DUMPSsheet

Free Questions for 500-285 by dumpssheet

Shared by Lee on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which option is true of the Packet Information portion of the Packet View screen?

Options:

A- provides a table view of events

B- allows you to download a PCAP formatted file of the session that triggered the event

C- displays packet data in a format based on TCP/IP layers

D- shows you the user that triggered the event

Answer:

C

Question 2

Question Type: MultipleChoice

Which option is not a characteristic of dashboard widgets or Context Explorer?

Options:

A- Context Explorer is a tool used primarily by analysts looking for trends across varying periods of time.

B- Context Explorer can be added as a widget to a dashboard.

C- Widgets offer users an at-a-glance view of their environment.

D- Widgets are offered to all users, whereas Context Explorer is limited to a few roles.

Answer:

B

Question 3

Question Type: MultipleChoice

One of the goals of geolocation is to identify which option?

Options:

A- the location of any IP address

B- the location of a MAC address

C- the location of a TCP connection

D- the location of a routable IP address

Answer:

D

Question 4

Question Type: **MultipleChoice**

Which option is true when configuring an access control rule?

Options:

A- You can use geolocation criteria to specify source IP addresses by country and continent, as well as destination IP addresses by country and continent.

B- You can use geolocation criteria to specify destination IP addresses by country but not source IP addresses.

C- You can use geolocation criteria to specify source and destination IP addresses by country but not by continent.

D- You can use geolocation criteria to specify source and destination IP addresses by continent but not by country.

Answer:

A

Question 5

Question Type: **MultipleChoice**

Which statement is true when adding a network to an access control rule?

Options:

A- You can select only source networks.

B- You must have preconfigured the network as an object.

C- You can select the source and destination networks or network groups.

D- You cannot include multiple networks or network groups as sources or destinations.

Answer:

C

Question 6

Question Type: **MultipleChoice**

Which option transmits policy-based alerts such as SNMP and syslog?

Options:

A- the Defense Center

B- FireSIGHT

C- the managed device

D- the host

Answer:

C

Question 7

Question Type: **MultipleChoice**

Access control policy rules can be configured to block based on the conditions that you specify in each rule. Which behavior block response do you use if you want to deny and reset the connection of HTTP traffic that meets the conditions of the access control rule?

Options:

A- interactive block with reset

B- interactive block

C- block

D- block with reset

Answer:

D

Question 8

Question Type: **MultipleChoice**

When adding source and destination ports in the Ports tab of the access control policy rule editor, which restriction is in place?

Options:

A- The protocol is restricted to TCP only.

B- The protocol is restricted to UDP only.

C- The protocol is restricted to TCP or UDP.

D- The protocol is restricted to TCP and UDP.

Answer:

C

Question 9

Question Type: MultipleChoice

How do you configure URL filtering?

Options:

A- Add blocked URLs to the global blacklist.

B- Create a Security Intelligence object that contains the blocked URLs and add the object to the access control policy.

C- Create an access control rule and, on the URLs tab, select the URLs or URL categories that are to be blocked or allowed.

D- Create a variable.

Answer:

C

Question 10

Question Type: MultipleChoice

Which statement is true in regard to the Sourcefire Security Intelligence lists?

Options:

A- The global blacklist universally allows all traffic through the managed device.

B- The global whitelist cannot be edited.

C- IP addresses can be added to the global blacklist by clicking on interactive graphs in Context Explorer.

D- The Security Intelligence lists cannot be updated.

Answer:

C

Question 11

Question Type: **MultipleChoice**

Which option is one of the three methods of updating the IP addresses in Sourcefire Security Intelligence?

Options:

A- subscribe to a URL intelligence feed

B- subscribe to a VRT

C- upload a list that you create

D- automatically upload lists from a network share

Answer:

C

Question 12

Question Type: **MultipleChoice**

Which option is true regarding the $HOME_NET variable?

Options:

A- is a policy-level variable

B- has a default value of 'all'

C- defines the network the active policy protects

D- is used by all rules to define the internal network

Answer:

C