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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What should an Incident Responder do to mitigate a false positive?

A. Add to Whitelist

B. Run an indicators of compromise (IOC) search

C. Submit to VirusTotal

D. Submit to Cynic

Correct Answer: B

QUESTION 2

Which prerequisite is necessary to extend the ATP: Network solution service in order to correlate email detections?

A. Email Security.cloud

B. Web security.cloud

C. Skeptic

D. Symantec Messaging Gateway

Correct Answer: A

Reference: https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-detection-andresponse-atp-endpoint-en.pdf

QUESTION 3

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

QUESTION 4

An Incident Responder has noticed that for the last month, the same endpoints have been involved with malicious traffic every few days. The network team also identified a large amount of bandwidth being used over P2P protocol.

Which two steps should the Incident Responder take to restrict the endpoints while maintaining normal use of the systems? (Choose two.)

A. Report the users to their manager for unauthorized usage of company resources

B. Blacklist the domains and IP associated with the malicious traffic

C. Isolate the endpoints

D. Blacklist the endpoints

E. Find and blacklist the P2P client application

Correct Answer: CE

QUESTION 5

What is the second stage of an Advanced Persistent Threat (APT) attack?

A. Exfiltration

B. Incursion

C. Discovery

D. Capture

Correct Answer: B