250-441$^{\text{Q\&As}}$

Administration of Symantec Advanced Threat Protection 3.0

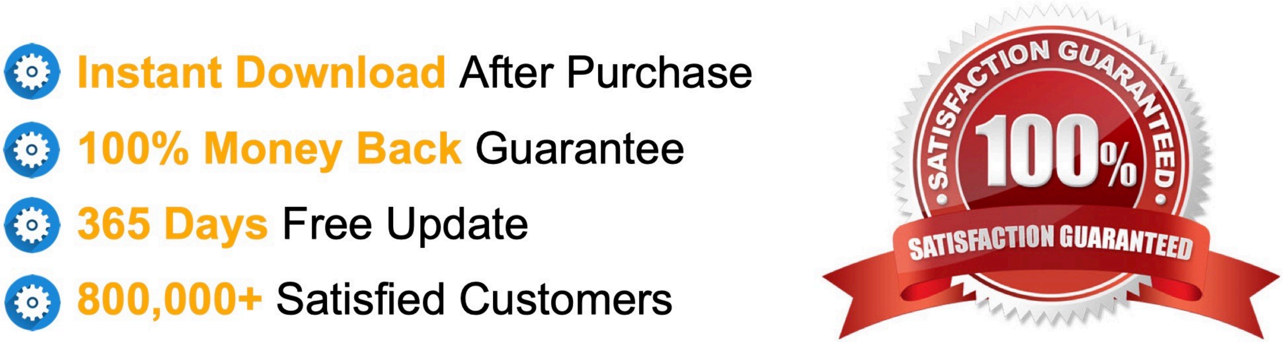
Pass Symantec 250-441 Exam with 100% Guarantee

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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

What is the second stage of an Advanced Persistent Threat (APT) attack?

A. Exfiltration

B. Incursion

C. Discovery

D. Capture

Correct Answer: B

QUESTION 2

Which stage of an Advanced Persistent Threat (APT) attack do attackers map an organization\\'s defenses from the inside?

A. Discovery

B. Capture

C. Exfiltration

D. Incursion

Correct Answer: A

Reference: http://www.whymeridian.com/blog/bid/399610/5-Stages-of-an-Advanced-Persistent-ThreatAttack-on-Your-Network

QUESTION 3

A customer has information about a malicious file that has NOT entered the network. The customer wants to know whether ATP is already aware of this threat without having to introduce a copy of the file to the infrastructure.

Which approach allows the customer to meet this need?

A. Use the Cynic portal to check whether the MD5 hash triggers a detection from Cynic

B. Use the ATP console to check whether the SHA-256 hash triggers a detection from Cynic

C. Use the ATP console to check whether the MD5 hash triggers a detection from Cynic

D. Use the Cynic portal to check whether the SHA-256 hash triggers a detection from Cynic

Correct Answer: C

QUESTION 4

An Incident Responder added a file\\'s MD5 hash to the blacklist. Which component of SEP enforces the blacklist?

A. Bloodhound

B. System Lockdown

C. Intrusion Prevention

D. SONAR

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.TECH234046.html

QUESTION 5

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