DUMPSARENA

Administration of Symantec Advanced Threat Protection 3.0

Symantec 250-441

Version Demo

Total Demo Questions: 10

Total Premium Questions: 95

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Where can an Incident Responder view Cynic results in ATP?

A. Events

B. Dashboard

C. File Details

D. Incident Details

ANSWER: D

Explanation:

Reference: https://support.symantec.com/en_US/article.HOWTO128417.html

QUESTION NO: 2

An Incident Responder wants to run a database search that will list all client named starting with SYM.

Which syntax should the responder use?

A. hostname like “SYM”

B. hostname “SYM”

C. hostname “SYM*”

D. hostname like “SYM*”

ANSWER: A

Explanation:

Reference: https://support.symantec.com/en_US/article.HOWTO124805.html

QUESTION NO: 3

Which stage of an Advanced Persistent Threat (APT) attack does social engineering occur?

A. Capture

B. Incursion

C. Discovery

D. Exfiltration

ANSWER: B

QUESTION NO: 4

Which two actions can an Incident Responder take in the Cynic portal? (Choose two.)

A. Configure a SIEM feed from the portal to the ATP environment

B. Configure email reports on convictions

C. Submit false positive and false negative files

D. Query hashes

E. Submit hashes to Insight

ANSWER: D E

QUESTION NO: 5

Which two non-Symantec methods for restricting traffic are available to the Incident Response team? (Choose two.)

A. Temporarily disconnect the local network from the internet.

B. Create an Access Control List at the router to deny traffic.

C. Analyze traffic using Wireshark protocol analyzer to identify the source of the infection.

D. Create a DNS sinkhole server to block malicious traffic.

E. Isolate computers so they are NOT compromised by infected computers.

ANSWER: C D

QUESTION NO: 6

An Incident Responder documented the scope of a recent outbreak by reviewing the incident in the ATP manager.

Which two entity relationship examples should the responder look for and document from the Incident Graph? (Choose two.)

A. An intranet website that is experiencing an increase in traffic from endpoints in a smaller branch office.

B. A server in the DMZ that was repeatedly accessed outside of normal business hours on the weekend.

C. A network share is repeatedly accessed during and after an infection indicating a more targeted attack.

D. A malicious file that was repeatedly downloaded by a Trojan or a downloader that infected multiple endpoints.

E. An external website that was the source of many malicious files.

ANSWER: D E

QUESTION NO: 7

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

ANSWER: C E

QUESTION NO: 8

An Incident Responder discovers an incident where all systems are infected with a file that has the same name and different hash. As a result, the organism view has multiple entries for the malicious file.

What is causing this issue?

A. This is a polymorphic threat

B. This is a DDoS attack

C. The file has multiple hashes

D. The file is trying to phone home

ANSWER: A

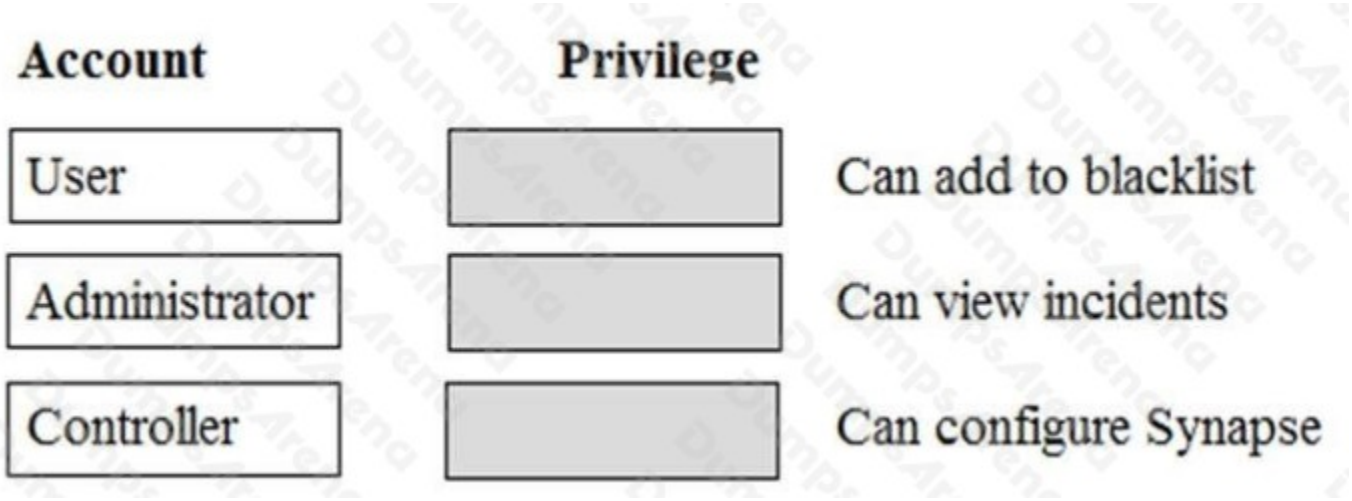
QUESTION NO: 9 - (DRAG DROP)

DRAG DROP

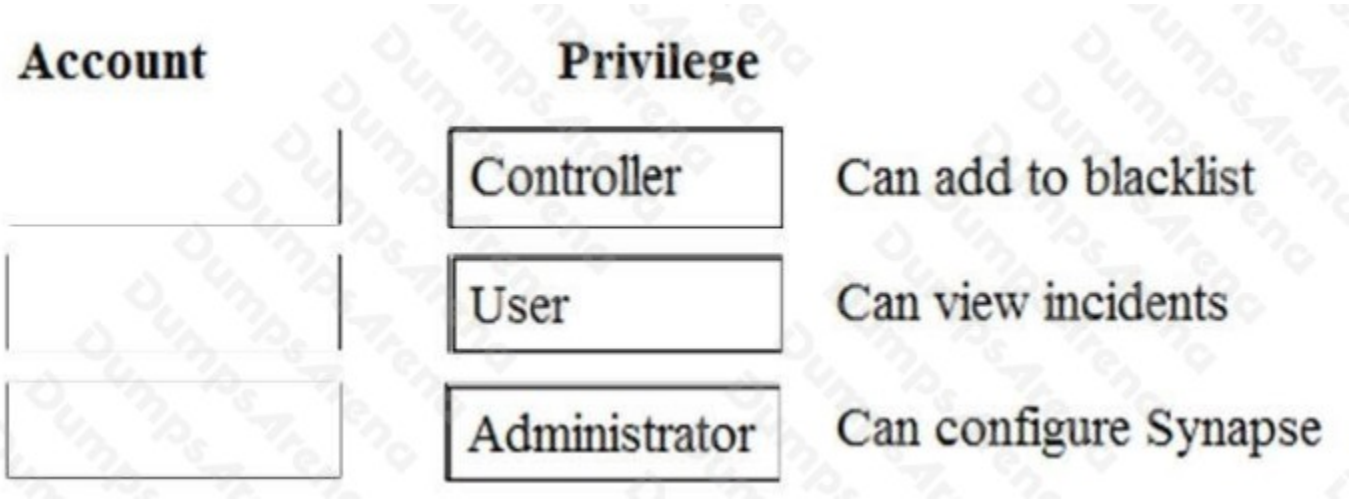
Which level of privilege corresponds to each ATP account type?

Match the correct account type to the corresponding privileges.

Select and Place:



ANSWER:



Explanation:

QUESTION NO: 10

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

ANSWER: D

Explanation:

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