250-441 Q&As

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/250-441.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec
Official Exam Center

QUESTION 1

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

Correct Answer: AB

Reference: https://support.symantec.com/en_US/article.HOWTO124779.html

QUESTION 2

Which SEP technology does an Incident Responder need to enable in order to enforce blacklisting on an endpoint?

A. System Lockdown

B. Intrusion Prevention System

C. Firewall

D. SONAR

Correct Answer: A

QUESTION 3

A customer has information about a malicious file that has NOT entered the network. The customer wants to know whether ATP is already aware of this threat without having to introduce a copy of the file to the infrastructure.

Which approach allows the customer to meet this need?

A. Use the Cynic portal to check whether the MD5 hash triggers a detection from Cynic

B. Use the ATP console to check whether the SHA-256 hash triggers a detection from Cynic

C. Use the ATP console to check whether the MD5 hash triggers a detection from Cynic

D. Use the Cynic portal to check whether the SHA-256 hash triggers a detection from Cynic

Correct Answer: C

QUESTION 4

Which SEP technologies are used by ATP to enforce the blacklisting of files?

A. Application and Device Control

B. SONAR and Bloodhound

C. System Lockdown and Download Insight

D. Intrusion Prevention and Browser Intrusion Prevention

Correct Answer: C

Reference: https://support.symantec.com/en_US/article.HOWTO101774.html

QUESTION 5

What is the role of Cynic within the Advanced Threat Protection (ATP) solution?

A. Reputation-based security

B. Event correlation

C. Network detection component

D. Detonation/sandbox

Correct Answer: D

Reference: https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-advanced-threat-protectionemail-DS-21349610.pdf

QUESTION 6

Which stage of an Advanced Persistent Threat (APT) attack does social engineering occur?

A. Capture

B. Incursion

C. Discovery

D. Exfiltration

Correct Answer: B

QUESTION 7

What is the role of Vantage within the Advanced Threat Protection (ATP) solution?

A. Network detection component

B. Event correlation

C. Reputation-based security

D. Detonation/sandbox

Correct Answer: A

Reference: https://support.symantec.com/en_US/article.HOWTO119277.html

QUESTION 8

Why is it important for an Incident Responder to review Related Incidents and Events when analyzing an incident for an After Actions Report?

A. It ensures that the Incident is resolved, and the responder can clean up the infection.

B. It ensures that the Incident is resolved, and the responder can determine the best remediation method.

C. It ensures that the Incident is resolved, and the threat is NOT continuing to spread to other parts of the environment.

D. It ensures that the Incident is resolved, and the responder can close out the incident in the ATP manager.

Correct Answer: C

QUESTION 9

While filling out the After Actions Report, an Incident Response Team noted that improved log monitoring could help detect future breaches.

What are two examples of how an organization can improve log monitoring to help detect future breaches? (Choose two.)

A. Periodically log into the ATP manager and review only the Dashboard.

B. Implement IT Analytics to create more flexible reporting.

C. Dedicate an administrator to monitor new events as they flow into the ATP manager.

D. Set email notifications in the ATP manager to message the Security team when a new incident is occurring.

E. Implement Syslog to aggregate information from other systems, including ATP, and review log data in a single console.

Correct Answer: DE

QUESTION 10

An organization is considering an ATP: Endpoint and Network deployment with multiple appliances. Which form factor will be the most effective in terms of performance and costs?

A. Virtual for management, physical for the network scanners and ATP: Endpoint

B. Physical for management and ATP: Endpoint, virtual for the network scanners

C. Virtual for management and ATP: Endpoint, physical for the network scanners

D. Virtual for management, ATP: Endpoint, and the network scanners

Correct Answer: B

QUESTION 11

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

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.TECH234046.html

QUESTION 12

What is the earliest stage at which a SQL injection occurs during an Advanced Persistent Threat (APT) attack?

A. Exfiltration

B. Incursion

C. Capture

D. Discovery

Correct Answer: B

QUESTION 13

An ATP administrator is setting up an Endpoint Detection and Response connection.

Which type of authentication is allowed?

A. Active Directory authentication

B. SQL authentication

C. LDAP authentication

D. Symantec Endpoint Protection Manager (SEPM) authentication

Correct Answer: A

QUESTION 14

What is the main constraint an ATP Administrator should consider when choosing a network scanner model?

A. Throughput

B. Bandwidth

C. Link speed

D. Number of users

Correct Answer: B

QUESTION 15

An Incident Responder launches a search from ATP for a file hash. The search returns the results immediately. The responder reviews the Symantec Endpoint Protection Manager (SEPM) command status and does NOT see an indicators of compromise (IOC) search command.

How is it possible that the search returned results?

A. The search runs and returns results in ATP and then displays them in SEPM.

B. This is only an endpoint search.

C. This is a database search; a command is NOT sent to SEPM for this type of search.

D. The browser cached result from a previous search with the same criteria.

Correct Answer: A