Number: 250-580
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 250-580

Exam Name: Endpoint Security Complete - R2 Technical Specialist

Exam A

QUESTION 1
What information is required to calculate retention rate?

A. Number of endpoints, EAR data per endpoint per day, available disk space, number of endpoint dumps, dump size
B. Number of endpoints, available bandwidth, available disk space, number of endpoint dumps, dump size
C. Number of endpoints, available bandwidth, number of days to retain, number of endpoint dumps, dump size
D. Number of endpoints, EAR data per endpoint per day, number of days to retain, number of endpoint dumps, dump size

Correct Answer: D
Section:
Explanation:
To calculate the retention rate in Symantec Endpoint Security (SES), the following information is required:
Number of Endpoints: Determines the total scope of data generation.
EAR Data per Endpoint per Day: This is the Endpoint Activity Recorder data size generated daily by each endpoint.
Number of Days to Retain: Defines the retention period for data storage, impacting the total data volume.
Number of Endpoint Dumps and Dump Size: These parameters contribute to overall storage needs for log data and event tracking.
This data allows administrators to accurately project storage requirements and ensure adequate capacity for data retention.

QUESTION 2
Which two (2) scan range options are available to an administrator for locating unmanaged endpoints? (Select two)

A. Entire Network
B. IP range within the network
C. Subnet Range
D. IP range within the subnet
E. Entire Subnet

Correct Answer: B, C
Section:
Explanation:
For locating unmanaged endpoints, administrators in Symantec Endpoint Protection Manager (SEPM) can use the following scan range options:
IP Range within the Network: This option allows scanning of specific IP address ranges to locate devices that may not have SEP installed.
Subnet Range: Administrators can scan within specific subnets, providing a focused range to detect unmanaged endpoints in targeted sections of the network.
These options enable precise scans, helping administrators efficiently identify and manage unmanaged devices.

QUESTION 3
An organization has several Symantec Endpoint Protection Management (SEPM) Servers without access to the internet. The SEPM can only run LiveUpdate within a specified 'maintenance window' outside of business hours.
What content distribution method should the organization utilize?

A. JDB file
B. External LiveUpdate
C. Internal LiveUpdate
D. Group Update Provider

Correct Answer: A
Section:
Explanation:
For organizations with Symantec Endpoint Protection Manager (SEPM) servers that do not have internet access and require updates only within a specific maintenance window, the JDB file method is an effective solution:
Offline Content Distribution: JDB files can be downloaded on an internet-connected device and then manually transferred to SEPM, allowing it to update content offline.
Flexible Timing: Since JDB files can be applied during the maintenance window, this method adheres to time restrictions, avoiding disruption during business hours.
Using JDB files ensures that SEPM remains updated in environments with limited connectivity or strict operational schedules.

QUESTION 4
Which client log shows that a client is downloading content from its designated source?

A. Risk Log
B. System Log
C. SesmLu.log
D. Log.LiveUpdate

Correct Answer: D
Section:
Explanation:
The Log.LiveUpdate log shows details related to content downloads on a Symantec Endpoint Protection (SEP) client. This log captures the activities associated with updates, including:
Content Source Information: It records the source from which the client downloads updates, whether from SEPM, a Group Update Provider (GUP), or directly from the LiveUpdate server.
Download Progress and Status: This log helps administrators monitor successful or failed download attempts, along with version details of the downloaded content.
By reviewing the Log.LiveUpdate, administrators can verify if a client is correctly downloading content from its designated source.

QUESTION 5
Which antimalware intensity level is defined by the following: 'Blocks files that are most certainly bad or potentially bad files results in a comparable number of false positives and false negatives.'

A. Level 6
B. Level 5
C. Level 2
D. Level 1

Correct Answer: B
Section:
Explanation:
In antimalware solutions, Level 5 intensity is defined as a setting where the software blocks files that are considered either most certainly malicious or potentially malicious. This level aims to balance security with usability by erring on the side of caution; however, it acknowledges that some level of both false positives (legitimate files mistakenly flagged as threats) and false negatives (malicious files mistakenly deemed safe) may still occur.
This level is typically used in environments where security tolerance is high but with an understanding that some legitimate files might occasionally be flagged. It provides robust protection without the extreme strictness of the highest levels, thus reducing, but not eliminating, the possibility of false alerts while maintaining an aggressive security posture.

QUESTION 6
The SES Intrusion Prevention System has blocked an intruder's attempt to establish an IRC connection inside the firewall. Which Advanced Firewall Protection setting should an administrator enable to prevent the intruder's system from communicating with the network after the IPS detection?

A. Enable port scan detection
B. Automatically block an attacker's IP address
C. Block all traffic until the firewall starts and after the firewall stops
D. Enable denial of service detection

Correct Answer: B
Section:
Explanation:
To enhance security and prevent further attempts from the intruder after the Intrusion Prevention System (IPS) has detected and blocked an attack, the administrator should enable the setting to Automatically block an attacker's IP address. Here's why this setting is critical:
Immediate Action Against Threats: By automatically blocking the IP address of the detected attacker, the firewall can prevent any further communication attempts from that address. This helps to mitigate the risk of subsequent attacks or reconnections.
Proactive Defense Mechanism: Enabling this feature serves as a proactive defense strategy, minimizing the chances of successful future intrusions by making it harder for the attacker to re-establish a connection to the network.
Reduction of Administrative Overhead: Automating this response allows the security team to focus on investigating and remediating the incident rather than manually tracking and blocking malicious IP addresses, thus optimizing incident response workflows.
Layered Security Approach: This setting complements other security measures, such as intrusion detection and port scan detection, creating a layered security approach that enhances overall network security.
Enabling automatic blocking of an attacker's IP address directly addresses the immediate risk posed by the detected intrusion and reinforces the organization's defense posture against future threats.

