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://dumpsboss.com

support@dumpsboss.com

QUESTION NO: 1

Which section of the ATP console should an ATP Administrator use to create blacklists and whitelists?

A. Reports

B. Settings

C. Action Manager

D. Policies

ANSWER: D

Explanation:

Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10986/en_US/satp_administration_guide_3.1.pdf?

__gda__=1541979133_5668f0b4c03c16ac1a30d54989313e76 (132)

QUESTION NO: 2

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

A. Loyphish

B. Aurora

C. ZeroAccess

D. Michelangelo

ANSWER: B

QUESTION NO: 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

ANSWER: B

QUESTION NO: 4

What are two policy requirements for using the Isolate and Rejoin features in ATP? (Choose two.)

A. Add a Quarantine firewall policy for non-compliant and non-remediated computers.

B. Add a Quarantine LiveUpdate policy for non-compliant and non-remediated computers.

C. Add and assign an Application and Device Control policy in the Symantec Endpoint Protection Manager (SEPM).

D. Add and assign a Host Integrity policy in the Symantec Endpoint Protection Manager (SEPM).

E. Add a Quarantine Antivirus and Antispyware policy for non-compliant and non-remediated computers.

ANSWER: A D

Explanation:

Reference: https://support.symantec.com/en_US/article.HOWTO128427.html

QUESTION NO: 5

Which two widgets can an Incident Responder use to isolate breached endpoints from the Incident details page? (Choose two.)

A. Affected Endpoints

B. Dashboard

C. Incident Graph

D. Events View

E. Actions Bar

ANSWER: C E

Explanation:

Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10899/en_US/satp_security_ops_guide_3.0.5.pdf?

__gda__=1541987119_a3559016c9355c98c2ec53278a8df2a0 (114)

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 runs an endpoint search on a client group with 100 endpoints. After one day, the responder sees the results for 90 endpoints.

What is a possible reason for the search only returning results for 90 of 100 endpoints?

A. The search expired after one hour

B. 10 endpoints are offline

C. The search returned 0 results on 10 endpoints

D. 10 endpoints restarted and cancelled the search

ANSWER: C

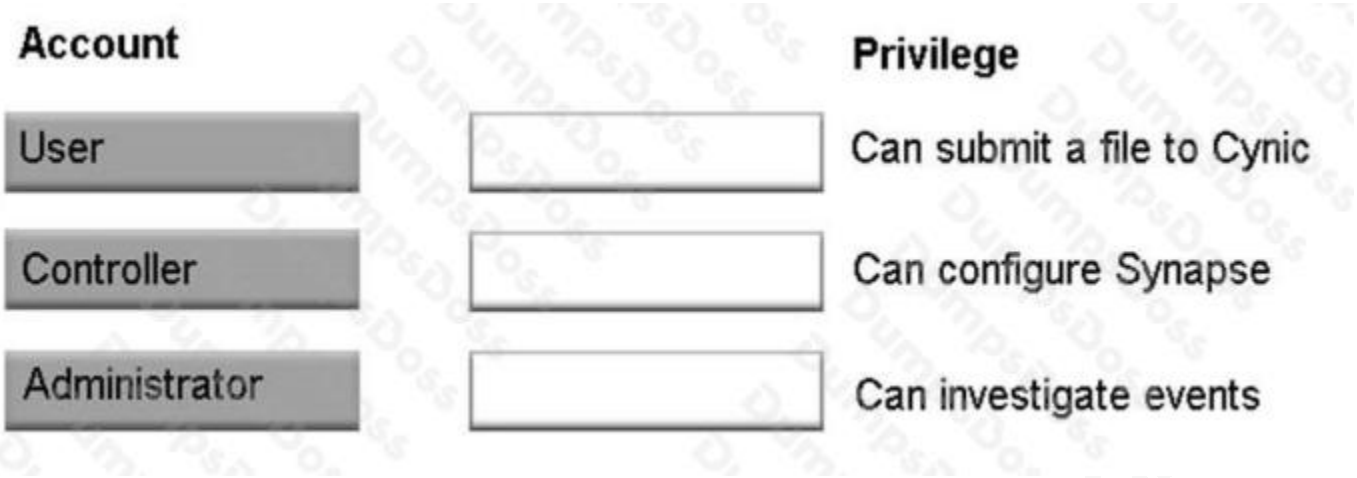
QUESTION NO: 8 - (DRAG DROP)

DRAG DROP

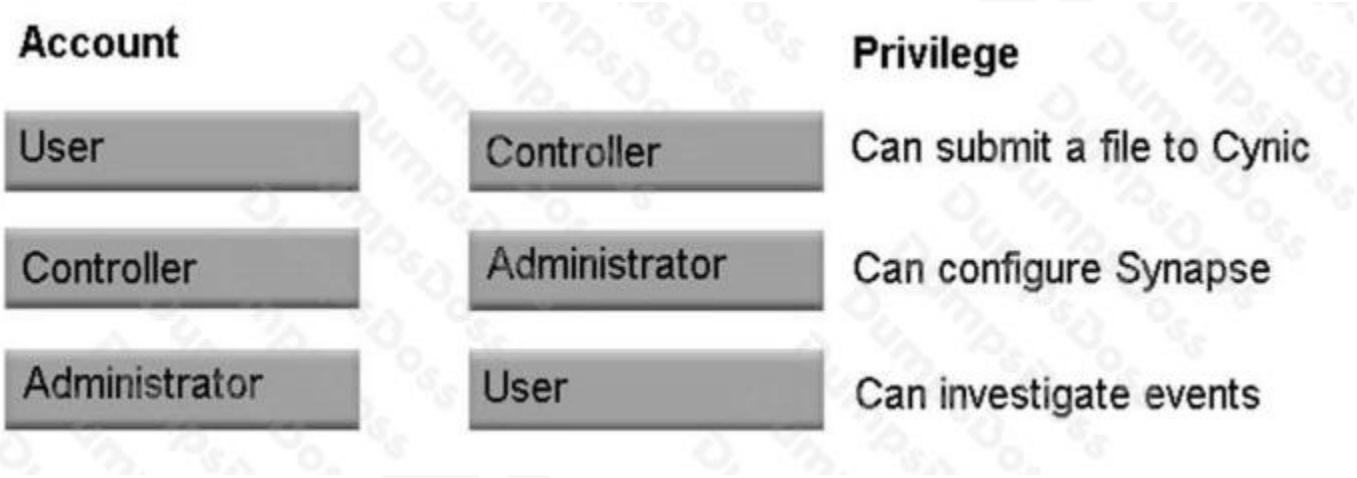
Which level of privilege corresponds to each ATP account type?

Match the correct account type to the corresponding privileges.

Select and Place:



ANSWER:



Explanation:

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

QUESTION NO: 9

Which prerequisite is necessary to extend the ATP: Network solution service in order to correlate email detections?

A. Email Security.cloud

B. Web security.cloud

C. Skeptic

D. Symantec Messaging Gateway

ANSWER: A

Explanation:

Reference: https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpointdetection-and-response-atp-endpoint-en.pdf

QUESTION NO: 10

Which two questions can an Incident Responder answer when analyzing an incident in ATP?

(Choose two.)

A. Does the organization need to do a healthcheck in the environment?

B. Are certain endpoints being repeatedly attacked?

C. Is the organization being attacked by this external entity repeatedly?

D. Do ports need to be blocked or opened on the firewall?

E. Does a risk assessment need to happen in the environment?

ANSWER: B E

DUMPSBOSS.COM