PassQueen
a.k.a dumpsqueen.com

Administration of Symantec Advanced Threat Protection 3.0

Symantec 250-441

Version Demo

Total Demo Questions: 13

Total Premium Questions: 133

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Planning and Design	36
Topic 2, Installation and Configuration	29
Topic 3, Monitoring and Management	55
Topic 4, Troubleshooting	13
Total	133

QUESTION NO: 1

An Incident Responder has confirmed that a suspicious executable is malicious and wants to identify other possible occurrences of the same file in the environment.

Which two file attributes are most useful for scoping the investigation? (Choose two.)

A. SHA-256 hash

B. MD5 hash

C. File creation date

D. File name

E. Endpoint IP address

ANSWER: A B

Explanation:

A **SHA-256 hash** is useful because it provides a highly specific identifier for a particular file. Searching for the hash helps the responder identify endpoints or events associated with the exact malicious sample.

The **MD5 hash** is also useful for scoping because threat intelligence, sandbox reports, and historical security records may identify the same file by its MD5 value. File names are easily changed by attackers and are therefore less reliable for determining whether files are identical. ATP supports investigation workflows that use file details and file-related indicators to identify related activity. See the Symantec Advanced Threat Protection 3.0 documentation.

QUESTION NO: 2

Which detection method identifies a file as malware after SEP has queried the file's reputation?

A. Skeptic

B. Vantage

C. Insight

D. Cynic

ANSWER: C

Explanation:

Insight is correct because it is Symantec Endpoint Protection’s reputation-based detection technology. When SEP encounters a file, it can query Symantec’s reputation service and evaluate the file using reputation information derived from broad community intelligence, including how commonly the file is seen, where it originated, and characteristics associated with trusted or malicious files. A file with a sufficiently poor reputation can therefore be identified as malware by Insight even when it is not detected through a conventional signature match alone.

This reputation-driven approach is especially valuable for identifying newly emerging, targeted, or otherwise uncommon threats. Rather than relying exclusively on a locally installed definition for a known threat, Insight uses cloud-supported intelligence to assess the trustworthiness of the file after the reputation query. In the context of an SEP detection event following a file-reputation lookup, the relevant detection method is Insight. Symantec’s description of Insight and reputation-based protection is available in the Symantec Endpoint Protection Insight documentation and the Broadcom Endpoint Protection support resources.

QUESTION NO: 3

What are the prerequisite products needed when deploying ATP: Endpoint, Network, and Email?

A. SEP and Symantec Messaging Gateway

B. SEP, Symantec Email Security.cloud, and Security Information and Event Management (SIEM)

C. SEP and Symantec Email Security.cloud

D. SEP, Symantec Messaging Gateway, and Symantec Email Security.cloud

ANSWER: C

Explanation:

SEP and Symantec Email Security.cloud is correct for this deployment combination. Advanced Threat Protection integrates with Symantec Endpoint Protection (SEP) to provide the ATP: Endpoint capability. SEP supplies endpoint telemetry and enables ATP to identify, investigate, and respond to suspicious activity observed on managed endpoint computers. For email protection in this scenario, ATP integrates with Symantec Email Security.cloud, which provides cloud-email message and attachment intelligence for ATP analysis and incident correlation. ATP: Network is delivered by the ATP appliance's network analysis capability and does not require a separate Symantec network-security product as a prerequisite. Together, SEP and Symantec Email Security.cloud provide the required external product integrations for the endpoint and cloud-email portions of the stated ATP deployment, while the appliance provides the network component. The ATP installation and deployment documentation describes the product integrations and prerequisites for the individual ATP components. See the Broadcom Advanced Threat Protection documentation and the Broadcom Security and Support portal for product documentation and supported-version information.

QUESTION NO: 4

An Incident Responder added a file's MD5 hash to the blacklist.

Which component of SEP enforces the blacklist?

