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

A network control point discovered a botnet phone-home attempt in the network stream.

Which detection method identified the event?

A. Vantage

B. Insight

C. Antivirus

D. Cynic

Correct Answer: C

QUESTION 2

Why is it important for an Incident Responder to review Related Incidents and Events when analyzing an incident for an After Actions Report?

A. It ensures that the Incident is resolved, and the responder can clean up the infection.

B. It ensures that the Incident is resolved, and the responder can determine the best remediation method.

C. It ensures that the Incident is resolved, and the threat is NOT continuing to spread to other parts of the environment.

D. It ensures that the Incident is resolved, and the responder can close out the incident in the ATP manager.

Correct Answer: C

QUESTION 3

An ATP administrator is setting up an Endpoint Detection and Response connection.

Which type of authentication is allowed?

A. Active Directory authentication

B. SQL authentication

C. LDAP authentication

D. Symantec Endpoint Protection Manager (SEPM) authentication

Correct Answer: A

QUESTION 4

Which National Institute of Standards and Technology (NIST) cybersecurity function is defined as "finding incursions"?

A. Protect

B. Identify

C. Respond

D. Detect

Correct Answer: B

QUESTION 5

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