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

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 2

An Incident Responder wants to run a database search that will list all client named starting with SYM. Which syntax should the responder use?

A. hostname like "SYM"

B. hostname "SYM"

C. hostname "SYM*"

D. hostname like "SYM*"

Correct Answer: A

Reference: https://support.symantec.com/en_US/article.HOWTO124805.html

QUESTION 3

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 4

In which scenario should an Incident Responder manually submit a file to the Cynic portal?

A. There is a file on a USB that an Incident Responder wants to analyze in a sandbox.

B. An Incident Responder is unable to remember the password to the .zip archive.

C. The file has generated multiple incidents in the ATP manager and an Incident Responder wants to blacklist the file.

D. The file is a legitimate application and an Incident Responder wants to report it to Symantec as a false positive.

Correct Answer: D

Reference: https://support.symantec.com/content/unifiedweb/en_US/article.HOWTO124806.html

QUESTION 5

An Incident Responder is going to run an indicators of compromise (IOC) search on the endpoints and wants to use operators in the expression.

Which tokens accept one or more of the available operators when building an expression?

A. All tokens

B. Domainname, Filename, and Filehash

C. Filename, Filehash, and Registry

D. Domainname and Filename only

Correct Answer: C

Reference: https://support.symantec.com/en_US/article.HOWTO125969.html#v115770112