DUMPSBOSS.

Endpoint Security Complete - Administration R1

Symantec 250-561

Version Demo

Total Demo Questions: 9

Total Premium Questions: 97

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture and Components	38
Topic 2, Installation and Configuration	16
Topic 3, Administration	30
Topic 4, Monitoring and Troubleshooting	13
Total	97

QUESTION NO: 1

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

A. Exfiltration

B. Discovery

C. Execution

D. Defense Evasion

ANSWER: D

Explanation:

Defense Evasion is the applicable MITRE ATT&CK tactic. ATT&CK describes the technique *Exploitation for Defense Evasion* as adversaries exploiting a software vulnerability to bypass or undermine defensive controls. Exploitation can involve manipulating memory or an application's execution state so that security mechanisms, such as access controls, mitigations, monitoring, or protective software behavior, are circumvented. The purpose of this activity is not merely to run a program; it is to avoid detection or prevent security controls from functioning as intended. This aligns with the question's emphasis on exploiting software faults to tamper directly with system memory, because memory-level manipulation can be used to defeat protections and conceal malicious activity. MITRE places this behavior under the Defense Evasion tactic because the adversary is using exploitation specifically to impair or bypass defenses. See MITRE ATT&CK's Exploitation for Defense Evasion (T1211) technique page and its Defense Evasion tactic reference.

QUESTION NO: 2

Which two (2) techniques are associated with the MITRE ATT&CK Credential Access tactic? (Select two)

A. OS Credential Dumping

B. Input Capture

C. Data Encrypted for Impact

D. Network Service Scanning

E. Ingress Tool Transfer

ANSWER: A B

Explanation:

OS Credential Dumping and **Input Capture** are techniques associated with the Credential Access tactic. OS Credential Dumping involves obtaining account credential material from operating-system resources, such as credential stores or process memory. Input Capture involves collecting user input, which can include keystrokes entered through a keyboard.

Both techniques can provide an attacker with credentials that enable further access, privilege escalation, lateral movement, or persistence. Security administrators should investigate these behaviors promptly because compromised credentials can remain useful to an attacker even after a malicious file has been removed. See the MITRE ATT&CK Credential Access tactic.

QUESTION NO: 3

An administrator selects the Discovered Items list in the ICDm to investigate a recent surge in suspicious file activity. What should an administrator do to display only high risk files?

A. Apply a list control

B. Apply a search rule

C. Apply a list filter

D. Apply a search modifier

ANSWER: C

Explanation:

Apply a list filter is correct because the Discovered Items view is a results list, and a list filter limits the currently displayed records according to a selected attribute. The administrator can use the risk attribute in that filter and select the high-risk value, narrowing the list to files that require the most immediate investigation. This is an efficient way to focus triage activity without changing the underlying discovered-item data or the scope of the discovery process. Filters operate on the displayed list and can be adjusted or cleared as the investigation progresses, allowing the administrator to move quickly from an overview of suspicious activity to the relevant high-risk subset. Broadcom's Endpoint Security resources describe the platform's administrative and investigative capabilities, while its technical documentation portal provides the product-specific console guidance used for managing and reviewing security data. See the Broadcom Endpoint Security product page and the Broadcom TechDocs portal.

QUESTION NO: 4

Which policy should an administrator configure to restrict the use of removable USB storage devices on managed endpoints?

A. Application and Device Control policy

B. Firewall policy

C. LiveUpdate policy

D. Intrusion Prevention policy

ANSWER: A

Explanation:

Application and Device Control policy is correct. This policy contains Device Control rules that administrators use to allow, block, or limit access to hardware devices such as USB storage, optical drives, printers, and other peripheral devices. The rules can be targeted according to device characteristics and arranged to apply the intended level of access.

Restricting removable storage can reduce the risk of unauthorized data transfer and malware introduction through portable media. Administrators should place narrowly scoped allow rules above broader blocking rules so that approved devices receive the required access. See the Broadcom Symantec Endpoint Protection documentation.

QUESTION NO: 5

Which two (2) content types can clients receive through LiveUpdate? (Select two)

A. Virus definitions

B. Intrusion Prevention signatures

C. Firewall rule descriptions

D. Administrator passwords

E. Device Control rule order

ANSWER: A B

Explanation:

Virus definitions and **Intrusion Prevention signatures** are content types that clients can receive through LiveUpdate. Virus definitions provide current detection information for known malware and security risks. Intrusion Prevention signatures provide updated network-attack detection logic for the endpoint IPS component.

