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.pass2lead.com/250-441.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Malware is currently spreading through an organization\\'s network. An Incident Responder sees some detections in SEP, but there is NOT an apparent relationship between them.

How should the responder look for the source of the infection using ATP?

A. Check for the file hash for each detection

B. Isolate a system and collect a sample

C. Submit the hash to Virus Total

D. Check of the threats are downloaded from the same domain or IP by looking at incidents

Correct Answer: D

QUESTION 2

Which service is the minimum prerequisite needed if a customer wants to purchase ATP: Email?

A. Email Protect (antivirus and anti-spam)

B. Email Safeguard (antivirus, anti-spam, encryption, data protection and image control)

C. Symantec Messaging Gateway

D. Skeptic

Correct Answer: A

Reference: http://www.ingrammicrocloud.nl/wp-content/uploads/sites/44/2016/06/Email-Security.cloudPricing-Licensing-Guide.pdf

QUESTION 3

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

QUESTION 4

Where can an Incident Responder view Cynic results in ATP?

A. Events

B. Dashboard

C. File Details

D. Incident Details

Correct Answer: D

Reference: https://support.symantec.com/en_US/article.HOWTO128417.html

QUESTION 5

An organization recently deployed ATP and integrated it with the existing SEP environment. During an outbreak, the Incident Response team used ATP to isolate several infected endpoints. However, one of the endpoints could NOT be isolated.

Which SEP protection technology is required in order to use the Isolate and Rejoin features in ATP?

A. Intrusion Prevention

B. Firewall

C. SONAR

D. Application and Device Control

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.HOWTO125535.html