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.leads4pass.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

An Incident Responder wants to use a STIX file to run an indicators of compromise (IOC) search. Which format must the administrator use for the file?

A. .csv

B. .xml

C. .mht

D. .html

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.howto125534.html

QUESTION 2

Which endpoint detection method allows for information about triggered processes to be displayed in ATP?

A. SONAR

B. Insight

C. System Lockdown

D. Antivirus

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.howto125308.html

QUESTION 3

What is the role of Insight within the Advanced Threat Protection (ATP) solution?

A. Reputation-based security

B. Detonation/sandbox

C. Network detection component

D. Event correlation

Correct Answer: A

Reference: https://www.symantec.com/content/dam/symantec/docs/brochures/atp-brochure-en.pdf

QUESTION 4

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

QUESTION 5

How can an Incident Responder generate events for a site that was identified as malicious but has NOT triggered any events or incidents in ATP?

A. Assign a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager (SEPM).

B. Run an indicators of compromise (IOC) search in ATP manager.

C. Create a firewall rule in the Symantec Endpoint Protection Manager (SEPM) or perimeter firewall that blocks traffic to the domain.

D. Add the site to a blacklist in ATP manager.

Correct Answer: D

Reference: https://support.symantec.com/en_US/article.HOWTO126023.html