Question 1

Which Antimalware technology is used after all local resources have been exhausted?

Options:

A- Sapient

B- ITCS

C- Emulator

D- Reputation

Answer:

B

Question 2

Which report template out format should an administrator utilize to generate graphical reports?

Options:

A- XML

B- HTML

C- PFD

D- XML

Answer:

B

Question 3

Question Type: **MultipleChoice**

An administrator learns of a potentially malicious file and wants to proactively prevent the file from ever being executed.

What should the administrator do?

Options:

A- Add the file SHA1 to a blacklist policy

B- Increase the Antimalware policy Intensity to Level 5

C- Add the filename and SHA-256 hash to a Blacklist policy

D- Adjust the Antimalware policy age and prevalence settings

Answer:

D

Question 4

Question Type: MultipleChoice

What version number is assigned to a duplicated policy?

Options:

A- One

B- Zero

C- The original policy's number plus one

D- The original policy's version numb

Answer:

C

Question 5

Question Type: MultipleChoice

What characterizes an emerging threat in comparison to traditional threat?

Options:

A- Emerging threats use new techniques and 0-day vulnerability to propagate.

B- Emerging threats requires artificial intelligence to be detected.

C- Emerging threats are undetectable by signature based engines.

D- Emerging threats are more sophisticated than traditional threats.

Answer:

A

Question 6

Question Type: MultipleChoice

Which Security Control dashboard widget should an administrator utilize to access detailed areas for a given security control ?

Options:

A- Learn More

B- Quick Links

C- More Info

D- Latest Tasks

Answer:

D

Question 7

Which Endpoint > Setting should an administrator utilize to locate unmanaged endpoints on a network subnet?

Options:

A- Discover Endpoints

B- Endpoint Enrollment

C- Discover and Deploy

D- Device Discovery

Answer:

A

Question 8

Which SES advanced feature detects malware by consulting a training model composed of known good and known bad fries?

Options:

A- Signatures

B- Advanced Machine Learning

C- Reputation

D- Artificial Intelligence

Answer:

B

Question 9

Question Type: MultipleChoice

What should an administrator know regarding the differences between a Domain and a Tenant in ICDm?

A- A tenant can contain multiple domains

B- A domain can contain multiple tenants

C- Each customer can have one domain and many tenant

D- Each customer can have one tenant and many domains

Answer:

A

Question 10

Question Type: **MultipleChoice**

What is the primary issue pertaining to managing roaming users while utilizing an on-premise solution?

Options:

A- The endpoint is missing timely policy update

B- The endpoint is absent of the management console

C- The endpoint fails to receive content update

D- The endpoint is more exposed to threats

Answer:

C

Question 11

Question Type: MultipleChoice

Which type of security threat is used by attackers to exploit vulnerable applications?

Options:

A- Lateral Movement

B- Privilege Escalation

C- Command and Control

D- Credential Access

Question 12

Question Type: **MultipleChoice**

An endpoint is offline, and the administrator issues a scan command. What happens to the endpoint when it restarts, if it lacks connectivity?

Options:

A- The system is scanning when started.

B- The system downloads the content without scanning.

C- The system starts without scanning.

D- The system scans after the content update is downloaded.

Answer:

B