ITCertTest

ITCERTTEST
IT Exam study guide / simulations

http://www.itcerttest.com

IT exam study guide / simulations

Exam : **250-580**

Title : Endpoint Security Complete - Administration R2

Vendor : Symantec

Version : DEMO

NO.1 What happens when a device fails a Host Integrity check?

A. An antimalware scan is initiated

B. The device is restarted

C. The device is quarantined

D. An administrative notification is logged

Answer: C

Explanation:

When a devicefails a Host Integrity checkin Symantec Endpoint Protection (SEP), it isquarantined. This means that the device's access to network resources may be restricted to prevent potential security risks from spreading within the network. Quarantine helps contain devices that do not meet the configured security standards, protecting the overall network integrity.

* Purpose of Quarantine on Host Integrity Failure:
* Host Integrity checks ensure that endpoint devices comply with security policies, such as having up-to-date antivirus signatures or required patches.
* If a device fails this check, quarantine limits its network connectivity, enabling remediation actions without exposing the network to possible risks from the non-compliant device.
* Why Other Options Are Less Suitable:
* Antimalware scans(Option A) anddevice restarts(Option B) are not default responses to integrity check failures.
* Administrative notifications(Option D) may be logged but do not provide containment as quarantine does.

References: Quarantining non-compliant devices is a standard response to Host Integrity check failures, ensuring network protection while remediation occurs.

NO.2 Which action is provided by Symantec EDR for the rapid remediation of impacted endpoints?

A. Quickly filtering for specific attributes

B. Detonate Memory Exploits in conjunction with SEP

C. Automatically stopping suspicious behaviors & unknown threats

D. Block Listing or Allow Listing of specific files

Answer: D

Explanation:

Symantec Endpoint Detection and Response (EDR) providesBlock Listing or Allow Listingof specific files as a rapid remediation action. This feature enables administrators to quickly contain or permit files across endpoints based on identified threat intelligence, thereby reducing the risk of further spread or false positives.

* Use of Block Listing and Allow Listing:
* Block Listing ensures that identified malicious files are immediately prevented from executing on other endpoints, providing containment for known threats.
* Allow Listing, conversely, can be used for trusted files to prevent unnecessary interruptions if false positives occur.
* Why Other Options Are Less Relevant:
* Filtering for specific attributes(Option A) aids in identifying threats but is not a remediation action.
* Detonating Memory Exploits(Option B) is a separate analysis action, not direct remediation.
* Automatically stopping behaviors(Option C) pertains to behavior analysis rather than the specific action of listing files for rapid response.

References: The Block List and Allow List capabilities in Symantec EDR are key for efficient endpoint remediation and control over detected files.

NO.3 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

Answer: B

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 settingwithin the SEPM.
* Re-enroll the SEPMback 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.

NO.4 Which SES feature helps administrators apply policies based on specific endpoint profiles?

A. Policy Bundles

B. Device Profiles

C. Policy Groups

D. Device Groups

Answer: D

Explanation:

In Symantec Endpoint Security (SES),Device Groupsenable administrators to apply policies based on specific endpoint profiles. Device Groups categorize endpoints according to characteristics like department, location, or device type, allowing tailored policy application that meets the specific security needs of each group. By using Device Groups, administrators can efficiently manage security policies, ensuring relevant protections are applied based on the endpoint's profile.

NO.5 Which technique randomizes the memory address map with Memory Exploit Mitigation?

A. ForceDEP

B. SEHOP

C. ASLR

D. ROPHEAP

Answer: C

Explanation:

ASLR (Address Space Layout Randomization)is a security technique used inMemory Exploit Mitigation thatrandomizes the memory address mapfor processes. By placing key data areas at random locations in memory, ASLR makes it more difficult for attackers to predict the locations of specific functions or buffers, thus preventing exploitation techniques that rely on fixed memory addresses.

* How ASLR Enhances Security:

* ASLR rearranges the location of executable code, heap, stack, and libraries each time a program is run, thwarting attacks that depend on known memory locations.
* Why Other Options Are Incorrect:
* ForceDEP(Option A) enforces Data Execution Prevention but does not randomize addresses.
* SEHOP(Option B) mitigates exploits by protecting exception handling but does not involve address randomization.
* ROPHEAP(Option D) refers to Return-Oriented Programming attacks rather than a mitigation technique.
References: ASLR is a widely used method in Memory Exploit Mitigation, adding randomness to memory locations to reduce vulnerability to exploitation.

NO.6 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

Answer: C

Explanation:
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.

NO.7 Files are blocked by hash in the deny list policy. Which algorithm is supported, in addition to MD5?

A. SHA2

B. SHA256

C. SHA256 "salted"

D. MD5 "Salted"

Answer: B

Explanation:
In Symantec Endpoint Protection (SEP), when files are blocked by hash in the deny list policy,SHA256is supported in addition to MD5. SHA256 provides a more secure hashing algorithm compared to MD5 due to its longer hash length and higher resistance to collisions, making it effective for uniquely identifying and blocking malicious files based on their fingerprint.

NO.8 Which security control is complementary to IPS, providing a second layer of protection against network attacks?

A. Host Integrity

B. Network Protection

C. Antimalware

D. Firewall

Answer: D
Explanation:
TheFirewallprovides a complementary layer of protection to Intrusion Prevention System (IPS) in Symantec Endpoint Protection.
* Firewall vs. IPS:
* While IPS detects and blocks network-based attacks by inspecting traffic for known malicious patterns, the firewall controls network access by monitoring and filtering inbound and outbound traffic based on policy rules.
* Together, these tools protect against a broader range of network threats. IPS is proactive in identifying malicious traffic, while the firewall prevents unauthorized access.
* Two-Layer Defense Mechanism:
* The firewall provides control over which ports, protocols, and applications can access the network, reducing the attack surface.
* When combined with IPS, the firewall blocks unauthorized connections, while IPS actively inspects and prevents malicious content within allowed traffic.
* Why Other Options Are Not Complementary:
* Host Integrity focuses on compliance and configuration validation rather than direct network traffic protection.
* Network Protection and Antimalware are essential but do not function as second-layer defenses for IPS within network contexts.
References: Symantec Endpoint Protection's network protection strategies outline the importance of firewalls in conjunction with IPS for comprehensive network defense.

