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.passapply.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

What are two policy requirements for using the Isolate and Rejoin features in ATP? (Choose two.)

A. Add a Quarantine firewall policy for non-compliant and non-remediated computers.

B. Add a Quarantine LiveUpdate policy for non-compliant and non-remediated computers.

C. Add and assign an Application and Device Control policy in the Symantec Endpoint Protection Manager (SEPM).

D. Add and assign a Host Integrity policy in the Symantec Endpoint Protection Manager (SEPM).

E. Add a Quarantine Antivirus and Antispyware policy for non-compliant and non-remediated computers.

Correct Answer: AD

Reference: https://support.symantec.com/en_US/article.HOWTO128427.html

QUESTION 2

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 3

What should an Incident Responder do to mitigate a false positive?

A. Add to Whitelist

B. Run an indicators of compromise (IOC) search

C. Submit to VirusTotal

D. Submit to Cynic

Correct Answer: B

QUESTION 4

An Incident Responder needs to remediate a group of endpoints but also wants to copy a potentially suspicious file to the ATP file store.

In which scenario should the Incident Responder copy a suspicious file to the ATP file store?

A. The responder needs to analyze with Cynic

B. The responder needs to isolate it from the network

C. The responder needs to write firewall rules

D. The responder needs to add the file to a whitelist

Correct Answer: A

Reference: https://support.symantec.com/us/en/article.HOWTO128772.html

QUESTION 5

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