QUESTION 7
After several failed logon attempts, the Symantec Endpoint Protection Manager (SEPM) has locked the default admin account. An administrator needs to make system changes as soon as possible to address an outbreak, but the admin account is the only account.
Which action should the administrator take to correct the problem with minimal impact on the existing environment?

A. Wait 15 minutes and attempt to log on again
B. Restore the SEPM from a backup
C. Run the Management Server and Configuration Wizard to reconfigure the server
D. Reinstall the SEPM

Correct Answer: A
Section:
Explanation:
In the situation where the default admin account of the Symantec Endpoint Protection Manager (SEPM) is locked after several failed login attempts, the best course of action for the administrator is to wait 15 minutes and attempt to log on again. Here's why this approach is advisable:
Account Lockout Policy: Most systems, including SEPM, are designed with account lockout policies that temporarily disable accounts after a number of failed login attempts. Typically, these policies include a reset time (often around 15 minutes), after which the account becomes active again.
Minimal Disruption: Waiting for the account to automatically unlock minimizes disruption to the existing environment. This avoids potentially complex recovery processes or the need to restore from a backup, which could introduce additional complications or data loss.
Avoiding System Changes: Taking actions such as restoring the SEPM from a backup, reconfiguring the server, or reinstalling could lead to significant changes in the configuration and might cause further complications, especially if immediate action is needed to address an outbreak.
Prioritizing Response to Threats: While it's important to respond to security incidents quickly, maintaining the integrity of the SEPM configuration and ensuring a smooth recovery is also crucial. Waiting for the lockout period respects the system's security protocols and allows the administrator to regain access with minimal risk.
In summary, waiting for the lockout to expire is the most straightforward and least disruptive solution, allowing the administrator to resume critical functions without unnecessary risk to the SEPM environment.

QUESTION 8
Which Incident View widget shows the parent-child relationship of related security events?

A. The Incident Summary Widget
B. The Process Lineage Widget
C. The Events Widget
D. The Incident Graph Widget

Correct Answer: B
Section:

Explanation:
The Process Lineage Widget in the Incident View of Symantec Endpoint Security provides a visual representation of the parent-child relationship among related security events, such as processes or activities stemming from a primary malicious action. This widget is valuable for tracing the origins and propagation paths of potential threats within a system, allowing security teams to identify the initial process that triggered subsequent actions. By displaying this hierarchical relationship, the Process Lineage Widget supports in-depth forensic analysis, helping administrators understand how an incident unfolded and assess the impact of each related security event in context.

QUESTION 9
Which Symantec Endpoint Protection technology blocks a downloaded program from installing browser plugins?

A. Intrusion Prevention
B. SONAR
C. Application and Device Control
D. Tamper Protection

Correct Answer: C
Section:
Explanation:
The Application and Device Control technology 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.

QUESTION 10
Which type of event does operation:1 indicate in a SEDR database search?

A. File Deleted.
B. File Closed.
C. File Open.
D. File Created.

Correct Answer: C
Section:
Explanation:
In a Symantec Endpoint Detection and Response (SEDR) database search, an event labeled with operation:1 corresponds to a File Open action. This identifier is part of SEDR's internal operation codes used to log file interactions. When querying or analyzing events in the SEDR database, recognizing this code helps Incident Responders understand that the action recorded was an attempt to access or open a file on the endpoint, which may be relevant in tracking suspicious or malicious activities.

QUESTION 11
An Incident Responder has determined that an endpoint is compromised by a malicious threat. What SEDR feature would be utilized first to contain the threat?

A. File Deletion
B. Incident Manager
C. Isolation
D. Endpoint Activity Recorder

Correct Answer: C
Section:
Explanation:

When an Incident Responder determines that an endpoint is compromised, the first action to contain the threat is to use the Isolation feature in Symantec Endpoint Detection and Response (SEDR). Isolation effectively disconnects the affected endpoint from the network, thereby preventing the malicious threat from communicating with other systems or spreading within the network environment. This feature enables the responder to contain the threat swiftly, allowing further investigation and remediation steps to be conducted without risk of lateral movement by the attacker.

QUESTION 12
If an administrator enables the setting to manage policies from the cloud, what steps must be taken to reverse this process?

A. Navigate to ICDm > Enrollment and disable the setting
B. Unenroll the SEPM > Disable the setting > Re-enroll the SEPM
C. Revoke policies from ICDm
D. Revoke policies from SEPM

Correct Answer: B
Section:
Explanation:
If an administrator has enabled the setting to manage policies from the cloud and needs to reverse this, they must follow these steps:
Unenroll the SEPM (Symantec Endpoint Protection Manager) from the cloud management (ICDm).
Disable the cloud policy management setting within the SEPM.
Re-enroll the SEPM back into the cloud if required.
This process ensures that policy control is reverted from cloud management to local management on the SEPM. By following these steps, administrators restore full local control over policies, disabling any cloud-based management settings previously in effect.

