Symantec

250-441 Exam

Administration of Symantec Advanced Threat Protection 3.0

Questions & Answers
Demo

Version: 8.0

Question: 1

What is the second stage of an Advanced Persistent Threat (APT) attack?

A. Exfiltration
B. Incursion
C. Discovery
D. Capture

Answer: B

Question: 2

Which SEP technology does an Incident Responder need to enable in order to enforce blacklisting on an
endpoint?

A. System Lockdown
B. Intrusion Prevention System
C. Firewall
D. SONAR

Answer: A

Question: 3

An Incident Responder wants to create a timeline for a recent incident using Syslog in addition to ATP for the
After Actions Report.
What are two reasons the responder should analyze the information using Syslog? (Choose two.)

A. To have less raw data to analyze
B. To evaluate the data, including information from other systems
C. To access expanded historical data
D. To determine what policy settings to modify in the Symantec Endpoint Protection Manager (SEPM)
E. To determine the best cleanup method

Answer: BE

Question: 4

Which SEP technologies are used by ATP to enforce the blacklisting of files?

A. Application and Device Control
B. SONAR and Bloodhound
C. System Lockdown and Download Insight
D. Intrusion Prevention and Browser Intrusion Prevention

Answer: C

Explanation:
Reference: https://support.symantec.com/en_US/article.HOWTO101774.html

Question: 5

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

A. Reputation-based security
B. Detonation/sandbox
C. Network detection component
D. Event correlation

Answer: A

Explanation:
Reference: https://www.symantec.com/content/dam/symantec/docs/brochures/atp-brochure-en.pdf

Question: 6

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: AD

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

Question: 7

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: 8

Which stage of an Advanced Persistent Threat (APT) attack does social engineering occur?

A. Capture
B. Incursion
C. Discovery
D. Exfiltration

Answer: B