PassQueen
a.k.a dumpsqueen.com

Endpoint Security Complete - R2 Technical Specialist

Symantec 250-580

Version Demo

Total Demo Questions: 16

Total Premium Questions: 163

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Planning and Design	55
Topic 2, Installation and Configuration	26
Topic 3, Administration	49
Topic 4, Monitoring and Troubleshooting	33
Total	163

QUESTION NO: 1

Which EDR feature is used to search for real-time indicators of compromise?

A. Domain search

B. Endpoint search

C. Cloud Database search

D. Device Group search

ANSWER: B

Explanation:

Endpoint search is the EDR capability intended to investigate indicators of compromise across managed endpoints. An analyst can submit an indicator-based query and use the endpoint telemetry collected by Symantec Endpoint Detection and Response to identify devices with evidence relevant to that indicator. This supports rapid triage and threat hunting: rather than waiting for a detection to be generated, the analyst can proactively look for endpoint artifacts associated with a suspected or known compromise.

Endpoint searches can be built around investigation-relevant data, such as files and their hashes, processes, network connections, registry-related artifacts, and other endpoint observations available to EDR. The resulting endpoint matches allow the analyst to determine the scope of exposure and continue investigation in the EDR console. This direct, endpoint-focused search workflow is what makes Endpoint search the appropriate feature for finding real-time or near-real-time IoCs.

Broadcom's Symantec Endpoint Detection and Response documentation describes the product's endpoint investigation and search capabilities: Symantec Endpoint Detection and Response documentation. Product documentation and related technical resources are also available through the Broadcom Support Portal.

QUESTION NO: 2

Which action must a Symantec Endpoint Protection administrator take before creating custom Intrusion Prevention signatures?

A. Change the custom signature order

B. Create a Custom Intrusion Prevention Signature library

C. Define signature variables

D. Enable signature logging

ANSWER: B

Explanation:

Create a Custom Intrusion Prevention Signature library is correct because custom IPS signatures in Symantec Endpoint Protection are organized and managed within signature libraries. The administrator must first establish a custom signature library to provide the container in which one or more custom signatures can be created, maintained, and later assigned through an Intrusion Prevention policy. This library-based structure lets an organization group related detections, control their deployment, and manage updates to custom content without modifying Symantec-provided signature content. Once the library exists, the administrator can create a signature, define its matching criteria and action, save it to that library, and enable the appropriate IPS policy for the relevant client groups. Signature variables can be used as part of a signature's design when applicable, but they are not the prerequisite organizational object required before custom signatures can be created. Broadcom's Endpoint Protection documentation describes IPS policy and custom-signature administration within the Endpoint Security documentation set: Broadcom Endpoint Protection documentation. Product administration resources are also available through the Broadcom Knowledge Base.

QUESTION NO: 3

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:

False positives may delete legitimate files. is a key consideration because cleaning is attempted first, but the configured fallback deletes the file when cleaning cannot succeed. Risk detections are based on signatures, heuristics, and reputation data; although these mechanisms are designed to be accurate, an incorrectly detected legitimate file could be removed after the clean attempt fails. Administrators should therefore validate detections, maintain appropriate exclusions for known safe business software, and ensure that recovery procedures are available before broadly applying a delete-on-failure policy.

A copy of the threat may still be in the quarantine. is also relevant because Endpoint Protection can retain a backup/quarantine copy of a file before remediation. This permits an administrator to review the detected object, submit it for further analysis where appropriate, or restore it if investigation establishes that the detection was a false positive. The availability and retention of such copies are governed by the client policy's quarantine and backup-related settings, so administrators should account for both recoverability and quarantine storage management. Broadcom's Endpoint Protection documentation describes Virus and Spyware Protection policy actions and quarantine behavior in the Endpoint Protection documentation portal and the Broadcom Knowledge Base.

QUESTION NO: 4

A Virus and Spyware Protection policy is configured to quarantine detected risks. Which two (2) operational benefits does quarantine provide? (Select two.)