QUESTION 13
How would an administrator specify which remote consoles and servers have access to the management server?

A. Edit the Server Properties and under the General tab, change the Server Communication Permission.
B. Edit the Communication Settings for the Group under the Clients tab.
C. Edit the External Communication Settings for the Group under the Clients tab.
D. Edit the Site Properties and under the General tab, change the server priority.

Correct Answer: A
Section:
Explanation:
To control which remote consoles and servers have access to the Symantec Endpoint Protection Management (SEPM) server, an administrator should edit the Server Properties and adjust the Server Communication Permission under the General tab. This setting specifies which remote systems are authorized to communicate with the management server, enhancing security by limiting access to trusted consoles and servers only. Adjusting the Server Communication Permission helps manage server access centrally and ensures only approved systems interact with the management server.

QUESTION 14
Which designation should an administrator assign to the computer configured to find unmanaged devices?

A. Discovery Device
B. Discovery Manager
C. Discovery Agent
D. Discovery Broker

Correct Answer: C
Section:
Explanation:

In Symantec Endpoint Protection, the Discovery Agent designation 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.

QUESTION 15
An administrator notices that some entries list that the Risk was partially removed. The administrator needs to determine whether additional steps are necessary to remediate the threat.
Where in the Symantec Endpoint Protection Manager console can the administrator find additional information on the risk?

A. Risk log
B. Computer Status report
C. Notifications
D. Infected and At-Risk Computers report

Correct Answer: A
Section:
Explanation:
To gather more details about threats that were only partially removed, an administrator should consult the Risk log in the Symantec Endpoint Protection Manager (SEPM) console. The Risk log provides comprehensive information about detected threats, their removal status, and any remediation actions taken. By examining these logs, the administrator can determine if additional steps are required to fully mitigate the threat, ensuring that the endpoint is entirely secure and free of residual risks.

QUESTION 16
Which Endpoint Setting should an administrator utilize to locate unmanaged endpoints on a network subnet?

A. Device Discovery
B. Endpoint Enrollment
C. Discover and Deploy
D. Discover Endpoints

Correct Answer: C
Section:
Explanation:
To locate unmanaged endpoints within a specific network subnet, an administrator should utilize the Discover and Deploy setting. This feature scans the network for endpoints without security management, enabling administrators to identify and initiate the deployment of Symantec Endpoint Protection agents on unmanaged devices. This proactive approach ensures comprehensive coverage across the network, allowing for efficient detection and management of all endpoints within the organization.

QUESTION 17
Why is it important for an Incident Responder to copy malicious files to the SEDR file store or create an image of the infected system during the Recovery phase?

A. To create custom IPS signatures
B. To test the effectiveness of the current assigned policy settings in the Symantec Endpoint Protection Manager (SEPM)
C. To have a copy of the file for policy enforcement
D. To document and preserve any pieces of evidence associated with the incident

Correct Answer: D
Section:
Explanation:
During the Recovery phase of an incident response, it is critical for an Incident Responder to copy malicious files to the SEDR file store or create an image of the infected system. This action preserves evidence associated with the incident, allowing for thorough investigation and analysis. By securing a copy of the malicious files or system state, responders maintain a record of the incident that can be analyzed for root cause assessment, used for

potential legal proceedings, or retained for post-incident review. Documenting and preserving evidence ensures that key information is available for future reference or audits.

QUESTION 18
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?

A. Restart the client system
B. Run a command on the computer to Update Content
C. Enable the padlock next to the setting in the policy
D. Withdraw the Virus and Spyware Protection policy

Correct Answer: C
Section:
Explanation:
If an administrator modifies the Virus and Spyware Protection policy to disable Auto-Protect, but finds it still enabled on the client, the likely cause is that the setting was not locked. In Symantec Endpoint Protection policies, enabling the padlock icon next 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.

QUESTION 19
In the virus and Spyware Protection policy, an administrator sets the First action to Clean risk and sets If first action fails to Delete risk. Which two (2) factors should the administrator consider? (Select two.)

A. The deleted file may still be in the Recycle Bin.
B. IT Analytics may keep a copy of the file for investigation.
C. False positives may delete legitimate files.
D. Insight may back up the file before sending it to Symantec.
E. A copy of the threat may still be in the quarantine.

Correct Answer: C, E
Section:
Explanation:
When configuring a Virus and Spyware Protection policy with the actions to 'Clean risk' first and 'Delete risk' if cleaning fails, two important considerations are:
False Positives (C): There is a risk that legitimate files may be falsely identified as threats and deleted if the cleaning action fails. This outcome underscores the importance of careful policy configuration to avoid loss of important files.
Quarantine Copy (E): Even if a file is deleted, a copy might still remain in the quarantine. This backup allows for retrieval if the deletion was a false positive or if further analysis of the file is required for investigation purposes.
These considerations help administrators avoid unintended data loss and maintain flexibility for future review of quarantined threats.

QUESTION 20
What protection technology should an administrator enable to prevent double executable file names of ransomware variants like Cryptolocker from running?

A. Download Insight
B. Intrusion Prevention System
C. SONAR
D. Memory Exploit Mitigation

Correct Answer: C
Section:
Explanation:

To prevent ransomware variants, such as Cryptolocker, from executing with double executable file names, an administrator should enable SONAR (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.

QUESTION 21
Which Indicator of Compromise might be detected as variations in the behavior of privileged users that indicate that their account is being used by someone else to gain a foothold in an environment?

