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

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.pass2lead.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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

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 2

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

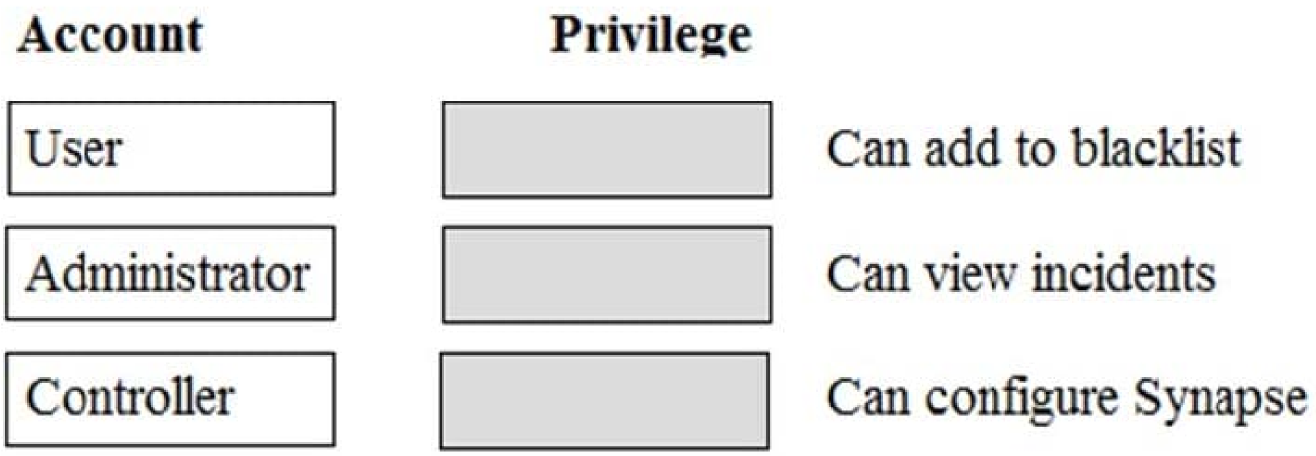
D. Check of the threats are downloaded from the same domain or IP by looking at incidents

Correct Answer: D

QUESTION 3

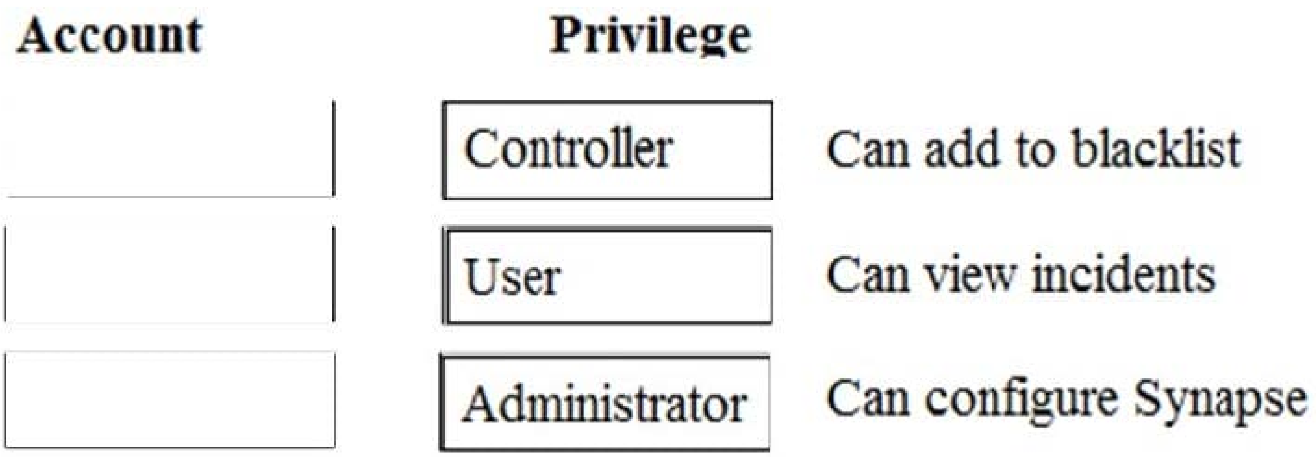
Which level of privilege corresponds to each ATP account type? Match the correct account type to the corresponding privileges.

Select and Place:



Account	Privilege	
User		Can add to blacklist
Administrator		Can view incidents
Controller		Can configure Synapse

Correct Answer:



Account	Privilege	
	Controller	Can add to blacklist
	User	Can view incidents
	Administrator	Can configure Synapse

QUESTION 4

What is the second stage of an Advanced Persistent Threat (APT) attack?

A. Exfiltration

B. Incursion

C. Discovery

D. Capture

Correct Answer: B

QUESTION 5

In which scenario would it be beneficial for an organization to eradicate a threat from the environment by deleting it?

A. The Incident Response team is identifying the scope of the infection and is gathering a list of infected systems.

B. The Incident Response team is reviewing detections in the risk logs and assigning a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager (SEPM).

C. The Incident Response team completed their analysis of the threat and added it to a blacklist.

D. The Incident Response team is analyzing the file to determine if it is a threat or a false positive.

Correct Answer: C

Latest 250-441 Dumps　250-441 VCE Dumps　250-441 Study Guide