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

An Incident Responder wants to create a timeline for a recent incident using Syslog in addition to ATP for the After Actions Report.

What are two reasons the responder should analyze the information using Syslog? (Choose two.)

A. To have less raw data to analyze

B. To evaluate the data, including information from other systems

C. To access expanded historical data

D. To determine what policy settings to modify in the Symantec Endpoint Protection Manager (SEPM)

E. To determine the best cleanup method

Correct Answer: BE

QUESTION 2

An Incident Responder wants to investigate whether msscrt.pdf resides on any systems. Which search query and type should the responder run?

A. Database search filename "msscrt.pdf"

B. Database search msscrt.pdf

C. Endpoint search filename like msscrt.pdf

D. Endpoint search filename ="msscrt.pdf"

Correct Answer: A

QUESTION 3

What is the main constraint an ATP Administrator should consider when choosing a network scanner model?

A. Throughput

B. Bandwidth

C. Link speed

D. Number of users

Correct Answer: B

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

Why is it important for an Incident Responder to copy malicious files to the ATP file store or create an image of the infected system during the Recovery phase?

A. To have a copy of the file policy enforcement

B. To test the effectiveness of the current assigned policy settings in the Symantec Endpoint Protection Manager (SEPM)

C. To create custom IPS signatures

D. To document and preserve any pieces of evidence associated with the incident

Correct Answer: B