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 medium-sized organization with 10,000 users at Site A and 20,000 users at Site B wants to use ATP: Network to scan internet traffic at both sites.

Which physical appliances should the organization use to act as a network scanner at each site while using the fewest appliances and assuming typical network usage?

A. Site A 8840 x4 ?Site B 8880 x2

B. Site A 8880 x2 ?Site B 8840 x1

C. Site A 8880 x1 ?Site B 8840 x6

D. Site A 8880 x1 ?Site B 8880 x2

Correct Answer: D

QUESTION 2

What is the role of Cynic within the Advanced Threat Protection (ATP) solution?

A. Reputation-based security

B. Event correlation

C. Network detection component

D. Detonation/sandbox

Correct Answer: D

Reference: https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-advanced-threat-protectionemail-DS-21349610.pdf

QUESTION 3

An Incident Responder observes an incident with multiple malware downloads from a malicious domain. The domain in question belongs to one of the organization\\'s suppliers. The organization needs access to the site to continue placing orders. ATP: Network is configured in Inline Block mode.

How should the Incident Responder proceed?

A. Whitelist the domain and close the incident as a false positive

B. Identify the pieces of malware and blacklist them, then notify the supplier

C. Blacklist the domain and IP of the attacking site

D. Notify the supplier and block the site on the external firewall

Correct Answer: D

QUESTION 4

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

A. Zeus

B. Melissa

C. Duqu

D. Code Red

Correct Answer: C

QUESTION 5

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