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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

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 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

Correct Answer: BD

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

An Incident Responder wants to investigate whether msscrt.pdf resides on any systems. Which search query and type should the responder run?

A. Database search filename "msscrt.pdf"

B. Database search msscrt.pdf

C. Endpoint search filename like msscrt.pdf

D. Endpoint search filename ="msscrt.pdf"

Correct Answer: A

QUESTION 5

What occurs when an endpoint fails its Host Integrity check and is unable to remediate?

A. The endpoint automatically switches to using a Compliance location, where a Compliance policy is applied to the computer.

B. The endpoint automatically switches to using a System Lockdown location, where a System Lockdown policy is applied to the computer.

C. The endpoint automatically switches to using a Host Integrity location, where a Host Integrity policy is applied to the computer.

D. The endpoint automatically switches to using a Quarantine location, where a Quarantine policy is applied to the computer.

Correct Answer: D