250-441$^{\text{Q\&As}}$

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

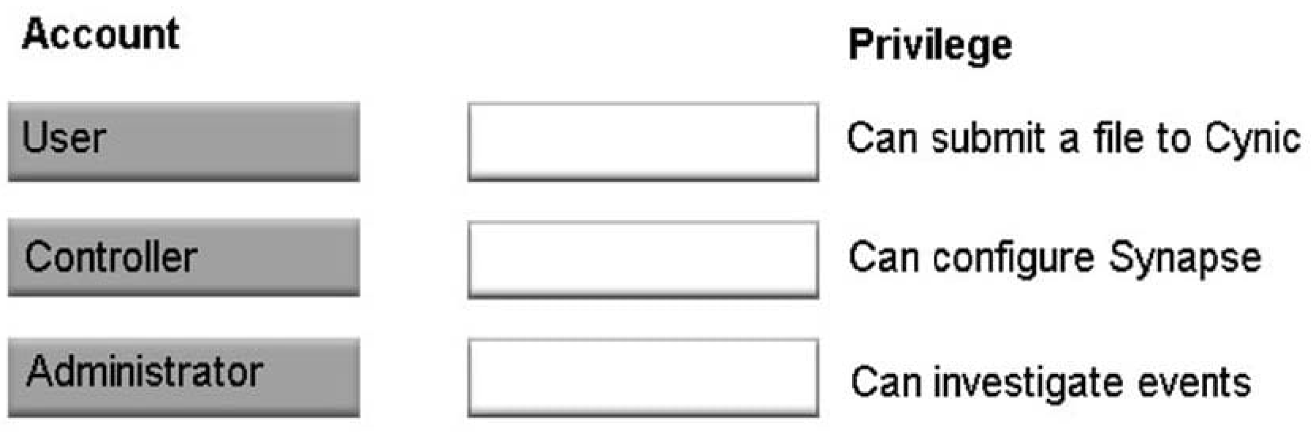
Following Questions and Answers are all new published by Symantec Official Exam Center

QUESTION 1

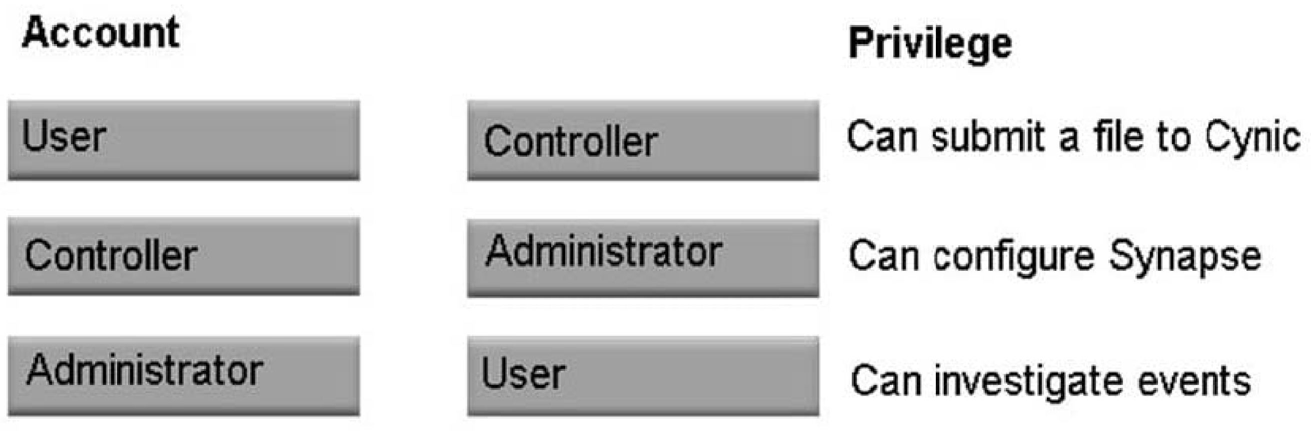
Which level of privilege corresponds to each ATP account type? Match the correct account type to the corresponding privileges.

Select and Place:

Correct Answer:



Account		Privilege
User		Can submit a file to Cynic
Controller		Can configure Synapse
Administrator		Can investigate events



Account		Privilege
User	Controller	Can submit a file to Cynic
Controller	Administrator	Can configure Synapse
Administrator	User	Can investigate events

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

QUESTION 2

Which default port does ATP use to communicate with the Symantec Endpoint Protection Manager (SEPM) web services?

A. 8446

B. 8081

C. 8014

D. 1433

Correct Answer: B

Reference: https://support.symantec.com/en_US/article.HOWTO81103.html

QUESTION 3

An Incident Responder wants to use a STIX file to run an indicators of compromise (IOC) search. Which format must the administrator use for the file?

A. .csv

B. .xml

C. .mht

D. .html

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.howto125534.html

QUESTION 4

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

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

QUESTION 6

Which section of the ATP console should an ATP Administrator use to evaluate prioritized threats within the environment?

A. Search

B. Action Manager

C. Incident Manager

D. Events

Correct Answer: B

QUESTION 7

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

A. Zeus

B. Melissa

C. Duqu

D. Code Red

Correct Answer: C

QUESTION 8

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 9

Which National Institute of Standards and Technology (NIST) cybersecurity function includes Risk Assessment or Risk Management Strategy?

A. Recover

B. Protect

C. Respond

D. Identify

Correct Answer: D

Reference: https://www.nist.gov/cyberframework/online-learning/five-functions

QUESTION 10

An Incident Responder notices traffic going from an endpoint to an IRC channel. The endpoint is listed in an incident. ATP is configured in TAP mode.

What should the Incident Responder do to stop the traffic to the IRC channel?

A. Isolate the endpoint with a Quarantine Firewall policy

B. Blacklist the IRC channel IP

C. Blacklist the endpoint IP

D. Isolate the endpoint with an application control policy

Correct Answer: C

QUESTION 11

Which policies are required for the quarantine feature of ATP to work?

A. Firewall Policy and Host Integrity Policy

B. Quarantine Policy and Firewall Policy

C. Host Integrity Policy and Quarantine Policy

D. Quarantine and Intrusion Prevention Policy

Correct Answer: C

Reference: https://support.symantec.com/us/en/article.tech248959.html

QUESTION 12

An Incident Responder wants to investigate whether msscrt.pdf resides on any systems. Which search query and type should the responder run?

A. Database search filename "msscrt.pdf"

B. Database search msscrt.pdf

C. Endpoint search filename like msscrt.pdf

D. Endpoint search filename ="msscrt.pdf"

Correct Answer: A

QUESTION 13

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

QUESTION 14

An Incident Responder added a file\\'s MD5 hash to the blacklist. Which component of SEP enforces the blacklist?

A. Bloodhound

B. System Lockdown

C. Intrusion Prevention

D. SONAR

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.TECH234046.html

QUESTION 15

What is a benefit of using Microsoft SQL as the Symantec Endpoint Protection Manager (SEPM) database in regard to ATP?

A. It allows for Microsoft Incident Responders to assist in remediation

B. ATP can access the database using a log collector on the SEPM host

C. It allows for Symantec Incident Responders to assist in remediation

D. ATP can access the database without any special host system requirements

Correct Answer: D