A. Bloodhound

B. System Lockdown

C. Intrusion Prevention

D. SONAR

ANSWER: B

Explanation:

System Lockdown is correct because Symantec Endpoint Protection uses this client component to enforce file-hash blacklist decisions that originate from Symantec Advanced Threat Protection incident response actions. When an Incident Responder adds a file's MD5 hash to the blacklist, ATP distributes that intelligence to the enrolled SEP endpoints. System Lockdown then prevents execution of a file that matches the blacklisted hash, allowing the organization to contain a known malicious artifact even when the file appears under a different name or in a different folder.

This enforcement is hash-specific: the MD5 value identifies the exact file content, and System Lockdown applies the resulting execution-control decision on the endpoint. This is particularly useful during response activities because it turns a centrally identified indicator into an endpoint-level block without requiring responders to locate and manually remove every copy first. The ATP documentation identifies System Lockdown as the SEP technology used for blacklist enforcement, and SEP documentation describes System Lockdown as an application-control capability for preventing unauthorized software from running. See Broadcom Support article TECH234046 and System Lockdown documentation.

QUESTION NO: 5

Which National Institute of Standards and Technology (NIST) cybersecurity function is defined as "finding incursions"?

A. Protect

B. Identify

C. Respond

D. Detect

ANSWER: D

Explanation:

Detect is the National Institute of Standards and Technology cybersecurity function concerned with finding incursions. In the Cybersecurity Framework, this function covers developing and implementing activities that identify the occurrence of a cybersecurity event. In practical security operations, that means collecting and analyzing relevant telemetry, recognizing suspicious activity, correlating alerts, and determining when an unauthorized action or compromise may be taking place. This is the function most directly associated with discovering an intrusion after or while it occurs.

The wording “finding incursions” is a concise way to describe detection capabilities such as continuous security monitoring, anomaly and event detection, and detection-process management. Symantec Advanced Threat Protection supports this operational objective by helping security teams identify potentially malicious activity across integrated control points and investigate detected threats. The framework distinguishes the act of discovering a potential cybersecurity event from the subsequent operational work of containing, mitigating, and recovering from that event.

For the framework’s definition of the Detect function, see the NIST Cybersecurity Framework, Version 1.1. The current framework also describes Detect as finding and analyzing possible cybersecurity attacks and compromises: NIST Cybersecurity Framework.

QUESTION NO: 6

Which two actions can an Incident Responder take in the Cynic portal? (Choose two.)

A. Configure a SIEM feed from the portal to the ATP environment

B. Configure email reports on convictions

C. Submit false positive and false negative files

D. Query hashes

E. Submit hashes to Insight

ANSWER: C D

Explanation:

An Incident Responder uses the Cynic portal primarily to investigate suspicious content and to provide feedback that improves the accuracy of threat analysis. **Query hashes** is an Incident Responder capability because a hash lookup lets the responder investigate whether a known file has already been analyzed and review the associated verdict or conviction information. This supports rapid incident triage without requiring another file submission.

Submit false positive and false negative files is also available to the Incident Responder. When a responder identifies a benign file that was convicted, or a malicious file that did not receive the appropriate conviction, the responder can submit the file for review. This feedback process helps Symantec refine analysis results and improves the quality of subsequent detections. These activities align with the operational investigation and verdict-feedback responsibilities assigned to the Incident Responder role in the Cynic service. For product documentation and the applicable administration resources, see the Broadcom Advanced Threat Protection documentation and the Broadcom Security Advisories portal.

QUESTION NO: 7

Which two steps must an Incident Responder take to isolate an infected computer in ATP?

(Choose two.)

A. Close any open shares

B. Identify the threat and understand how it spreads

C. Create subnets or VLANs and configure the network devices to restrict traffic

D. Set executables on network drives as read only

E. Identify affected clients

ANSWER: A E

Explanation:

To isolate an infected computer effectively, the Incident Responder must first identify affected clients. ATP's incident investigation and endpoint telemetry help establish which hosts are associated with the detected threat, ensuring that containment is directed at the systems requiring action. Accurately identifying the affected endpoints is essential before disrupting access or applying network-level containment.

