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

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

A. Skeptic

B. Vantage

C. Insight

D. Cynic

Correct Answer: C

Reference: https://support.symantec.com/us/en/article.howto80989.html

QUESTION 2

Which two non-Symantec methods for restricting traffic are available to the Incident Response team? (Choose two.)

A. Temporarily disconnect the local network from the internet.

B. Create an Access Control List at the router to deny traffic.

C. Analyze traffic using Wireshark protocol analyzer to identify the source of the infection.

D. Create a DNS sinkhole server to block malicious traffic.

E. Isolate computers so they are NOT compromised by infected computers.

Correct Answer: CD

QUESTION 3

Which two ATP control points are able to report events that are detected using Vantage? Enter the two control point names:

A. ATP: network ATP: Endpoint

Correct Answer: A

Reference: https://support.symantec.com/en_US/article.HOWTO126027.html

QUESTION 4

What is a benefit of using Microsoft SQL as the Symantec Endpoint Protection Manager (SEPM) database in regard to ATP?

A. It allows for Microsoft Incident Responders to assist in remediation

B. ATP can access the database using a log collector on the SEPM host

C. It allows for Symantec Incident Responders to assist in remediation

D. ATP can access the database without any special host system requirements

Correct Answer: D

QUESTION 5

ATP detects a threat phoning home to a command and control server and creates a new incident. The threat is NOT being detected by SEP, but the Incident Response team conducted an indicators of compromise (IOC) search for the machines that are contacting the malicious sites to gather more information.

Which step should the Incident Response team incorporate into their plan of action?

A. Perform a healthcheck of ATP

B. Create firewall rules in the Symantec Endpoint Protection Manager (SEPM) and the perimeter firewall

C. Use ATP to isolate non-SEP protected computers to a remediation VLAN

D. Rejoin the endpoints back to the network after completing a final virus scan

Correct Answer: C