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.pass4itsure.com/250-441.html

100% Passing Guarantee
100% Money Back Assurance

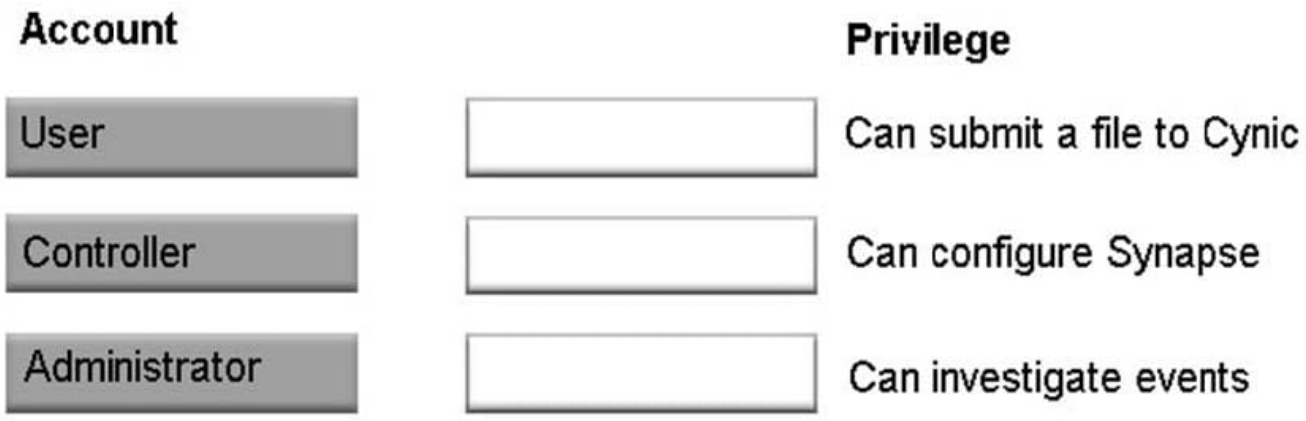
Following Questions and Answers are all new published by Symantec
Official Exam Center

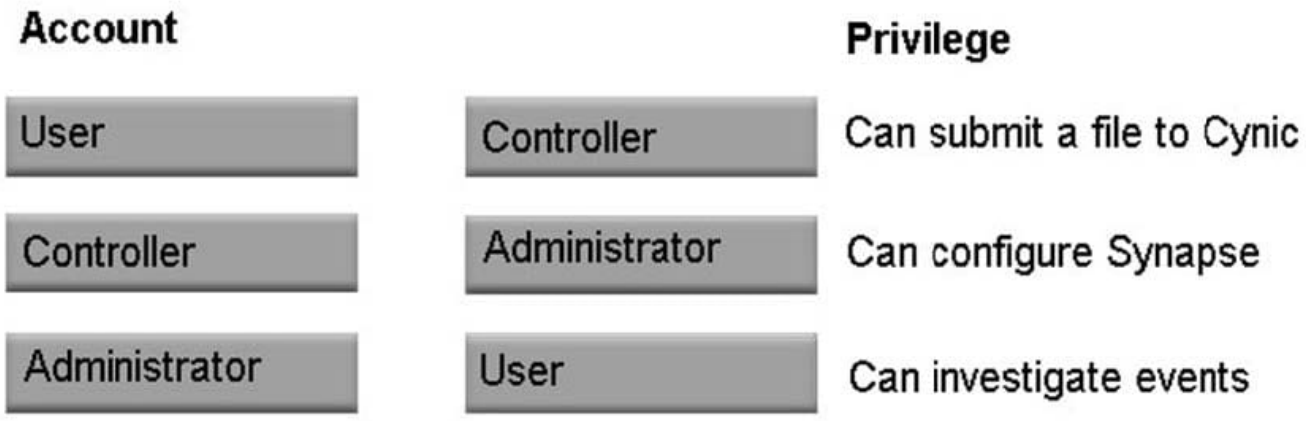
QUESTION 1

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

QUESTION 2

An ATP administrator is setting up correlation with Email Security.cloud.

What is the minimum Email Security.cloud account privilege required?

A. Standard User Role - Report

B. Standard User Role - Service

C. Standard User Role - Support

D. Standard User Role - Full Access

Correct Answer: B

QUESTION 3

Which two actions an Incident Responder take when downloading files from the ATP file store? (Choose two.)

A. Analyze suspicious code with Cynic

B. Email the files to Symantec Technical Support

C. Double-click to open the files

D. Diagnose the files as a threat based on the file names

E. Submit the files to Security Response

Correct Answer: AC

QUESTION 4

Why is it important for an Incident Responder to review Related Incidents and Events when analyzing an incident for an After Actions Report?

A. It ensures that the Incident is resolved, and the responder can clean up the infection.

B. It ensures that the Incident is resolved, and the responder can determine the best remediation method.

C. It ensures that the Incident is resolved, and the threat is NOT continuing to spread to other parts of the environment.

D. It ensures that the Incident is resolved, and the responder can close out the incident in the ATP manager.

Correct Answer: C

QUESTION 5

Which National Institute of Standards and Technology (NIST) cybersecurity function is defined as "finding incursions"?

A. Protect

B. Identify

C. Respond

D. Detect

Correct Answer: B

250-441 Practice Test 250-441 Study Guide 250-441 Exam Questions