A. Mismatched Port - Application Traffic
B. Irregularities in Privileged User Account Activity
C. Surges in Database Read Volume
D. Geographical Irregularities

Correct Answer: B
Section:
Explanation:
An Indicator of Compromise (IOC), such as irregularities in privileged user account activity, can signal that a privileged account may be compromised and used maliciously. This can involve deviations from typical login times, unusual commands or requests, or access to resources not typically utilized by the user. Monitoring such anomalies can help detect when an attacker has gained access to a privileged account and is attempting to establish control within the environment.

QUESTION 22
Why is Active Directory a part of nearly every targeted attack?

A. AD administration is managed by weak legacy APIs.
B. AD is, by design, an easily accessed flat file name space directory database
C. AD exposes all of its identities, applications, and resources to every endpoint in the network
D. AD user attribution includes hidden elevated admin privileges

Correct Answer: C
Section:
Explanation:
Active Directory (AD) is commonly targeted in attacks because it serves as a central directory for user identities, applications, and resources accessible across the network. This visibility makes it an attractive target for attackers to exploit for lateral movement, privilege escalation, and reconnaissance. Once compromised, AD provides attackers with significant insight into an organization's internal structure, enabling further exploitation and access to sensitive data.

QUESTION 23
Which technology can prevent an unknown executable from being downloaded through a browser session?

A. Intrusion Prevention
B. Insight
C. Application Control
D. Advanced Machine Learning

Correct Answer: B
Section:
Explanation:
Symantec Insight technology can prevent the download of unknown executables through a browser session by leveraging a cloud-based reputation service. Insight assesses the reputation of files based on data collected from millions of endpoints, blocking downloads that are unknown or have a low reputation. This technology is particularly effective against zero-day threats or unknown files that do not yet have established signatures.

QUESTION 24
When can an administrator add a new replication partner?

A. Immediately following the first LiveUpdate session of the new site
B. During a Symantec Endpoint Protection Manager upgrade
C. During the initial installation of the new site
D. Immediately following a successful Active Directory sync

Correct Answer: C
Section:
Explanation:
An administrator can add a new replication partner during the initial installation of a new site in Symantec Endpoint Protection Manager (SEPM). This timing is essential because:
Initial Setup of Replication: Configuring replication during installation ensures that the new site can immediately synchronize policies, logs, and other critical data with the existing SEPM environment.
Seamless Data Consistency: Setting up replication from the beginning avoids the need for complex data merging later and ensures both sites are aligned in real time.
Configuring replication at the installation stage facilitates a smoother integration and consistent data flow between SEPM sites.

QUESTION 25
Which device page should an administrator view to track the progress of an issued device command?

A. Command History
B. Activity Update
C. Command Status
D. Recent Activity

Correct Answer: C
Section:
Explanation:
The Command Status page is where an administrator should track the progress of issued device commands in Symantec Endpoint Security. This page provides:
Real-Time Command Updates: It shows the current status of commands, such as 'Pending,' 'Completed,' or 'Failed,' providing immediate insights into the command's execution.
Detailed Progress Tracking: Command Status logs offer details on each command, enabling the administrator to confirm that actions, such as scans, updates, or reboots, have been successfully processed by the endpoint.
The Command Status page is essential for effective device management, as it helps administrators monitor and verify the outcome of their issued commands.

QUESTION 26
Which two (2) considerations must an administrator make when enabling Application Learning in an environment? (Select two.)

A. Application Learning can generate increased false positives.
B. Application Learning should be deployed on a small group of systems in the enterprise.
C. Application Learning can generate significant CPU or memory use on a Symantec Endpoint Protection Manager.
D. Application Learning requires a file fingerprint list to be created in advance.
E. Application Learning is dependent on Insight.

Correct Answer: A, B
Section:
Explanation:
When enabling Application Learning in 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.

QUESTION 27
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 effectively protect against Ransomware attacks, an administrator should enable the following Symantec Endpoint Protection (SEP) technologies:
IPS (Intrusion Prevention System): IPS detects and blocks network-based ransomware attacks, preventing exploitation attempts before they reach the endpoint.
SONAR (Symantec Online Network for Advanced Response): SONAR provides real-time behavioral analysis, identifying suspicious activity characteristic of ransomware, such as unauthorized file modifications.
Download Insight: This technology helps prevent ransomware by evaluating the reputation of files downloaded from the internet, blocking those with a high risk of infection.
Together, these technologies offer comprehensive protection against ransomware by covering network, behavior, and download-based threat vectors.

QUESTION 28
Which of the following is a benefit of choosing a hybrid SES Complete architecture?

