250-441 Q&As

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

QUESTION 1

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 2

Which stage of an Advanced Persistent Threat (APT) attack do attackers map an organization\\'s defenses from the inside?

A. Discovery

B. Capture

C. Exfiltration

D. Incursion

Correct Answer: A

Reference: http://www.whymeridian.com/blog/bid/399610/5-Stages-of-an-Advanced-Persistent-ThreatAttack-on-Your-Network

QUESTION 3

Which access credentials does an ATP Administrator need to set up a deployment of ATP: Endpoint, Network, and Email?

A. Email Security.cloud credentials for email correlation, credentials for the Symantec Endpoint Protection Manager (SEPM) database, and a System Administrator login for the SEPM

B. Active Directory login to the Symantec Endpoint Protection Manager (SEPM) database, and an Email Security.cloud login with full access

C. Symantec Endpoint Protection Manager (SEPM) login and ATP: Email login with service permissions

D. Credentials for the Symantec Endpoint Protection Manager (SEPM) database, and an administrator login for Symantec Messaging Gateway

Correct Answer: C

Reference: https://support.symantec.com/us/en/article.howto124667.html

QUESTION 4

Which service is the minimum prerequisite needed if a customer wants to purchase ATP: Email?

A. Email Protect (antivirus and anti-spam)

B. Email Safeguard (antivirus, anti-spam, encryption, data protection and image control)

C. Symantec Messaging Gateway

D. Skeptic

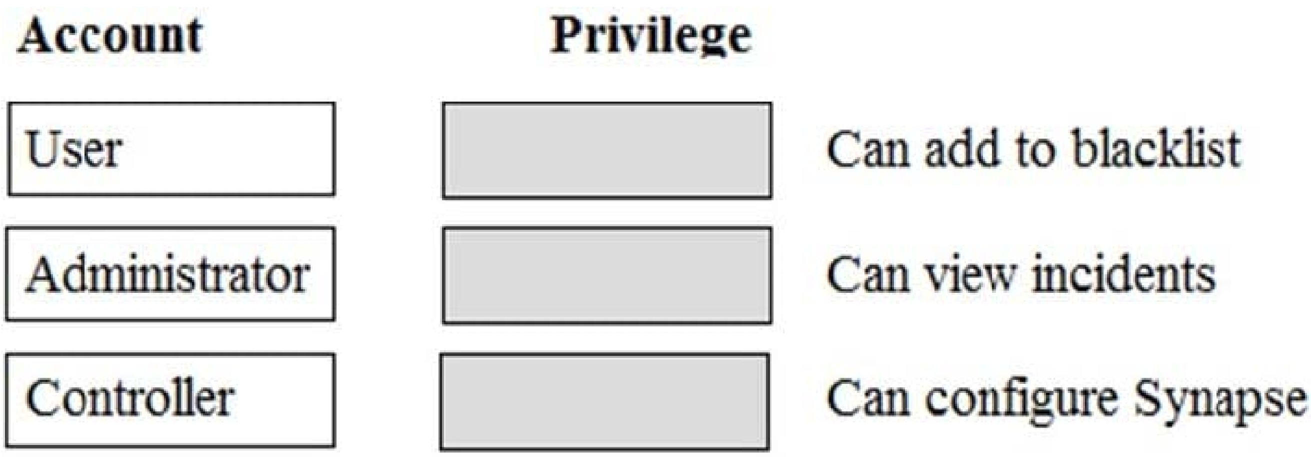
Correct Answer: A

Reference: http://www.ingrammicrocloud.nl/wp-content/uploads/sites/44/2016/06/Email-Security.cloudPricing-Licensing-Guide.pdf

QUESTION 5

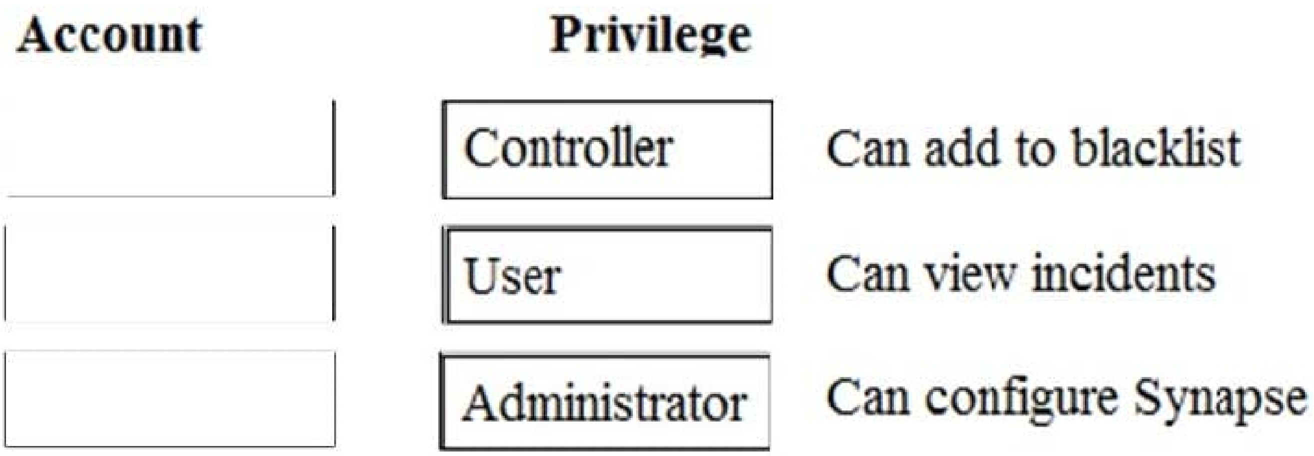
Which level of privilege corresponds to each ATP account type? Match the correct account type to the corresponding privileges.

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

[Latest 250-441 Dumps](#) [250-441 PDF Dumps](#) [250-441 Study Guide](#)