Question 1

Which option describes Spero file analysis?

Options:

A- a method of analyzing the SHA-256 hash of a file to determine whether a file is malicious or not

B- a method of analyzing the entire contents of a file to determine whether it is malicious or not

C- a method of analyzing certain file characteristics, such as metadata and header information, to determine whether a file is malicious or not

D- a method of analyzing a file by executing it in a sandbox environment and observing its behaviors to determine if it is malicious or not

Answer:

C

Question 2

Which statement is true regarding malware blocking over HTTP?

Options:

A- It can be done only in the download direction.

B- It can be done only in the upload direction.

C- It can be done in both the download and upload direction.

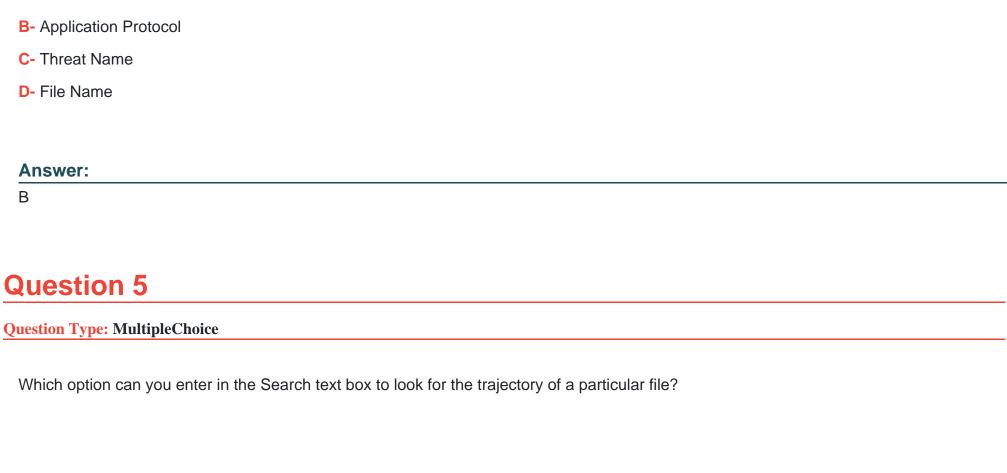**D-** HTTP is not a supported protocol for malware blocking.

Answer:

C

Question 3

Question Type: **MultipleChoice**

Which policy controls malware blocking configuration?

A- file policy

B- malware policy

C- access control policy

D- IPS policy

Answer:

A

Question 4

Question Type: **MultipleChoice**

A context box opens when you click on an event icon in the Network File Trajectory map for a file. Which option is an element of the box?

Options:

A- Scan

B- Application Protocol

C- Threat Name

D- File Name

Answer:

B

Question 5

Question Type: MultipleChoice

Which option can you enter in the Search text box to look for the trajectory of a particular file?

Options:

A- the MD5 hash value of the file

B- the SHA-256 hash value of the file

C- the URL of the file

D- the SHA-512 hash value of the file

Answer:

B

Question 6

Question Type: MultipleChoice

Other than navigating to the Network File Trajectory page for a file, which option is an alternative way of accessing the network trajectory of a file?

Options:

A- from Context Explorer

B- from the Analysis menu

C- from the cloud

D- from the Defense Center

Answer:

A

Question 7

Question Type: MultipleChoice

A user discovery agent can be installed on which platform?

Options:

A- OpenLDAP

B- Windows

C- RADIUS

D- Ubuntu

Answer:

B

Question 8

Question Type: MultipleChoice

In addition to the discovery of new hosts, FireSIGHT can also perform which function?

Options:

A- block traffic

B- determine which users are involved in monitored connections

C- discover information about users

D- route traffic

Answer:

B

Question 9

The IP address ::/0 is equivalent to which IPv4 address and netmask?

Options:

A- 0.0.0.0

B- 0.0.0.0/0

C- 0.0.0.0/24

D- The IP address ::/0 is not valid IPv6 syntax.

Answer:

B