A. It removes the detected file from its original operational location.

B. It can retain a copy for review or possible restoration.

C. It moves the detected file to the Windows Recycle Bin.

D. It automatically verifies that the file is safe to execute.

E. It eliminates the need to investigate the affected endpoint.

ANSWER: A B

Explanation:

Quarantine removes the detected object from its original location so that it cannot continue to be used normally on the endpoint. It also retains a controlled copy that an administrator can review and, when investigation confirms a false positive, restore according to the organization's procedures.

Quarantine does not place a file in the Windows Recycle Bin, does not automatically make the file safe to execute, and does not replace the need to investigate related endpoint activity.

QUESTION NO: 5

Which action does SONAR take before convicting a process?

A. Quarantines the process

B. Blocks suspicious behavior

C. Restarts the system

D. Checks the reputation of the process

ANSWER: D

Explanation:

SONAR checks the reputation of the process before convicting it. SONAR, which stands for Symantec Online Network for Advanced Response, is Endpoint Security's proactive behavior-based detection technology. Its analysis considers the behavior of running processes and correlates that information with reputation intelligence. Looking up reputation first gives the product important context about whether a file or process has a known, trusted, suspicious, or poor reputation. This helps SONAR make a more informed conviction decision while maintaining effective protection against previously unknown threats. Reputation information is derived from Symantec's Global Intelligence Network and is designed to improve the accuracy of endpoint threat decisions. In the SONAR workflow described by Symantec, reputation checking is therefore a pre-conviction assessment step rather than the resulting remediation action. For additional background on SONAR's behavioral protection and reputation-based intelligence, see Broadcom's SONAR overview and the Endpoint Protection documentation for proactive threat protection.

QUESTION NO: 6

An administrator is reviewing the layered protection technologies used by Symantec Endpoint Protection.

Which two (2) statements correctly distinguish Symantec Insight from SONAR? (Select two.)

A. Insight provides reputation information for binary executables.

B. SONAR evaluates the behavior of running processes.

C. Insight replaces the need for Virus and Spyware Protection signatures.

D. SONAR is used to create firewall rules for network ports.

E. Insight is used to configure SEPM replication between sites.

ANSWER: A B

Explanation:

Symantec Insight evaluates binary executables by using reputation intelligence, including characteristics such as prevalence and age. It provides contextual information about whether a file is widely known and trusted or uncommon and potentially suspicious.

SONAR is a proactive behavioral protection technology. It monitors running processes and their behavior, using reputation as part of its decision process before convicting a process. Traditional signatures and firewall rules provide different types of protection.

QUESTION NO: 7

An organization wants malware scanning to occur immediately when users open, copy, save, or execute files. The organization does not want to rely only on scans that occur at scheduled times.

Which protection capability should the administrator configure?

A. Auto-Protect

B. Scheduled Scan

C. Application Learning

D. Unmanaged Detector

ANSWER: A

Explanation:

Auto-Protect is the real-time protection capability that scans files as users and processes access them. It is intended to detect and remediate threats during normal file activity, including when files are opened, copied, written, or executed.

A scheduled scan runs according to its configured schedule and can provide additional coverage, but it does not provide the immediate on-access protection required in this situation.

QUESTION NO: 8

Which type of activity recorder does EDR provide?

A. Virtual

B. Endpoint

C. Email

D. Temporary

ANSWER: B

Explanation:

Endpoint is correct because Symantec Endpoint Detection and Response records endpoint telemetry to support threat detection, investigation, and response. Its endpoint-focused activity recording captures and correlates behavioral information associated with activity on managed devices, enabling analysts to investigate how a threat executed and what actions it performed. This endpoint visibility is central to EDR: security teams need historical evidence of processes and related activity to search for indicators, reconstruct incident timelines, and assess the scope of suspicious behavior. In Symantec's documentation, Endpoint Detection and Response is positioned as a solution that collects and analyzes endpoint activity to identify advanced threats and provide investigation capabilities. The recorder is therefore identified by the source of the telemetry—the endpoint—rather than by a delivery channel or a temporary recording state. This endpoint activity data complements other security telemetry and gives responders the context required to investigate events directly on affected devices. See Broadcom's Endpoint Detection and Response documentation and the Symantec EDR product overview for information on endpoint monitoring, detection, and investigation capabilities.