A. The ability to use the cloud EDR functionality
B. The ability to manage legacy clients running an embedded OS
C. The ability to manage Active Directory group structure without Azure
D. The ability to use Adaptive Protection features

Correct Answer: A
Section:
Explanation:
A hybrid SES (Symantec Endpoint Security) Complete architecture offers several unique advantages by combining on-premises and cloud-based management and security features. One of the key benefits of choosing this architecture is the ability to utilize cloud-based Endpoint Detection and Response (EDR) functionality.
Cloud EDR Functionality:
Cloud EDR provides advanced threat detection and response capabilities that leverage cloud resources for enhanced threat intelligence, scalability, and data processing power.
By integrating cloud EDR, a hybrid architecture allows organizations to conduct real-time threat analysis, access global threat intelligence, and receive more rapid response options due to the centralized nature of cloud analytics.
This capability is essential for organizations looking to strengthen their endpoint security posture with adaptive and responsive solutions that can analyze, detect, and respond to emerging threats across the enterprise.
Advantages Over Legacy Systems:
A hybrid SES Complete architecture's cloud EDR functionality surpasses traditional, strictly on-premises solutions. Legacy systems may lack the adaptive protection, quick updates, and comprehensive intelligence that cloud solutions offer, which makes them less effective against modern threats.
Adaptive Protection Features:
While hybrid architectures indeed enable adaptive protection, the specific functionality of cloud EDR adds further analytical and actionable insights, thereby extending the security capabilities of an organization's infrastructure.
This answer is based on the Endpoint Security architecture and Symantec Endpoint Protection 14.x documentation, which emphasizes the importance of cloud integration in delivering scalable and adaptive security responses for hybrid deployments.

QUESTION 29
An organization runs a weekly backup using the Backup and Restore Wizard. This week, the process failed to complete due to low disk space.
How does the SEP Administrator change the SEPM backup file location?

A. Move the data directory by reconfiguring the SEPM in the Management Server Configuration Wizard.
B. Move the backup directory by reconfiguring the SEPM in the Management Server Configuration Wizard.
C. Move the install directory by reconfiguring the SEPM in the Management Server Configuration Wizard.
D. Move the database directory by reconfiguring the SEPM in the Management Server Configuration Wizard.

Correct Answer: B
Section:
Explanation:
When a backup fails due to low disk space, the Symantec Endpoint Protection Manager (SEPM) Administrator can change the backup file location to free up space on the primary drive. To do this:
Management Server Configuration Wizard:
SEPM provides an option to reconfigure certain directories, including the backup directory, through the Management Server Configuration Wizard.
By selecting the option to move the backup directory, administrators can specify a new location with sufficient space to store backup files without disrupting the default data or install directories.
Steps to Change Backup Directory Location:
Launch the SEPM Management Server Configuration Wizard.
Choose the option to reconfigure or move the backup directory specifically. This step does not affect the core SEPM installation or database directories.
Specify a new path for the backup directory where sufficient storage is available to prevent future failures.
Reasoning Behind the Choice:
Options A, C, and D involve moving the data, install, or database directories, which are unrelated to backup storage issues. Only the backup directory relocation addresses the low disk space issue during backup processes.

QUESTION 30
An administrator needs to add an Application Exception. When the administrator accesses the Application Exception dialog window, applications fail to appear.
What is the likely problem?

A. The Learn applications that run on the client computer setting are disabled.
B. The client computers already have exclusions for the applications.
C. The Symantec Endpoint Protection Manager is installed on a Domain Controller.
D. The clients are in a trusted Symantec Endpoint Protection domain.

Correct Answer: A
Section:
Explanation:
When the Application Exception dialog fails to display applications, it is typically because the 'Learn applications that run on the client computer' setting is disabled. This setting allows SEPM to learn and list the applications running on client systems, enabling administrators to create application-specific exceptions.
Explanation of Application Learning:
Application Learning is a feature that gathers data on applications executed on client systems. When enabled, SEPM records information about these applications in its database, allowing administrators to review and manage exceptions for detected applications.
If this setting is disabled, SEPM will not record or display applications in the Application Exception dialog, making it impossible for administrators to create exceptions based on learned applications.
Steps to Enable Application Learning:
In SEPM, navigate to Clients > Policies > Communications.
Check the box for 'Learn applications that run on the client computers' to enable the feature.
Once enabled, SEPM will start collecting data, and applications will appear in the Application Exception dialog after the clients report back.
Rationale Against Other Options:
Option B (existing exclusions) would not prevent applications from appearing, as these would still be listed for reference.
Option C (installing SEPM on a Domain Controller) and Option D (trusted SEP domain) do not impact application learning visibility in SEPM.

QUESTION 31
What version number is assigned to a duplicated policy?

A. The original policy's version number
B. Zero
C. The original policy's number plus one
D. One

Correct Answer: D
Section:
Explanation:
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.

QUESTION 32
How should an administrator set up an alert to be notified when manual remediation is needed on an endpoint?

A. Add a Single Risk Event notification and specify 'Left Alone' for the action taken. Choose to log the notification and send an e-mail to the system administrators.
B. Add a Client security alert notification and specify 'Left Alone' for the action taken. Choose to log the notification and send an e-mail to the system administrators.
C. Add a System event notification and specify 'Left Alone' for the action taken. Choose to log the notification and send an e-mail to the system administrators.
D. Add a New risk detected notification and specify 'Left Alone' for the action taken. Choose to log the notification and send an email to the system administrators.

Correct Answer: A
Section:
Explanation:
To notify administrators when manual remediation is required on an endpoint, the administrator should set up a Single Risk Event notification in SEP, with the action specified as 'Left Alone'. This configuration allows SEP to alert administrators only when the system does not automatically handle a detected risk, indicating that further manual intervention is required.
Setting Up the Notification:
Navigate to Notifications in the SEP management console.
Select Single Risk Event as the notification type and specify 'Left Alone' for the action taken.
Enable options to log the notification and send an email alert to system administrators.
Rationale:
This approach ensures that administrators are only alerted when SEP detects a threat but cannot automatically remediate it, signaling a need for manual review and action.
Other options (e.g., System event notification, New risk detected) are broader and may trigger alerts unnecessarily, rather than focusing on cases needing manual attention.

