250-441 Q&As

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

QUESTION 1

During a recent virus outbreak, an Incident Responder found that the Incident Response team was successful in identifying malicious domains that were communicating with the infected endpoints.

Which two options should the Incident Responder select to prevent endpoints from communicating with malicious domains? (Select two.)

A. Use the isolate command in ATP to move all endpoints to a quarantine network.

B. Blacklist suspicious domains in the ATP manager.

C. Deploy a High-Security Antivirus and Antispyware policy in the Symantec Endpoint Protection Manager (SEPM).

D. Create a firewall rule in the Symantec Endpoint Protection Manager (SEPM) or perimeter firewall that blocks traffic to the domain.

E. Run a full system scan on all endpoints.

Correct Answer: DE

Reference: https://www.symantec.com/connect/articles/symantec-endpoint-protection-virus-incidentmanagement

QUESTION 2

Which two steps must an Incident Responder take to isolate an infected computer in ATP? (Choose two.)

A. Close any open shares

B. Identify the threat and understand how it spreads

C. Create subnets or VLANs and configure the network devices to restrict traffic

D. Set executables on network drives as read only

E. Identify affected clients

Correct Answer: AE

QUESTION 3

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 4

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?

Correct Answer: BE

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