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 the prerequisite products needed when deploying ATP: Endpoint, Network, and Email?

A. SEP and Symantec Messaging Gateway

B. SEP, Symantec Email Security.cloud, and Security Information and Event Management (SIEM)

C. SEP and Symantec Email Security.cloud

D. SEP, Symantec Messaging Gateway, and Symantec Email Security.cloud

Correct Answer: C

Reference: https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10684/en_US/satp_installation_guide_3.0.pdf?__gda__=1567983829_2908c94bffb019f1870796b9dddb60ad

QUESTION 2

An Incident Responder has noticed that for the last month, the same endpoints have been involved with malicious traffic every few days. The network team also identified a large amount of bandwidth being used over P2P protocol.

Which two steps should the Incident Responder take to restrict the endpoints while maintaining normal use of the systems? (Choose two.)

A. Report the users to their manager for unauthorized usage of company resources

B. Blacklist the domains and IP associated with the malicious traffic

C. Isolate the endpoints

D. Blacklist the endpoints

E. Find and blacklist the P2P client application

Correct Answer: CE

QUESTION 3

Which two actions can an Incident Responder take in the Cynic portal? (Choose two.)

A. Configure a SIEM feed from the portal to the ATP environment

B. Configure email reports on convictions

C. Submit false positive and false negative files

D. Query hashes

E. Submit hashes to Insight

Correct Answer: DE

QUESTION 4

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 5

Which National Institute of Standards and Technology (NIST) cybersecurity function includes Risk Assessment or Risk Management Strategy?

A. Recover

B. Protect

C. Respond

D. Identify

Correct Answer: D

Reference: https://www.nist.gov/cyberframework/online-learning/five-functions