QUESTION 33
An administrator is investigating a possible threat that occurs during the Windows startup. A file is observed that is NOT digitally signed by Microsoft. Which Anti-malware feature should the administrator enable to scan this file for threats?

A. Enable Early Launch Antimalware
B. Enable Auto-Protect
C. Enable Behavioral Analysis
D. Enable Microsoft ELAM

Correct Answer: A
Section:
Explanation:
Early Launch Antimalware (ELAM) is a feature that is designed to provide anti-malware protection during the early stages of Windows startup. When ELAM is enabled, it scans drivers and files that load during startup, especially those not digitally signed by trusted sources like Microsoft.
How ELAM Works:
ELAM loads before other drivers at startup and scans critical files and drivers, identifying potential malware that may attempt to execute before other security layers are fully operational.

Since the file observed is not digitally signed by Microsoft, ELAM would detect and analyze it at boot, preventing possible threats from initializing.
Advantages of ELAM:
It provides proactive defense against rootkits and other threats that may try to gain persistence on the system by loading during the Windows boot process.
Why Other Options Are Less Suitable:
Auto-Protect and Behavioral Analysis are effective but operate after the system has booted.
Microsoft ELAM is already enabled by default in Windows but does not provide the same customizability as SEP's ELAM feature.

QUESTION 34
A company uses a remote administration tool that is detected as Hacktool.KeyLoggPro and quarantined by Symantec Endpoint Protection (SEP).
Which step can an administrator perform to continue using the remote administration tool without detection by SEP?

A. Create a Tamper Protect exception for the tool
B. Create an Application to Monitor exception for the tool
C. Create a Known Risk exception for the tool
D. Create a SONAR exception for the tool

Correct Answer: C
Section:
Explanation:
To allow the use of a remote administration tool detected as Hacktool.KeyLoggPro without interference from SEP, the administrator should create a Known Risk exception for the tool. This exception type allows specific files or applications to bypass detection, thereby avoiding quarantine or blocking actions.
Steps to Create a Known Risk Exception:
In the SEP management console, navigate to Policies > Exceptions.
Choose to create a Known Risk exception and specify the tool's executable file or file path to prevent SEP from identifying it as a threat.
Why Known Risk Exception is Appropriate:
This type of exception is designed for tools that SEP detects as potentially risky (like hacktools or keyloggers) but are authorized for legitimate use by the organization.
Creating this exception allows the tool to operate without being flagged or quarantined.
Reasons Other Options Are Less Effective:
Tamper Protect exceptions only prevent SEP from being tampered with by other applications.
Application to Monitor exceptions monitor applications without preventing quarantine actions.
SONAR exceptions are specific to behavior-based detections, not risk definitions.

QUESTION 35
An organization is considering a single site for their Symantec Endpoint Protection environment. What are two (2) reasons that the organization should consider? (Select two)

A. Organizational merger
B. Sufficient WAN bandwidth
C. Delay-free, centralized reporting
D. 24x7 admin availability
E. Legal constraints

Correct Answer: B, C
Section:
Explanation:
When considering a single-site deployment for Symantec Endpoint Protection (SEP), the following two factors support this architecture:
Sufficient WAN Bandwidth (B):
A single-site SEP environment relies on robust WAN bandwidth to support endpoint communication, policy updates, and threat data synchronization across potentially distant locations.
High bandwidth ensures that endpoints remain responsive to management commands and receive updates without significant delays.

Vdumps

Delay-free, Centralized Reporting (C):
A single-site architecture enables all reporting data to be stored and accessed from one location, providing immediate insights into threats and system health across the organization.
Centralized reporting is ideal when administrators need quick access to consolidated data for faster decision-making and incident response.
Why Other Options Are Not As Relevant:
Organizational mergers (A) and legal constraints (E) do not necessarily benefit from a single-site architecture.
24x7 admin availability (D) is more related to staffing requirements rather than a justification for a single-site SEP deployment.

QUESTION 36
The Security Status on the console home page is failing to alert a Symantec Endpoint Protection (SEP) administrator when virus definitions are out of date.
How should the SEP administrator enable the Security Status alert?

A. Lower the Security Status thresholds
B. Raise the Security Status thresholds
C. Change the Notifications setting to 'Show all notifications'
D. Change the Action Summary display to 'By number of computers'

Correct Answer: A
Section:
Explanation:
To ensure that the Security Status on the SEP console alerts administrators when virus definitions are out of date, the Security Status thresholds should be lowered. Adjusting these thresholds determines the point at which the system flags certain conditions as a security risk. By lowering the threshold, SEP will alert the administrator sooner when virus definitions fall behind.
How to Lower Security Status Thresholds:
In the SEP console, go to Admin > Servers > Local Site > Configure Site Settings.
Under Security Status, adjust the threshold settings for virus definition status to trigger alerts when definitions are outdated by a shorter time frame.
Purpose and Effect:
Lowering thresholds is particularly useful in ensuring timely alerts and maintaining up-to-date endpoint security across the network.
Why Other Options Are Less Effective:
Raising thresholds (Option B) would delay alerts rather than enable them earlier.
Show all notifications (Option C) and Action Summary display (Option D) do not affect the alert for virus definition status.

