250-441 Q&As

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

Following Questions and Answers are all new published by Symantec Official Exam Center

QUESTION 1

Which prerequisite is necessary to extend the ATP: Network solution service in order to correlate email detections?

A. Email Security.cloud

B. Web security.cloud

C. Skeptic

D. Symantec Messaging Gateway

Correct Answer: A

Reference: https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-detection-andresponse-atp-endpoint-en.pdf

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 is setting up an Endpoint Detection and Response connection.

Which type of authentication is allowed?

A. Active Directory authentication

B. SQL authentication

C. LDAP authentication

D. Symantec Endpoint Protection Manager (SEPM) authentication

Correct Answer: A

QUESTION 4

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 5

Which stage of an Advanced Persistent Threat (APT) attack do attackers break into an organization\\'s network to deliver targeted malware?

A. Incursion

B. Discovery

C. Capture

D. Exfiltration

Correct Answer: A

Reference: https://www.symantec.com/content/en/us/enterprise/white_papers/badvanced_persistent_threats_WP_21215957.en-us.pdf