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

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

QUESTION 1

An Incident Responder observes an incident with multiple malware downloads from a malicious domain. The domain in question belongs to one of the organization\\'s suppliers. The organization needs access to the site to continue placing orders. ATP: Network is configured in Inline Block mode.

How should the Incident Responder proceed?

A. Whitelist the domain and close the incident as a false positive

B. Identify the pieces of malware and blacklist them, then notify the supplier

C. Blacklist the domain and IP of the attacking site

D. Notify the supplier and block the site on the external firewall

Correct Answer: D

QUESTION 2

What is the role of Cynic within the Advanced Threat Protection (ATP) solution?

A. Reputation-based security

B. Event correlation

C. Network detection component

D. Detonation/sandbox

Correct Answer: D

Reference: https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-advanced-threat-protectionemail-DS-21349610.pdf

QUESTION 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

Correct Answer: B

QUESTION 4

Why is it important for an Incident Responder to copy malicious files to the ATP file store or create an image of the infected system during the Recovery phase?

A. To have a copy of the file policy enforcement

B. To test the effectiveness of the current assigned policy settings in the Symantec Endpoint Protection Manager (SEPM)

C. To create custom IPS signatures

D. To document and preserve any pieces of evidence associated with the incident

Correct Answer: B

QUESTION 5

Which default port does ATP use to communicate with the Symantec Endpoint Protection Manager (SEPM) web services?

A. 8446

B. 8081

C. 8014

D. 1433

Correct Answer: B

Reference: https://support.symantec.com/en_US/article.HOWTO81103.html