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.pass2lead.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

In which scenario would it be beneficial for an organization to eradicate a threat from the environment by deleting it?

A. The Incident Response team is identifying the scope of the infection and is gathering a list of infected systems.

B. The Incident Response team is reviewing detections in the risk logs and assigning a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager (SEPM).

C. The Incident Response team completed their analysis of the threat and added it to a blacklist.

D. The Incident Response team is analyzing the file to determine if it is a threat or a false positive.

Correct Answer: C

QUESTION 2

An ATP Administrator has deployed ATP: Network, Endpoint, and Email and now wants to ensure that all connections are properly secured.

Which connections should the administrator secure with signed SSL certificates?

A. ATP and the Symantec Endpoint Protection Manager (SEPM) ATP and SEP clients Web access to the GUI

B. ATP and the Symantec Endpoint Protection Manager (SEPM) ATP and SEP clients ATP and Email Security.cloud Web access to the GUI

C. ATP and the Symantec Endpoint Protection Manager (SEPM)

D. ATP and the Symantec Endpoint Protection Manager (SEPM) Web access to the GUI

Correct Answer: C

QUESTION 3

An ATP administrator is setting up correlation with Email Security.cloud.

What is the minimum Email Security.cloud account privilege required?

A. Standard User Role - Report

B. Standard User Role - Service

C. Standard User Role - Support

D. Standard User Role - Full Access

Correct Answer: B

QUESTION 4

An Incident Responder added a file\\'s MD5 hash to the blacklist. Which component of SEP enforces the blacklist?

A. Bloodhound

B. System Lockdown

C. Intrusion Prevention

D. SONAR

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.TECH234046.html

QUESTION 5

While filling out the After Actions Report, an Incident Response Team noted that improved log monitoring could help detect future breaches.

What are two examples of how an organization can improve log monitoring to help detect future breaches? (Choose two.)

A. Periodically log into the ATP manager and review only the Dashboard.

B. Implement IT Analytics to create more flexible reporting.

C. Dedicate an administrator to monitor new events as they flow into the ATP manager.

D. Set email notifications in the ATP manager to message the Security team when a new incident is occurring.

E. Implement Syslog to aggregate information from other systems, including ATP, and review log data in a single console.

Correct Answer: DE

250-441 VCE Dumps 250-441 Exam Questions 250-441 Braindumps