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

How does an attacker use a zero-day vulnerability during the Incursion phase?

A. To perform a SQL injection on an internal server

B. To extract sensitive information from the target

C. To perform network discovery on the target

D. To deliver malicious code that breaches the target

Correct Answer: D

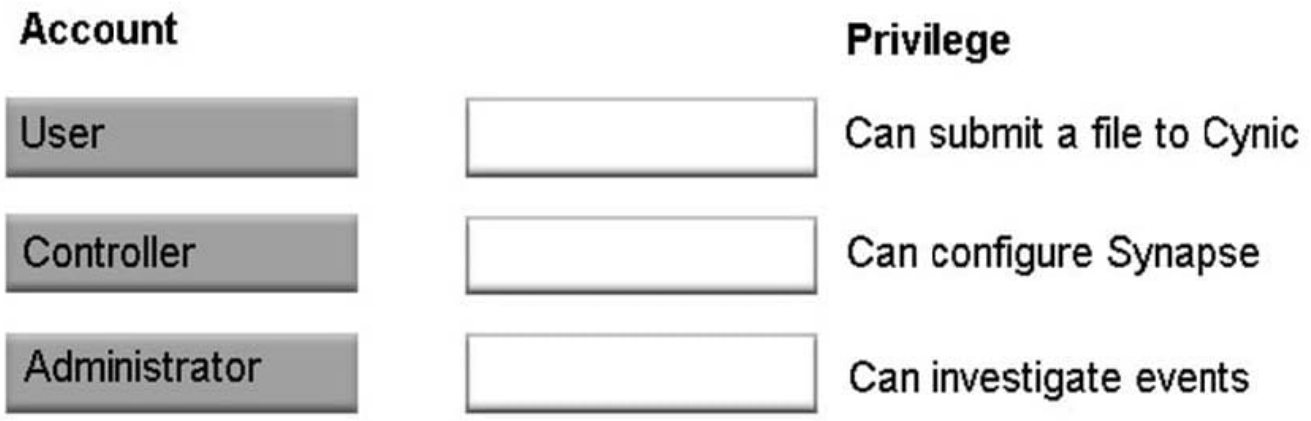
Reference: https://www.symantec.com/connect/blogs/guide-zero-day-exploits

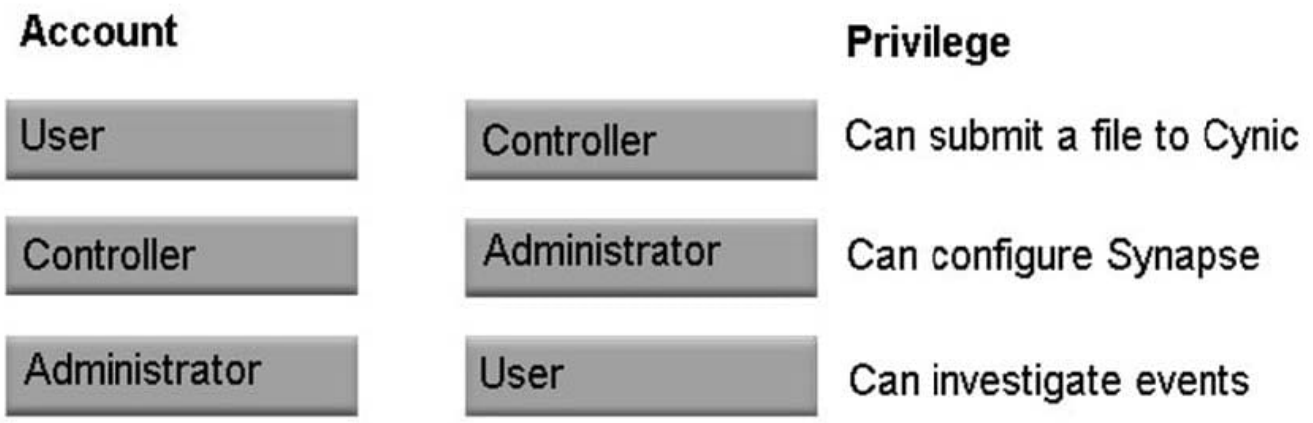
QUESTION 2

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 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

Which two tasks should an Incident Responder complete when recovering from an incident? (Choose two.)

A. Rejoin healthy endpoints back to the network

B. Blacklist any suspicious files found in the environment

C. Submit any suspicious files to Cynic

D. Isolate infected endpoints to a quarantine network

E. Delete threat artifacts from the environment

Correct Answer: BE

QUESTION 5

An Incident Responder wants to create a timeline for a recent incident using Syslog in addition to ATP for the After Actions Report.

What are two reasons the responder should analyze the information using Syslog? (Choose two.)

A. To have less raw data to analyze

B. To evaluate the data, including information from other systems

C. To access expanded historical data

D. To determine what policy settings to modify in the Symantec Endpoint Protection Manager (SEPM)

E. To determine the best cleanup method

Correct Answer: BE