The responder must also close any open shares. Open shared resources can provide a path for malicious files, ransomware activity, or lateral movement between the infected device and other systems. Closing those shares limits the infected computer's ability to access or expose shared content while the incident is investigated and remediated. This is a containment action intended to reduce the threat's opportunity to spread without prematurely performing eradication or recovery tasks.

These actions align with the containment phase of incident response: establish the affected scope and restrict the avenues through which the compromised endpoint can communicate with or affect other resources. Symantec ATP documentation describes using incident information and endpoint-related context to support investigation and response workflows. See the Symantec Advanced Threat Protection 3.0 documentation and the CISA incident response guidance.

QUESTION NO: 8

Which final steps should an Incident Responder take before using ATP to rejoin a remediated endpoint to the network, according to Symantec best practices?

A. Run an additional antivirus scan with the latest definitions. If the scan comes back as clean, rejoin the computer to the production network.

B. Run Windows Update to patch the system with the latest service pack. Once the system is upto-date, rejoin the computer to the production network.

C. Use SymDiag to run a Threat Scan Analysis on the machine. Once the analysis comes back as clean, rejoin the computer to the production network.

D. Upgrade the client to the latest version of SEP. Once the client is upgraded, rejoin the computer to the production network.

ANSWER: C

Explanation:

Use SymDiag to run a Threat Scan Analysis on the machine. Once the analysis comes back as clean, rejoin the computer to the production network. This is the appropriate final validation because SymDiag's Threat Analysis Scan is intended to inspect the endpoint for indicators and residual evidence of compromise after remediation actions have been performed. A clean result provides the responder with a final endpoint-level assessment that the host no longer presents the threat condition that justified its isolation. This validation fits the ATP incident-response workflow: contain the potentially compromised endpoint, investigate and remediate the identified threat, confirm the endpoint is clean through the diagnostic threat analysis, and then restore network connectivity through ATP. Rejoining only after this clean assessment helps ensure that a remediated device can safely resume normal communication and reduces the risk of reintroducing malicious activity into the production environment. Broadcom's ATP documentation describes the product's incident investigation and endpoint-response capabilities, while its support resources document SymDiag as the diagnostic utility used for endpoint

analysis. See the Symantec Advanced Threat Protection 3.0 documentation and Broadcom SymDiag support documentation.

QUESTION NO: 9 - (SIMULATION)

Which two ATP control points are able to report events that are detected using Vantage?

Enter the two control point names:

ANSWER: See the explanation for the answer

Explanation:

The two ATP control points that can report events detected using Vantage are:
Email
Network

Vantage provides cloud-based file analysis for suspicious content observed through the Email and Network control points; resulting malicious detections are reported as ATP events.

QUESTION NO: 10

Malware is currently spreading through an organization's network. An Incident Responder sees some

detections in SEP, but there is NOT an apparent relationship between them.

How should the responder look for the source of the infection using ATP?

A. Check for the file hash for each detection

B. Isolate a system and collect a sample

C. Submit the hash to Virus Total

D. Check whether the threats were downloaded from the same domain or IP address by looking at incidents

ANSWER: D

Explanation:

Checking whether the threats were downloaded from the same domain or IP address by looking at incidents is the appropriate ATP investigation method. ATP aggregates and correlates telemetry from connected Symantec Endpoint Protection clients and other data sources into incidents, giving the responder a consolidated view of artifacts and activity associated with a potential attack. Rather than treating each SEP detection as an isolated event, the responder can open the relevant incidents and review the associated network indicators, including domains, IP addresses, URLs, file activity, affected devices, and event timelines. A shared download domain or remote IP across otherwise separate endpoint detections is a strong pivot point for identifying the initial delivery infrastructure and determining the likely infection source. From that common indicator, the responder can assess scope, identify all affected endpoints, and take containment actions based on the correlated evidence. This incident-centric workflow is a core ATP capability because it turns disconnected endpoint alerts into an investigation that exposes relationships among attack artifacts and systems. Broadcom's ATP documentation is available through the Advanced Threat Protection documentation portal; product documentation and downloads are also provided through the Broadcom Support product-downloads page.

