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.pass4itsure.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

Which two actions an Incident Responder take when downloading files from the ATP file store? (Choose two.)

A. Analyze suspicious code with Cynic

B. Email the files to Symantec Technical Support

C. Double-click to open the files

D. Diagnose the files as a threat based on the file names

E. Submit the files to Security Response

Correct Answer: AC

QUESTION 2

Which two questions can an Incident Responder answer when analyzing an incident in ATP? (Choose two.)

A. Does the organization need to do a healthcheck in the environment?

B. Are certain endpoints being repeatedly attacked?

C. Is the organization being attacked by this external entity repeatedly?

D. Do ports need to be blocked or opened on the firewall?

E. Does a risk assessment need to happen in the environment?

Correct Answer: BE

QUESTION 3

How should an ATP Administrator configure Endpoint Detection and Response according to Symantec best practices for a SEP environment with more than one domain?

A. Create a unique Symantec Endpoint Protection Manager (SEPM) domain for ATP

B. Create an ATP manager for each Symantec Endpoint Protection Manager (SEPM) domain

C. Create a Symantec Endpoint Protection Manager (SEPM) controller connection for each domain

D. Create a Symantec Endpoint Protection Manager (SEPM) controller connection for the primary domain

Correct Answer: C

Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10986/en_US/satp_administration_guide_3.1.pdf?__gda__=1541979133_5668f0b4c03c16ac1a30d54989313e76 (46)

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

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