isolation functions, ensuring that non-compliant or compromised systems are restricted from communicating with the network.

* How Host Integrity Policy Supports Isolation:

* By enforcing Host Integrity, SEP can ensure that endpoints adhere to security requirements before they are allowed network access, and if they do not comply, they can be isolated.

* This policy provides the framework that integrates with SEDR’s isolate function for responsive threat containment.

* Why Other Options Are Not Suitable:

* Host Isolation Policy(Option A) is not an actual SEP feature.

* Application Control(Option B) manages application behavior but is not tied to endpoint isolation.

* Application Detection(Option D) identifies applications but does not handle isolation.

References: The Host Integrity Policy in SEP is integral to implementing isolation capabilities in conjunction with SEDR.

Q76. Which designation should an administrator assign to the computer configured to find unmanaged devices?
* Discovery Device
* Discovery Manager
* Discovery Agent
* Discovery Broker

In Symantec Endpoint Protection, theDiscovery Agentdesignation is assigned to a computer responsible for identifying unmanaged devices within a network. This role is crucial for discovering endpoints that lack protection or are unmanaged, allowing the administrator to deploy agents or take appropriate action.

Configuring a Discovery Agent facilitates continuous monitoring and helps ensure that all devices on the network are recognized and managed.

Symantec 250-580 (Endpoint Security Complete - Administration R2) is an advanced certification exam that is designed for professionals who want to demonstrate their expertise in managing Symantec Endpoint Security Complete. 250-580 exam assesses the knowledge and skills of the candidates in areas such as endpoint security management, risk management, threat prevention, and incident response. Endpoint Security Complete - Administration R2 certification exam is ideal for IT professionals, system administrators, and security engineers who are responsible for managing endpoint security solutions in their organization.

Passing Key To Getting 250-580 Certified Exam Engine PDF: https://www.vceprep.com/250-580-latest-vce-prep.html]