QUESTION NO: 11

Which two database attributes are needed to create a Microsoft SQL SEP database connection?

(Choose two.)

A. Database version

B. Database IP address

C. Database domain name

D. Database hostname

E. Database name

ANSWER: B E

Explanation:

A Microsoft SQL Server connection for a Symantec Endpoint Protection database requires the location of the SQL Server and the specific database to which ATP will connect. The server location can be supplied as an IP address, making *Database IP address* a valid connection attribute. The connection must also identify the target SEP database, so *Database name* is required. In a typical SEP deployment using Microsoft SQL Server, this is commonly the SEP database created for the management server, such as the `sem5` database. The SQL Server host may alternatively be specified by a resolvable hostname rather than an IP address, but these are alternative ways to provide the server endpoint, not two attributes that must both be entered. ATP also requires valid SQL authentication credentials and the relevant SQL Server port as part of the complete configuration; however, among the listed database attributes, the server IP address and database name provide the required endpoint and database identification. Broadcom's documentation for Symantec Endpoint Protection database configuration describes the SQL Server database and connection details used by the management environment: Broadcom Knowledge Base: SQL database configuration. Microsoft also documents that SQL Server connections identify a server and a database in the connection string: Microsoft SQL Server connection-string syntax.

QUESTION NO: 12

An Incident Responder has reviewed a STIX report and now wants to ensure that their systems have NOT been compromised by any of the reported threats.

Which two objects in the STIX report will ATP search against? (Choose two.)

A. SHA-256 hash

B. MD5 hash

C. MAC address

D. SHA-1 hash

E. Registry entry

ANSWER: A B

Explanation:

ATP uses supported file-hash observables from an imported or reviewed STIX report to check its available telemetry for evidence that a reported threat has been seen in the environment. **SHA-256 hash** is a supported indicator value for this search workflow and provides a highly specific identifier for a file. **MD5 hash** is also supported, allowing ATP to correlate the STIX-provided MD5 value with file information and detections retained by ATP-integrated products and sensors. Searching these observables helps the Incident Responder determine whether files associated with the threat intelligence report have appeared on monitored endpoints or in collected network and security telemetry. The search is based on the observable values supplied by the STIX intelligence and ATP's supported indicator-processing capabilities, rather than attempting a generic compromise assessment. Symantec's ATP STIX documentation identifies the supported objects and behavior for using STIX reports in investigations; see Broadcom Support: ATP and STIX reports. Additional ATP product documentation is available from the Broadcom TechDocs ATP library.

