250-441 Q&As

Administration of Symantec Advanced Threat Protection 3.0

QUESTION 1

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 2

Which policies are required for the quarantine feature of ATP to work?

A. Firewall Policy and Host Integrity Policy

B. Quarantine Policy and Firewall Policy

C. Host Integrity Policy and Quarantine Policy

D. Quarantine and Intrusion Prevention Policy

Correct Answer: C

Reference: https://support.symantec.com/us/en/article.tech248959.html

QUESTION 3

An organization has five (5) shops with a few endpoints and a large warehouse where 98% of all computers are located. The shops are connected to the warehouse using leased lines and access internet through the warehouse network.

How should the organization deploy the network scanners to observe all inbound and outbound traffic based on Symantec best practices for Inline mode?

A. Deploy a virtual network scanner at each shop

B. Deploy a virtual network scanner at the warehouse and a virtual network scanner at each shop

C. Deploy a physical network scanner at each shop

D. Deploy a physical network scanner at the warehouse gateway

Correct Answer: D

QUESTION 4

Why is it important for an Incident Responder to review Related Incidents and Events when analyzing an incident for an After Actions Report?

A. It ensures that the Incident is resolved, and the responder can clean up the infection.

B. It ensures that the Incident is resolved, and the responder can determine the best remediation method.

C. It ensures that the Incident is resolved, and the threat is NOT continuing to spread to other parts of the environment.

D. It ensures that the Incident is resolved, and the responder can close out the incident in the ATP manager.

Correct Answer: C

QUESTION 5

What impact does changing from Inline Block to SPAN/TAP mode have on blacklisting in ATP?

A. ATP will continue to block previously blacklisted addresses but NOT new ones.

B. ATP does NOT block access to blacklisted addresses unless block mode is enabled.

C. ATP will clear the existing blacklists.

D. ATP does NOT block access to blacklisted addresses unless TAP mode is enabled.

Correct Answer: B

Reference: https://support.symantec.com/en_US/article.HOWTO125537.html