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.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

QUESTION 1

Which SEP technology does an Incident Responder need to enable in order to enforce blacklisting on an endpoint?

A. System Lockdown

B. Intrusion Prevention System

C. Firewall

D. SONAR

Correct Answer: A

QUESTION 2

Which Advanced Threat Protection (ATP) component best isolates an infected computer from the network?

A. ATP: Email

B. ATP: Endpoint

C. ATP: Network

D. ATP: Roaming

Correct Answer: B

Reference: https://www.symantec.com/products/advanced-threat-protection

QUESTION 3

What should an Incident Responder do to mitigate a false positive?

A. Add to Whitelist

B. Run an indicators of compromise (IOC) search

C. Submit to VirusTotal

D. Submit to Cynic

Correct Answer: B

QUESTION 4

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

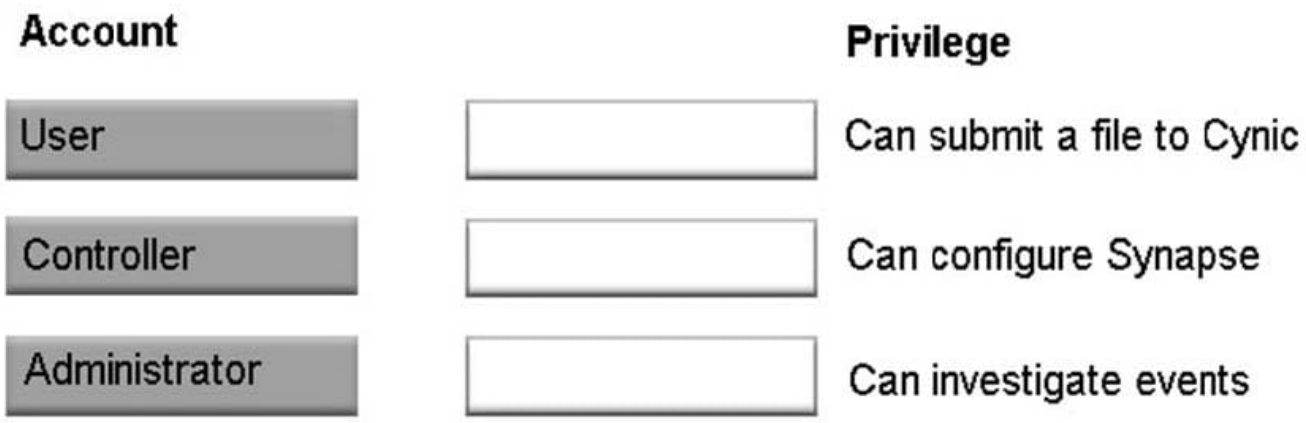
Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10986/en_US/satp_administration_guide_3.1.pdf?__gda__=1541979133_5668f0b4c03c16ac1a30d54989313e76 (132)

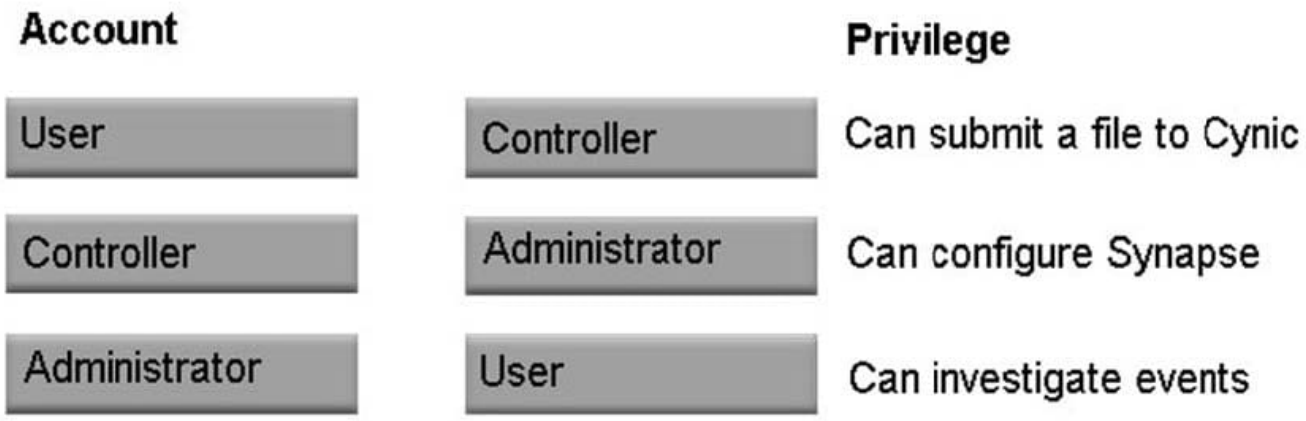
QUESTION 5

Which level of privilege corresponds to each ATP account type? Match the correct account type to the corresponding privileges.

Select and Place:

Correct Answer:





Reference: https://support.symantec.com/us/en/article.HOWTO125620.html

250-441 VCE Dumps 250-441 Practice Test 250-441 Exam Questions