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

A. Capture

B. Incursion

C. Discovery

D. Exfiltration

Correct Answer: B

QUESTION 2

An Incident Responder discovers an incident where all systems are infected with a file that has the same name and different hash. As a result, the organism view has multiple entries for the malicious file.

What is causing this issue?

A. This is a polymorphic threat

B. This is a DDoS attack

C. The file has multiple hashes

D. The file is trying to phone home

Correct Answer: A

QUESTION 3

Which attribute is required when configuring the Symantec Endpoint Protection Manager (SEPM) Log Collector?

A. SEPM embedded database name

B. SEPM embedded database type

C. SEPM embedded database version

D. SEPM embedded database password

Correct Answer: D

Reference: https://support.symantec.com/en_US/article.HOWTO125960.html

QUESTION 4

An organization recently deployed ATP and integrated it with the existing SEP environment. During an outbreak, the Incident Response team used ATP to isolate several infected endpoints. However, one of the endpoints could NOT be isolated.

Which SEP protection technology is required in order to use the Isolate and Rejoin features in ATP?

A. Intrusion Prevention

B. Firewall

C. SONAR

D. Application and Device Control

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.HOWTO125535.html

QUESTION 5

In which two locations should an Incident Responder gather data for an After Actions Report in ATP? (Choose two.)

A. Policies page

B. Action Manager

C. Syslog

D. Incident Manager

E. Indicators of compromise (IOC) search

Correct Answer: CD