NO.9 What happens when an administrator adds a file to the deny list?
A. The file is assigned to a chosen Deny List policy
B. The file is assigned to the Deny List task list
C. The file is automatically quarantined
D. The file is assigned to the default Deny List policy
Answer: D
Explanation:
When an administrator adds a file to the deny list in Symantec Endpoint Protection, the file is automatically assigned to the default Deny List policy. This action results in the following:
* Immediate Blocking:The file is blocked from executing on any endpoint where the Deny List policy is enforced, effectively preventing the file from causing harm.
* Consistent Enforcement:Using the default Deny List policy ensures that the file is denied access across all relevant endpoints without the need for additional customization.
* Centralized Management:Administrators can manage and review the default Deny List policy within SEPM, providing an efficient method for handling potentially harmful files across the network.
This default behavior ensures swift response to threats by leveraging a centralized deny list policy.

NO.10 What type of Threat Defense for Active Directory alarms are displayed after domain misconfigurations or hidden backdoors are detected?
A. Computer Information Gathering
B. Pass-The-Ticket
C. Credential Theft

D. Dark Corners

Answer: D

Explanation:

Dark Cornersalarms are part of Threat Defense for Active Directory and are triggered when domain misconfigurations or hidden backdoors are detected within the directory environment. Here's how this alarm functions:

* Detection of Hidden Threats:Dark Corners identifies and alerts administrators to hidden vulnerabilities within the Active Directory, such as unauthorized access paths or misconfigurations that could be exploited.
* Security Assurance:By identifying these issues, administrators can proactively address and rectify potential risks that are otherwise challenging to detect.
* Improved Active Directory Security:The Dark Corners alarm helps ensure that backdoors and misconfigurations do not provide attackers with hidden access points, strengthening the overall security posture of Active Directory.

This feature allows for a deeper level of inspection within Active Directory, safeguarding against subtle yet critical security risks.

NO.11 The LiveUpdate Download Schedule is set to the default on the Symantec Endpoint Protection Manager (SEPM).

How many content revisions must the SEPM keep to ensure clients that check in to the SEPM every 10 days receive xdelta content packages instead of full content packages?

A. 10

B. 20

C. 30

D. 60

Answer: C

Explanation:

To ensure that clients checking in every 10 days receivexdelta content packagesinstead of full content packages,30 content revisionsmust be retained on the Symantec Endpoint Protection Manager (SEPM). Here' s why:

* Incremental Updates:xdelta packages are incremental updates that only download changes since the last update, conserving bandwidth and speeding up client updates.
* Content Revision Retention:SEPM needs to retain a sufficient number of content revisions to allow clients that check in intermittently (such as every 10 days) to download incremental rather than full content packages.
* Default Retention Recommendation:Retaining 30 content revisions ensures that clients are covered for up to 10 days of updates, meeting the requirement for xdelta delivery.

This setup optimizes resource usage by reducing the load on network and client systems.

NO.12 When a SEPM is enrolled in ICDm, which policy can only be managed from the cloud?

A. LiveUpdate

B. Firewall

C. Network Intrusion Prevention

D. Intensive Protection

Answer: C

Explanation:
When Symantec Endpoint Protection Manager (SEPM) is enrolled in the Integrated Cyber Defense Manager (ICDm), theNetwork Intrusion Preventionpolicy is exclusively managed from the cloud. This setup enables:
* Centralized Policy Management:By managing Network Intrusion Prevention in the cloud, ICDm ensures that policy updates and threat intelligence can be applied across all endpoints efficiently.
* Real-Time Policy Updates:Cloud-based management allows immediate adjustments to intrusion prevention settings, improving responsiveness to new threats.
* Consistent Security Posture:Managing Network Intrusion Prevention from the cloud ensures that all endpoints maintain a unified defense strategy against network-based attacks.
Cloud management of this policy provides flexibility and enhances security across hybrid environments.

NO.13 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.

Answer: C E

Explanation:
When configuring aVirus and Spyware Protection policywith 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.

NO.14 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

Answer: C

Explanation:
An administrator can add anew replication partnerduring theinitial installation of a new sitein 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.

NO.15 Which Firewall rule components should an administrator configure to blockfacebook.comuse during business hours?

A. Host(s), Network Interface, and Network Service

B. Application, Host(s), and Network Service

C. Action, Hosts(s), and Schedule

D. Action, Application, and Schedule

Answer: C

Explanation:
Toblock facebook.com use during business hours, the SEP administrator should configure theAction, Hosts (s), and Schedulecomponents within the Firewall rule.
* Explanation of Each Component:
* Action: Set to "Block" to deny access to the specified site.
* Hosts(s): Specify facebook.com as the target host, ensuring that all traffic to this domain is blocked.
* Schedule: Define the rule to apply only during business hours, ensuring that access is restricted within the designated time frame.
* Why Other Options Are Incorrect:
* Network InterfaceandNetwork Service(Options A and B) are not specific to blocking domain access.
* Application(Options B and D) is unnecessary if the goal is to block access based on domain and schedule.
References: Configuring Action, Hosts, and Schedule within SEP firewall rules enables precise access control based on time and target domain.