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

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

Malware is currently spreading through an organization\\'s network. An Incident Responder sees some detections in SEP, but there is NOT an apparent relationship between them.

How should the responder look for the source of the infection using ATP?

A. Check for the file hash for each detection

B. Isolate a system and collect a sample

C. Submit the hash to Virus Total

D. Check of the threats are downloaded from the same domain or IP by looking at incidents

Correct Answer: D

QUESTION 2

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 3

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 4

An Incident Responder has noticed that for the last month, the same endpoints have been involved with malicious traffic every few days. The network team also identified a large amount of bandwidth being used over P2P protocol.

Which two steps should the Incident Responder take to restrict the endpoints while maintaining normal use of the systems? (Choose two.)

A. Report the users to their manager for unauthorized usage of company resources

B. Blacklist the domains and IP associated with the malicious traffic

C. Isolate the endpoints

D. Blacklist the endpoints

E. Find and blacklist the P2P client application

Correct Answer: CE

QUESTION 5

Which stage of an Advanced Persistent Threat (APT) attack do attackers break into an organization\\'s network to deliver targeted malware?

A. Incursion

B. Discovery

C. Capture

D. Exfiltration

Correct Answer: A

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

QUESTION 6

An Incident Responder is going to run an indicators of compromise (IOC) search on the endpoints and wants to use operators in the expression.

Which tokens accept one or more of the available operators when building an expression?

A. All tokens

B. Domainname, Filename, and Filehash

C. Filename, Filehash, and Registry

D. Domainname and Filename only

Correct Answer: C

Reference: https://support.symantec.com/en_US/article.HOWTO125969.html#v115770112

QUESTION 7

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 8

Which endpoint detection method allows for information about triggered processes to be displayed in ATP?

A. SONAR

B. Insight

C. System Lockdown

D. Antivirus

Correct Answer: B

Reference: https://support.symantec.com/us/en/article.howto125308.html

QUESTION 9

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 10

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

QUESTION 11

An ATP administrator is setting up an Endpoint Detection and Response connection.

Which type of authentication is allowed?

A. Active Directory authentication

B. SQL authentication

C. LDAP authentication

D. Symantec Endpoint Protection Manager (SEPM) authentication

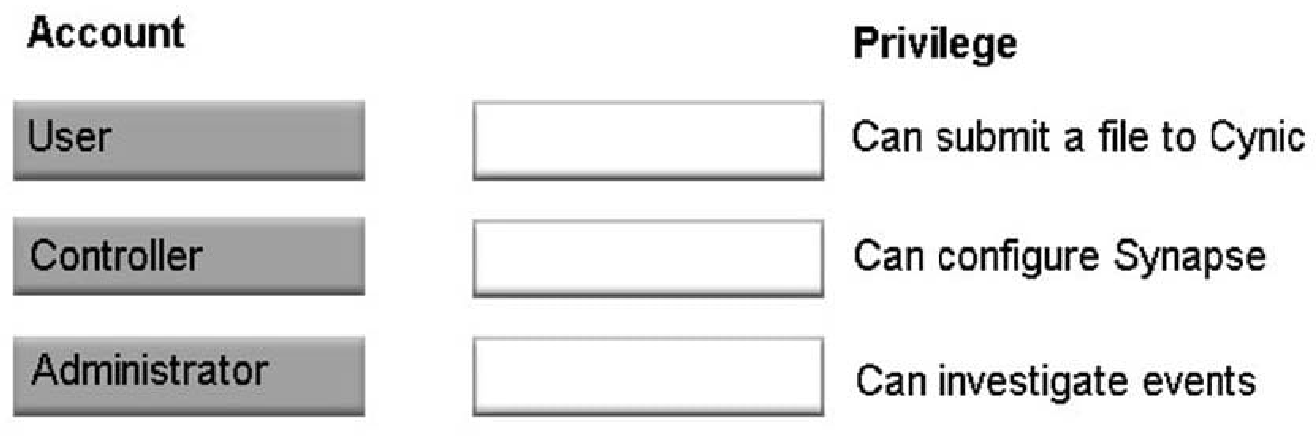
Correct Answer: A

QUESTION 12

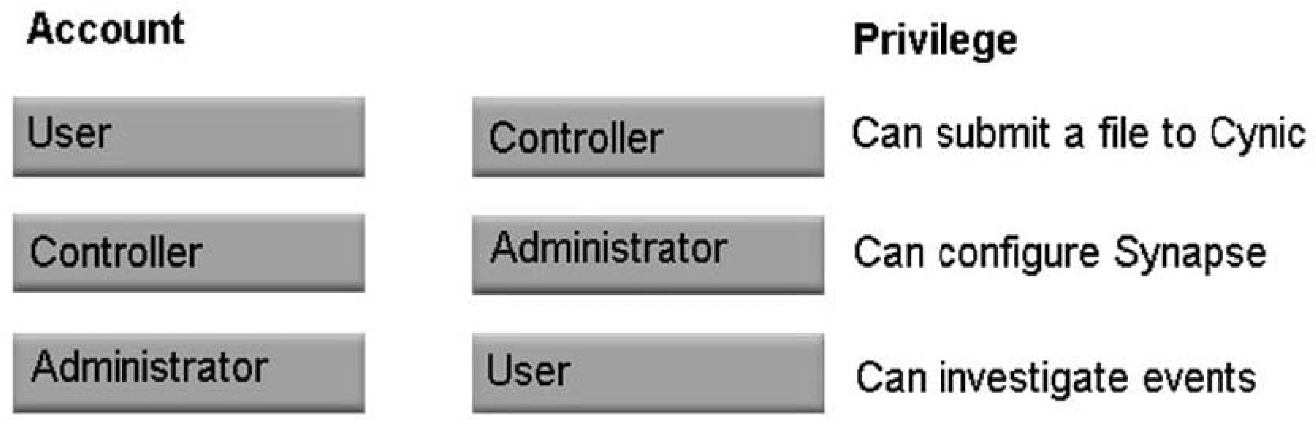
Which level of privilege corresponds to each ATP account type? Match the correct account type to the corresponding privileges.

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 13

An ATP Administrator set up ATP: Network in TAP mode and has placed URLs on the blacklist. What will happen when a user attempts to access one of the blacklisted URLs?

A. Access to the website is blocked by the network scanner but an event is NOT generated

B. Access to the website is blocked by the network scanner and a network event is generated

C. Access to the website is allowed by the network scanner but blocked by ATP: Endpoint and an endpoint event is generated

D. Access to the website is allowed by the network scanner but a network event is generated

Correct Answer: D

Reference: https://support.symantec.com/us/en/article.HOWTO125951.html

QUESTION 14

A network control point discovered a botnet phone-home attempt in the network stream.

Which detection method identified the event?

A. Vantage

B. Insight

C. Antivirus

D. Cynic

Correct Answer: C

QUESTION 15

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