QUESTION 37
What EDR function minimizes the risk of an endpoint infecting other resources in the environment?

A. Quarantine
B. Block
C. Deny List
D. Firewall

Correct Answer: A
Section:
Explanation:
The function of 'Quarantine' in Endpoint Detection and Response (EDR) minimizes the risk of an infected endpoint spreading malware or malicious activities to other systems within the network environment. This is accomplished by isolating or restricting access of the infected endpoint to contain any threat within that specific machine. Here's how Quarantine functions as a protective measure:
Detection and Isolation: When EDR detects potential malicious behavior or files on an endpoint, it can automatically place the infected file or process in a 'quarantine' area. This means the threat is separated from the rest of the system, restricting its ability to execute or interact with other resources.
Minimizing Spread: By isolating compromised files or applications, Quarantine ensures that malware or suspicious activities do not propagate to other endpoints, reducing the risk of a widespread infection.
Administrative Review: After an item is quarantined, administrators can review it to determine if it should be deleted or restored based on a false positive evaluation. This controlled environment allows for further analysis without risking network security.
Endpoint-Specific Control: Quarantine is designed to act at the endpoint level, applying restrictions that affect only the infected system without disrupting other network resources.

Vdumps
IT Certification Exams - Questions & Answers | Vdumps.com

Using Quarantine as an EDR response mechanism aligns with best practices outlined in endpoint security documentation, such as Symantec Endpoint Protection, which emphasizes containment as a critical first response to threats. This approach supports the proactive defense strategy of limiting lateral movement of malware across a network, thus preserving the security and stability of the entire system.

QUESTION 38
What priority would an incident that may have an impact on business be considered?

A. Low
B. Critical
C. High
D. Medium

Correct Answer: C
Section:
Explanation:
An incident that may have an impact on business is typically classified with a High priority in cybersecurity frameworks and incident response protocols. Here's a detailed rationale for this classification:
Potential Business Disruption: An incident that affects or threatens to affect business operations, even if indirectly, is assigned a high priority to ensure swift response. This classification prioritizes incidents that may not be immediately critical but could escalate if not addressed promptly.
Risk of Escalation: High-priority incidents are situations that, while not catastrophic, have the potential to impact critical systems or compromise sensitive data, thus needing attention before they lead to severe business repercussions.
Rapid Response Requirement: Incidents labeled as high priority are flagged for immediate investigation and containment measures to prevent further business impact or operational downtime.
In this context, while Critical incidents involve urgent threats with immediate, severe effects (such as active data breaches), a High priority applies to incidents with significant risk or potential for business impact. This prioritization is essential for effective incident management, enabling resources to focus on potential risks to business continuity.

QUESTION 39
Which type of communication is blocked, when isolating the endpoint by clicking on the isolate button in SEDR?

A. All non-SEP and non-SEDR network communications
B. All network communications
C. Only SEP and SEDR network communications
D. Only Web and UNC network communications

Correct Answer: A
Section:
Explanation:
When an endpoint is isolated in Symantec Endpoint Detection and Response (SEDR), the isolation blocks all network communication except for SEP and SEDR-related traffic. This selective blocking allows the endpoint to remain manageable by SEP and SEDR administrators while cutting off other potentially harmful network interactions.
How Isolation Works:
Isolation blocks all non-SEP and non-SEDR network communications, effectively preventing the endpoint from connecting to or being accessed by other network entities.
This method helps contain threats while keeping the endpoint connected to management servers for monitoring or further response actions.
Why Other Options Are Incorrect:
All network communications (Option B) would prevent SEP/SEDR management traffic, which is contrary to the design.
Only SEP and SEDR network communications (Option C) is incorrect as it implies only SEP and SEDR are blocked, while in reality, all other traffic is blocked.
Only Web and UNC network communications (Option D) does not cover the full extent of the isolation functionality.

QUESTION 40
Which Discover and Deploy process requires the LocalAccountTokenFilterPolicy value to be added to the Windows registry of endpoints, before the process begins?

A. Push Enrollment

B. Auto Discovery
C. Push Discovery
D. Device Enrollment

Correct Answer: C
Section:
Explanation:
The Push Discovery process in Symantec Endpoint Protection requires the LocalAccountTokenFilterPolicy registry value to be configured on Windows endpoints. This registry setting enables remote management and discovery operations by allowing administrator credentials to pass correctly when discovering and deploying SEP clients.
Purpose of LocalAccountTokenFilterPolicy:
By adding this value to the Windows registry, administrators ensure that SEP can discover endpoints on the network and initiate installations or other management tasks without being blocked by local account filtering.
How to Configure the Registry:
The administrator should add LocalAccountTokenFilterPolicy in the Windows Registry under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System and set it to 1.
This configuration allows for remote actions essential for Push Discovery.
Reasoning Against Other Options:
Push Enrollment and Device Enrollment are distinct processes and do not require this registry setting.
Auto Discovery passively finds systems and does not rely on registry changes for remote access.

QUESTION 41
What does SONAR use to reduce false positives?

