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 threat is an example of an Advanced Persistent Threat (APT)?

A. Loyphish

B. Aurora

C. ZeroAccess

D. Michelangelo

Correct Answer: B

QUESTION 2

Why is it important for an Incident Responder to analyze an incident during the Recovery phase?

A. To determine the best plan of action for cleaning up the infection

B. To isolate infected computers on the network and remediate the threat C. To gather threat artifacts and review the malicious code in a sandbox environment

D. To access the current security plan, adjust where needed, and provide reference materials in the event of a similar incident

Correct Answer: D

QUESTION 3

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

QUESTION 4

Malware is currently spreading through an organization\\'s network. An Incident Responder sees some detections in SEP, but there is NOT an apparent relationship between them.

How should the responder look for the source of the infection using ATP?

A. Check for the file hash for each detection

B. Isolate a system and collect a sample

C. Submit the hash to Virus Total

D. Check of the threats are downloaded from the same domain or IP by looking at incidents

Correct Answer: D

QUESTION 5

Which SEP technology does an Incident Responder need to enable in order to enforce blacklisting on an endpoint?

A. System Lockdown

B. Intrusion Prevention System

C. Firewall

D. SONAR

Correct Answer: A