QUESTION NO: 9

What permissions does the Security Analyst Role have?

A. Trigger dumps, get & quarantine files, enroll new sites

B. Search endpoints, trigger dumps, get & quarantine files

C. Trigger dumps, get & quarantine files, create device groups

D. Search endpoints, trigger dumps, create policies

ANSWER: B

Explanation:

The Security Analyst Role is intended for investigation and incident-response work in the Endpoint Security console. Accordingly, **Search endpoints, trigger dumps, get & quarantine files** is correct because it combines the core operational

capabilities an analyst needs when examining a suspected compromise. Endpoint search lets the analyst locate devices and investigate endpoint-related information across the environment. Triggering a dump allows the analyst to request diagnostic or forensic data from an endpoint when deeper examination is needed. Getting and quarantining files supports safe evidence collection and containment: a suspicious file can be retrieved for analysis and isolated so that it cannot continue to execute on the affected device. These permissions support an analyst's workflow of finding affected endpoints, gathering evidence, and taking immediate file-level containment action without granting broad administrative configuration responsibilities. Broadcom's Endpoint Security documentation describes the product's endpoint investigation, response, and administration capabilities, while its documentation portal is the authoritative source for role and access-control guidance for the relevant product release. See Broadcom Endpoint Security documentation and Broadcom Support Knowledge Base.

QUESTION NO: 10

Which two (2) statements describe the operation of a Group Update Provider (GUP) in a Symantec Endpoint Protection environment? (Select two.)

A. It runs the Symantec Endpoint Protection client.

B. It receives content from a designated content source before distributing it to clients.

C. It replicates policies and logs between SEPM sites.

D. It replaces the management server for client policy communication.

E. It imports Active Directory computer accounts into SEPM.

ANSWER: A B

Explanation:

A GUP is a computer that runs the Symantec Endpoint Protection client and is configured to provide content to other clients. The GUP first obtains content from its designated source, such as SEPM, and then makes that content available to the clients configured to use it.

A GUP does not replace SEPM policy management, does not act as a replication partner, and does not supply client-to-SEPM management communication.

QUESTION NO: 11

Which two (2) instances could cause Symantec Endpoint Protection to be unable to remediate a file? (Select two.)

A. Another scan is in progress.

B. The detected file is in use.

C. There are insufficient file permissions.

D. The file is marked for deletion by Windows on restart.

E. The file has good reputation.

ANSWER: B D

Explanation:

Symantec Endpoint Protection can be unable to remediate a detected item when **The detected file is in use.** A file that is open or locked by an active process cannot always be deleted, repaired, or quarantined immediately. SEP may defer the required action until the process releases the file or until the endpoint is restarted, depending on the remediation action and policy configuration.

The file is marked for deletion by Windows on restart. is also a condition that can prevent SEP from taking immediate remediation action. Windows uses pending file operations during startup and shutdown for files that cannot be removed at

the time the deletion is requested. When a file already has such a pending deletion state, SEP may report that remediation cannot be completed immediately because Windows controls the outstanding operation. Administrators should review the client's risk and system logs and, where appropriate, restart the computer to allow pending operations to complete. SEP documentation describes remediation behavior and the handling of detections on managed endpoints in the Broadcom Endpoint Protection documentation. Additional product support guidance is available through the Broadcom Knowledge Base.

QUESTION NO: 12

Which option should an administrator utilize to temporarily or permanently block a file?

A. Delete

B. Hide

C. Encrypt

D. Deny List

ANSWER: D

Explanation:

Deny List is the appropriate administrative control for blocking a known unwanted or suspicious file across managed endpoints. A deny-list entry identifies the file—typically through a file hash or other supported file identifier—and instructs endpoint protection to prevent that file from being used or executed. This provides a centrally managed enforcement mechanism rather than relying on an action taken only on one local computer.

The block can be temporary when the administrator removes the entry after the investigation, remediation, or containment period is complete. It can also remain in place indefinitely when the file is confirmed to be prohibited or malicious. This makes the Deny List useful for rapid incident containment as well as for maintaining an ongoing restriction on known harmful files. Administrators should identify the intended file carefully before adding it, document the reason for the block, and review long-lived entries periodically as part of endpoint-security policy maintenance. Broadcom's Endpoint Security documentation is available through the Endpoint Security documentation portal, and current product guidance and knowledge articles can be accessed through the Broadcom Support Knowledge Base.