Keeping both types of content current is important because attackers continually introduce new malware samples and exploit techniques. Administrators should monitor update status and investigate clients that have not received current protection content. See the Broadcom Symantec Endpoint Protection documentation and the Broadcom LiveUpdate guidance.

QUESTION NO: 6

Which two (2) statements describe the purpose of quarantining a detected file? (Select two)

A. It prevents the file from being used in its original location

B. It retains the file for administrative review

C. It automatically adds the file to a Whitelist policy

D. It permanently encrypts all copies of the file

E. It disables the endpoint network adapter

ANSWER: A B

Explanation:

Quarantine prevents a detected file from being used in its original location and retains the file for later administrative review. Moving the file into quarantine helps stop accidental execution while allowing the administrator to examine the detection, collect evidence, or determine whether the file was incorrectly identified.

A quarantined file can also be restored when an administrator confirms that it is legitimate and required. Restoration should be performed only after validating the file's origin, publisher, and business purpose. If the detection is confirmed as malicious, the quarantined copy can be removed as part of remediation. See the Broadcom Symantec Endpoint Security documentation.

QUESTION NO: 7

Which two (2) Discovery and Deploy features could an administrator use to enroll MAC endpoints? (Select two)

A. Push Enroll

B. A custom Installation Package Creator package

C. A default Direct Installation package

D. Invite User

E. A custom Direct installation package

ANSWER: B E

Explanation:

A custom Installation Package Creator package and a custom Direct installation package can be used to enroll macOS endpoints. The Installation Package Creator lets an administrator build a tailored installer for deployment through the organization’s chosen software-distribution process. The administrator can configure the package for the appropriate endpoint platform and policy requirements, then distribute the resulting macOS installer to targeted devices. This is useful where endpoint deployment is managed through an established third-party deployment tool or an internally controlled installation workflow.

A custom Direct installation package also supports macOS enrollment. It provides a customized enrollment and installation workflow so that the endpoint installs the Symantec agent and registers with the organization's Endpoint Security Complete environment. Customizing the package enables the administrator to apply the intended deployment configuration before distributing the installation link or package to Mac users. In both cases, successful enrollment connects the Mac endpoint to the management console, allowing it to receive the organization's configured protection policies and report endpoint status.

Broadcom's Endpoint Security Enterprise documentation includes the administrative guidance for client deployment, enrollment, and platform-specific installation workflows: Broadcom TechDocs: Endpoint Security Enterprise. Product deployment resources are also available through Broadcom Security Support.

QUESTION NO: 8

What version number is assigned to a duplicated policy?

A. One

B. Zero

C. The original policy's number plus one

D. The original policy's version numb

ANSWER: A

Explanation:

One is correct. In Symantec Endpoint Security, duplicating a policy creates a separate, new policy object rather than another revision of the source policy. Although the duplicate carries forward the policy settings selected during the duplication process, its policy-version lifecycle begins independently. Therefore, the newly duplicated policy is assigned version 1. This distinction is important operationally: later edits to the duplicate increment that duplicate policy's own version, while the original policy retains its separate version history. Administrators can use policy versioning to identify which revision is deployed, review changes, and roll back a policy when required. Duplicating is consequently a useful way to preserve an existing policy as a baseline while creating an independently managed policy for a different group, environment, or testing purpose. Broadcom's Endpoint Security documentation describes policy management and the policy lifecycle in the cloud console; see the Symantec Endpoint Security documentation portal. Product administration and policy-management resources are also available from the Broadcom Security support portal.

QUESTION NO: 9

Which Antimalware technology is used after all local resources have been exhausted?

A. Sapient

B. ITCS

C. Emulator

D. Reputation

ANSWER: B

Explanation:

ITCS is correct. ITCS, or Intelligent Threat Cloud Service, is the cloud-assisted antimalware capability used when the Endpoint Protection client has exhausted its local detection resources and still needs a determination for a suspicious file. The client can submit relevant file intelligence to Symantec's cloud infrastructure, where additional analysis and current threat intelligence can be applied. This extends protection beyond the content, reputation data, and analysis available locally on the endpoint, while allowing the final detection decision to benefit from cloud-scale telemetry and continuously updated intelligence.

This layered approach is important because malware changes rapidly and an endpoint may encounter a file that is not conclusively identified using its installed definitions and local analysis. By escalating unresolved cases to ITCS, the product can use broader, current intelligence to classify the file and provide a detection result. Broadcom's Endpoint Protection documentation describes the product's protection technologies and cloud-connected security capabilities in its Endpoint Protection documentation. Additional product and threat-protection information is available from the Broadcom Endpoint Protection product page.