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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which section of the ATP console should an ATP Administrator use to create blacklists and whitelists?

A. Reports

B. Settings

C. Action Manager

D. Policies

Correct Answer: D

Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10986/en_US/satp_administration_guide_3.1.pdf?__gda__=1541979133_5668f0b4c03c16ac1a30d54989313e76 (132)

QUESTION 2

Which threat is an example of an Advanced Persistent Threat (APT)?

A. ILOVEYOU

B. Conficker

C. MyDoom

D. GhostNet

Correct Answer: D

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

QUESTION 3

An Incident Responder runs an endpoint search on a client group with 100 endpoints. After one day, the responder sees the results for 90 endpoints.

What is a possible reason for the search only returning results for 90 of 100 endpoints?

A. The search expired after one hour

B. 10 endpoints are offline

C. The search returned 0 results on 10 endpoints

D. 10 endpoints restarted and cancelled the search

Correct Answer: C

QUESTION 4

Which two steps must an Incident Responder take to isolate an infected computer in ATP? (Choose two.)

A. Close any open shares

B. Identify the threat and understand how it spreads

C. Create subnets or VLANs and configure the network devices to restrict traffic

D. Set executables on network drives as read only

E. Identify affected clients

Correct Answer: AE

QUESTION 5

An Incident Responder has reviewed a STIX report and now wants to ensure that their systems have NOT been compromised by any of the reported threats.

Which two objects in the STIX report will ATP search against? (Choose two.)

A. SHA-256 hash

B. MD5 hash

C. MAC address

D. SHA-1 hash

E. Registry entry

Correct Answer: AB

Reference: https://support.symantec.com/en_US/article.HOWTO124779.html