Symantec 250-441 Exam

Volume: 70 Questions

Question: 1
Which threat is an example of an Advanced Persistent Threat (APT)?

A. Loyphish

B. Aurora

C. ZeroAccess

D. Michelangelo

Answer: B

Question: 2
Which stage of an Advanced Persistent Threat (APT) attack do attackers break into an organization's network to deliver targeted malware?

A. Incursion

B. Discovery

C. Capture

D. Exfiltration

Answer: A

Question: 3
Which stage of an Advanced Persistent Threat (APT) attack do attackers send information back to the home base?

A. Capture

B. Incursion

C. Discovery

D. Exfiltration

Answer: D

Question: 4
Which service is the minimum prerequisite needed if a customer wants to purchase ATP: Email?

A. Email Protect (antivirus and anti-spam)

B. Email Safeguard (antivirus, anti-spam, encryption, data protection and image control)

C. Symantec Messaging Gateway

D. Skeptic

Answer: A

Question: 5
Which National Institute of Standards and Technology (NIST) cybersecurity function includes Risk Assessment or Risk Management Strategy?

A. Recover

B. Protect

C. Respond

D. Identify

Answer: D

Question: 6
Which attribute is required when configuring the Symantec Endpoint Protection Manager (SEPM) Log Collector?

A. SEPM embedded database name

B. SEPM embedded database type

C. SEPM embedded database version

D. SEPM embedded database password

Answer: D

Question: 7
Which prerequisite is necessary to extend the ATP: Network solution service in order to correlate email detections?

A. Email Security cloud

B. Web security cloud

C. Skeptic

D. Symantec Messaging Gateway

Answer: A

Question: 8
Which two widgets can an Incident Responder use to isolate breached endpoints from the Incident details page? (Choose two.)

A. Affected Endpoints

B. Dashboard

C. Incident Graph

D. Events View

E. Actions Bar

Answer: C,E

Question: 9
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

Answer: A

Question: 10
A large company has 150,000 endpoints with 12 SEP sites across the globe. The company now wants to implement ATP: Endpoint to improve their security. However, a consultant recently explained that the company needs to implement more than one ATP manager.
Why does the company need more than one ATP manager?

A. An ATP manager can only connect to a SQL backend

B. An ATP manager can only support 30,000 SEP clients

C. An ATP manager can only support 10 SEP site connections.

D. An ATP manager needs to be installed at each location where a Symantec Endpoint Protection Manager (SEPM) is located.

Answer: D

Question: 11
A medium-sized organization with 10,000 users at Site A and 20,000 users at Site B wants to use ATP: Network to scan internet traffic at both sites.
Which physical appliances should the organization use to act as a network scanner at each site while using the fewest appliances and assuming typical network usage?

A. Site A 8840 x4 – Site B 8880 x2

B. Site A 8880 x2 – Site B 8840 x1

C. Site A 8880 x1 – Site B 8840 x6

D. Site A 8880 x1 – Site B 8880 x2

Answer: D

Question: 12
What is a benefit of using Microsoft SQL as the Symantec Endpoint Protection Manager (SEPM) database in regard to ATP?

A. It allows for Microsoft Incident Responders to assist in remediation

B. ATP can access the database using a log collector on the SEPM host

C. It allows for Symantec Incident Responders to assist in remediation

D. ATP can access the database without any special host system requirements

Answer: D

Question: 13
Which two questions can an Incident Responder answer when analyzing an incident in ATP? (Choose two.)

A. Does the organization need to do a health check 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?

Answer: B,E

Question: 14
Which National Institute of Standards and Technology (NIST) cybersecurity function is defined as “finding incursions”?

A. Protect

B. Identify

C. Respond

D. Detect

Answer: B