# 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**

Which Advanced Threat Protection (ATP) component best isolates an infected computer from the network?

A. ATP: Email

B. ATP: Endpoint

C. ATP: Network

D. ATP: Roaming

Correct Answer: B

Reference: https://www.symantec.com/products/advanced-threat-protection

**QUESTION 2**

Why is it important for an Incident Responder to analyze an incident during the Recovery phase?

A. To determine the best plan of action for cleaning up the infection

B. To isolate infected computers on the network and remediate the threat C. To gather threat artifacts and review the malicious code in a sandbox environment

D. To access the current security plan, adjust where needed, and provide reference materials in the event of a similar incident

Correct Answer: D

**QUESTION 3**

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 4**

An Incident Responder runs an endpoint search on a client group with 100 endpoints. After one day, the responder sees the results for 90 endpoints.

What is a possible reason for the search only returning results for 90 of 100 endpoints?

A. The search expired after one hour

B. 10 endpoints are offline

C. The search returned 0 results on 10 endpoints

D. 10 endpoints restarted and cancelled the search

Correct Answer: C

**QUESTION 5**

An organization recently deployed ATP and integrated it with the existing SEP environment. During an outbreak, the Incident Response team used ATP to isolate several infected endpoints. However, one of the endpoints could NOT be isolated.

Which SEP protection technology is required in order to use the Isolate and Rejoin features in ATP?

A. Intrusion Prevention

B. Firewall

C. SONAR

D. Application and Device Control

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.HOWTO125535.html