QUESTION NO: 13

An administrator decides to migrate an SES Complete hybrid environment to a fully cloud-managed one. After cleaning up on-premise group structure and policies. What is the next recommended step for migration?

A. Export unique policies from SEPM

B. Enroll the SEPM in ICDm

C. Migrate the agents from ICDm

ANSWER: A

Explanation:

Export unique policies from SEPM is the recommended next step because policy cleanup identifies the settings that must be retained before the organization moves endpoint management fully to the cloud. Exporting the remaining unique SEPM policies creates a reliable record of the organization's approved security configuration, including exceptions and settings that may have been tailored for particular endpoint populations. The administrator can use that record while recreating or aligning equivalent policies in the cloud management console, avoiding the loss of necessary business-specific protections during the transition.

This activity should be completed before endpoint migration so that cloud policy design is ready to protect devices as they are enrolled and reassigned to cloud management. It also supports a controlled migration by separating configuration

preparation from the endpoint move itself: first identify and preserve the intended policy state, then establish the corresponding cloud configuration, and finally transition the managed devices. Broadcom's Endpoint Security documentation describes cloud and hybrid management concepts and the administrative policy capabilities involved in managing endpoint protection. See the Broadcom Endpoint Security documentation and the Symantec Endpoint Protection documentation for current migration and policy-management guidance.

QUESTION NO: 14

During a threat-hunting investigation, an analyst suspects that an attacker established persistence on several Windows endpoints.

Which two (2) artifacts should the analyst prioritize for investigation? (Select two.)

A. Unexpected Registry Run or RunOnce entries and Startup folder executables

B. New services configured to start automatically

C. Temporary browser cache entries

D. DNS resolver cache entries

E. Recently viewed documents in a user profile

ANSWER: A B

Explanation:

Registry Run and RunOnce keys, as well as Startup folder items, are common persistence locations because they can cause a program to execute when a user logs on. A newly installed service configured for automatic startup is also significant because it can start malicious code during system startup.

Browser cache entries and DNS resolver cache entries can provide investigative context, but they are not persistence mechanisms by themselves.

QUESTION NO: 15

An administrator plans to increase antimalware intensity for a large population of endpoints. Which two (2) practices help reduce the operational risk of legitimate business applications being blocked? (Select two.)

A. Deploy the policy first to a representative pilot group.

B. Create narrowly scoped exclusions for validated business software when required.

C. Disable all protection technologies during the rollout.

D. Exclude all local drives from antimalware scanning.

E. Ignore detections until the enterprise deployment is complete.

ANSWER: A B

Explanation:

A staged deployment to a representative pilot group allows the administrator to observe detections and application impact before enforcing the setting across the enterprise. Creating narrowly scoped exclusions for validated business software helps prevent known legitimate applications from being disrupted while retaining protection for other files and systems.

Disabling all protection technologies or broadly excluding entire drives would reduce visibility and protection. Ignoring detections prevents the administrator from identifying false positives or unexpected application impact during the rollout.

QUESTION NO: 16

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

ANSWER: B D

Explanation:

The available scan-range selections for locating unmanaged endpoints are **IP range within the network** and **IP range within the subnet**. These settings are used by the Symantec Endpoint Protection Manager Unmanaged Detector to define the address scope it probes for computers that are reachable on the network but are not managed by the endpoint environment. An administrator can use an IP range within the network when the target addresses span the broader routed network address space. An IP range within the subnet is appropriate when discovery should be constrained to addresses in a particular subnet, allowing a more focused discovery operation. Selecting an appropriate range helps control the discovery workload and supports staged searches for unmanaged computers before deploying or otherwise managing the Symantec Endpoint Protection client. The Unmanaged Detector is part of the product's discovery capabilities and relies on defined network scope to locate candidate endpoints. Broadcom's Endpoint Protection documentation is available through the Symantec Endpoint Protection documentation portal; see also the Broadcom knowledge base for Endpoint Protection administration resources.