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.geekcert.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

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

QUESTION 2

Which two tasks should an Incident Responder complete when recovering from an incident? (Choose two.)

A. Rejoin healthy endpoints back to the network

B. Blacklist any suspicious files found in the environment

C. Submit any suspicious files to Cynic

D. Isolate infected endpoints to a quarantine network

E. Delete threat artifacts from the environment

Correct Answer: BE

QUESTION 3

Which stage of an Advanced Persistent Threat (APT) attack does social engineering occur?

A. Capture

B. Incursion

C. Discovery

D. Exfiltration

Correct Answer: B

QUESTION 4

An Incident Responder notices traffic going from an endpoint to an IRC channel. The endpoint is listed in an incident. ATP is configured in TAP mode.

What should the Incident Responder do to stop the traffic to the IRC channel?

A. Isolate the endpoint with a Quarantine Firewall policy

B. Blacklist the IRC channel IP

C. Blacklist the endpoint IP

D. Isolate the endpoint with an application control policy

Correct Answer: C

QUESTION 5

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

A. Zeus

B. Melissa

C. Duqu

D. Code Red

Correct Answer: C