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

Administration of Symantec Advanced Threat Protection 3.0

QUESTION 1

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

Correct Answer: DE

QUESTION 2

How should an ATP Administrator configure Endpoint Detection and Response according to Symantec best practices for a SEP environment with more than one domain?

A. Create a unique Symantec Endpoint Protection Manager (SEPM) domain for ATP

B. Create an ATP manager for each Symantec Endpoint Protection Manager (SEPM) domain

C. Create a Symantec Endpoint Protection Manager (SEPM) controller connection for each domain

D. Create a Symantec Endpoint Protection Manager (SEPM) controller connection for the primary domain

Correct Answer: C

Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10986/en_US/satp_administration_guide_3.1.pdf?__gda__=1541979133_5668f0b4c03c16ac1a30d54989313e76 (46)

QUESTION 3

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.

Correct Answer: AD

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

QUESTION 4

What occurs when an endpoint fails its Host Integrity check and is unable to remediate?

A. The endpoint automatically switches to using a Compliance location, where a Compliance policy is applied to the computer.

B. The endpoint automatically switches to using a System Lockdown location, where a System Lockdown policy is applied to the computer.

C. The endpoint automatically switches to using a Host Integrity location, where a Host Integrity policy is applied to the computer.

D. The endpoint automatically switches to using a Quarantine location, where a Quarantine policy is applied to the computer.

Correct Answer: D

QUESTION 5

What does a Quarantine Firewall policy enable an ATP Administrator to do?

A. Isolate a computer while it is manually being remediated

B. Submit files to a Central Quarantine server

C. Filter all traffic leaving the network

D. Intercept all traffic entering the network

Correct Answer: A