A. Virus and Spyware definitions
B. File Fingerprint list
C. Symantec Insight
D. Extended File Attributes (EFA) table

Correct Answer: C
Section:
Explanation:
SONAR (Symantec Online Network for Advanced Response) utilizes Symantec Insight to help reduce false positives in malware detection. Symantec Insight provides a reputation-based system that evaluates the trustworthiness of files based on data gathered from millions of endpoints worldwide.
How Symantec Insight Reduces False Positives:
Insight assigns reputation scores to files, which helps SONAR determine whether a file is likely benign or potentially malicious. Files with high reputation scores are less likely to be flagged as threats.
This reputation-based analysis allows SONAR to avoid marking trusted files (e.g., common, widely-used applications) as malicious, thus reducing the rate of false positives.
Advantages Over Other Options:
While virus and spyware definitions (Option A) provide detection signatures, they are static and do not offer the real-time, behavior-based analysis that Insight provides.
The File Fingerprint list (Option B) and Extended File Attributes (EFA) table (Option D) are not used by SONAR specifically for false-positive reduction.

QUESTION 42
What Threat Defense for Active Directory feature disables a process's ability to spawn another process, overwrite a part of memory, run recon commands, or communicate to the network?

A. Process Mitigation
B. Process Protection
C. Memory Analysis
D. Threat Monitoring

Correct Answer: B
Section:

Explanation:
The Process Protection feature in Threat Defense for Active Directory (TDAD) prevents processes from performing certain actions that could indicate malicious activity. This includes disabling the process's ability to spawn other processes, overwrite memory, execute reconnaissance commands, or communicate over the network.
Functionality of Process Protection:
By restricting these high-risk actions, Process Protection reduces the chances of lateral movement, privilege escalation, or data exfiltration attempts within Active Directory.
This feature is critical in protecting AD environments from techniques commonly used in advanced persistent threats (APTs) and malware targeting AD infrastructure.
Comparison with Other Options:
Process Mitigation (Option A) generally refers to handling or reducing the effects of an attack but does not encompass all the control aspects of Process Protection.
Memory Analysis (Option C) and Threat Monitoring (Option D) involve observing and detecting threats rather than actively restricting process behavior.

QUESTION 43
How does Memory Exploit Mitigation protect applications?

A. Injects a DLL (IPSEng32.dll or IPSEng64.dll) into protected processes and when an exploit attempt is detected, terminates the protected process to prevent the malicious code from running.
B. Injects a DLL (UMEngx86.dll) into applications that run in user mode and if the application behaves maliciously, then SEP detects it.
C. Injects a DLL (sysfer.dll) into processes being launched on the machine and if the process isn't trusted, prevents the process from running.
D. Injects a DLL (IPSEng32.dll) into browser processes and protects the machine from drive-by downloads.

Correct Answer: A
Section:
Explanation:
Memory Exploit Mitigation in Symantec Endpoint Protection (SEP) works by injecting a DLL (Dynamic Link Library) --- specifically, IPSEng32.dll for 32-bit processes or IPSEng64.dll for 64-bit processes --- into applications that require protection. Here's how it works:
DLL Injection:
When Memory Exploit Mitigation is enabled, SEP injects IPSEng DLLs into processes that it monitors for potential exploit attempts.
This injection allows SEP to monitor the behavior of the process at a low level, enabling it to detect exploit attempts on protected applications.
Exploit Detection and Response:
If an exploit attempt is detected within a protected process, SEP will terminate the process immediately. This termination prevents malicious code from running, stopping potential exploit actions from completing.
Why This Approach is Effective:
By terminating the process upon exploit detection, SEP prevents any code injected or manipulated by an exploit from executing. This proactive approach effectively stops many types of memory-based attacks, such as buffer overflows, before they can harm the system.
Clarification on Other Options:
Option B (UMEngx86.dll) pertains to user-mode protection, which isn't used for Memory Exploit Mitigation.
Option C (sysfer.dll) is involved in file system driver activities, not direct exploit prevention.
Option D is partially correct about IPSEng32.dll but inaccurately specifies that it's for browser processes only; the DLL is used for multiple types of processes.

QUESTION 44
In which phase of the MITRE framework would attackers exploit faults in software to directly tamper with system memory?

A. Defense Evasion
B. Execution
C. Exfiltration
D. Discovery

Correct Answer: B
Section:
Explanation:
In the MITRE ATT&CK framework, the Execution phase encompasses techniques that attackers use to run malicious code on a target system. This includes methods for exploiting software vulnerabilities to tamper directly with system memory, often by triggering unintended behaviors such as arbitrary code execution or modifying memory contents to inject malware.

IT Certification Exams - Questions & Answers | Vdumps.com

Execution Phase Overview:
The Execution phase is specifically focused on methods that enable an attacker to run unauthorized code. This might involve exploiting software faults to manipulate memory and bypass defenses.
Memory Exploit Relevance:
Memory exploits, such as buffer overflows or code injections, fall into this phase as they allow attackers to gain control over system processes by tampering with memory.
These exploits can directly manipulate memory, enabling attackers to execute arbitrary instructions, thereby gaining unauthorized control over the application or even the operating system.
Why Other Phases Are Incorrect:
Defense Evasion involves hiding malicious activities rather than direct execution.
Exfiltration pertains to the theft of data from a system.
Discovery is focused on gathering information about the system or network, not executing code.

QUESTION 45
What prevention technique does Threat Defense for Active Directory use to expose attackers?

A. Process Monitoring
B. Obfuscation
C. Honeypot Traps
D. Packet Tracing

Correct Answer: C
Section:
Explanation:
Threat Defense for Active Directory (TDAD) employs Honeypot Traps as 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.