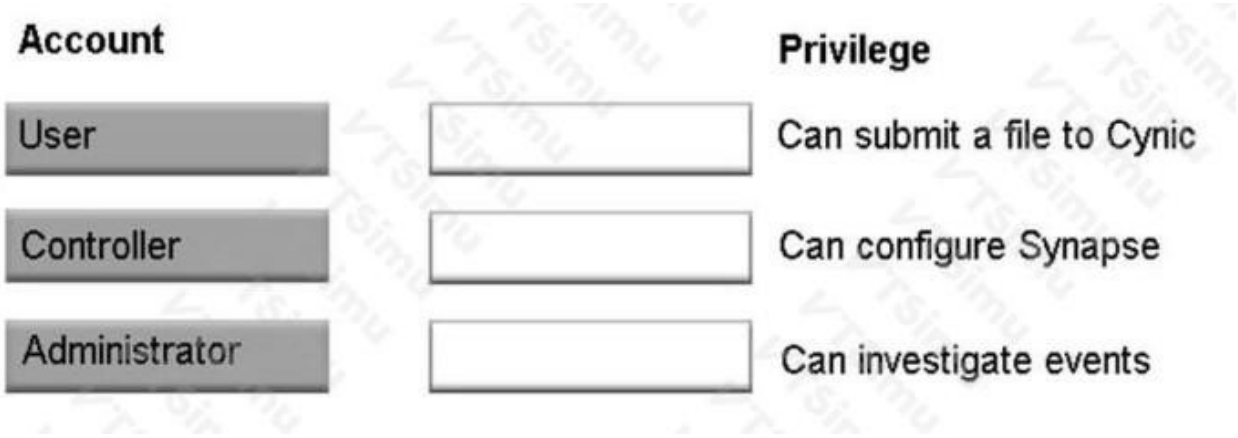
QUESTION NO: 13 - (DRAG DROP)

DRAG DROP

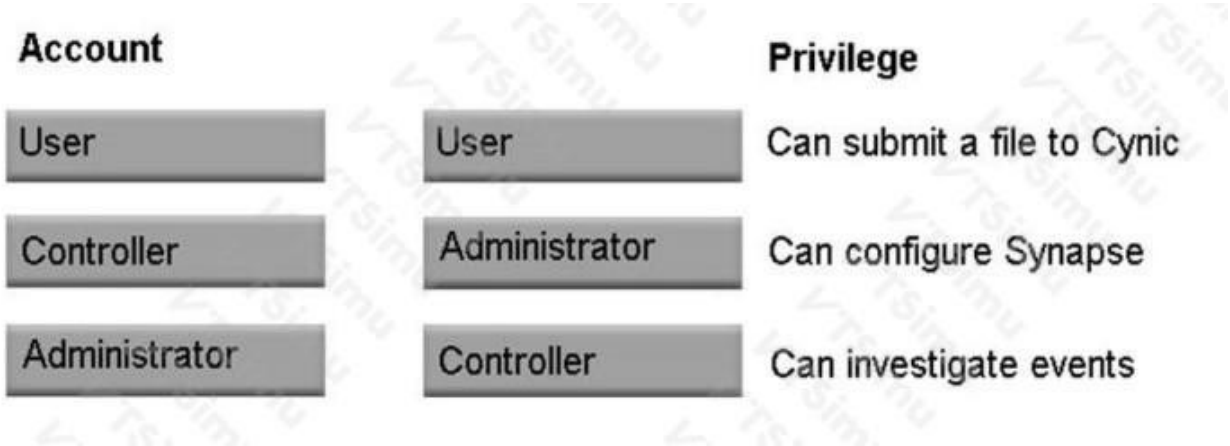
Which level of privilege corresponds to each ATP account type?

Match the correct account type to the corresponding privileges.

Select and Place:



ANSWER:



Explanation:

Symantec Advanced Threat Protection separates account types according to the operational tasks that each person needs to perform. A User account supports the basic analyst workflow of sending a suspicious file to Cynic for sandbox analysis. This allows a person to initiate an analysis of a potentially malicious file without granting broader administrative access to the ATP environment. A Controller account is the investigation-focused role. Controllers work with ATP detections and events, using the event information and investigation workflow to assess suspicious activity and determine the appropriate response. An Administrator account has the elevated permissions required to maintain and configure ATP components, including configuration of Synapse. Synapse is an ATP integration component, so configuring it is an administrative task rather than a standard submission or event-investigation task. Thus, the correct privilege alignment follows the intended workflow boundary: file submission belongs to the User role, event investigation belongs to the Controller role, and Synapse configuration belongs to the Administrator role. Symantec's ATP account and authorization guidance is available in the Symantec Support knowledge-base article HOWTO125620. Additional ATP product documentation can be accessed through the Broadcom Advanced Threat Protection documentation portal.