DUMPSARENA

Securing Cisco Networks with Sourcefire IPS

Cisco 500-285

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Object Management	4
Topic 2, Access Control Policy	6
Topic 3, Event Analysis	3
Topic 4, IPS Policy Basics	3
Topic 5, FireSIGHT Technologies	7
Topic 6, Network Based Malware Detection	6
Topic 7, Basic Administration	7
Topic 8, Account Management	3
Topic 9, Creating Snort Rules	3
Topic 10, Device Management	6
Topic 11, Correlation Policies	6
Topic 12, Advanced IPS Policy Configuration	6
Total	60

QUESTION NO: 1

What does the whitelist attribute value "not evaluated" indicate?

A. The host is not a target of the whitelist.

B. The host could not be evaluated because no profile exists for it.

C. The whitelist status could not be updated because the correlation policy it belongs to is not enabled.

D. The host is not on a monitored network segment.

ANSWER: A

QUESTION NO: 2

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

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

QUESTION NO: 3

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

A. the Defense Center

B. FireSIGHT

C. the managed device

D. the host

ANSWER: C

QUESTION NO: 4

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

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 NO: 5

Which statement describes the meaning of a red health status icon?

A. A critical threshold has been exceeded.

B. At least one health module has failed.

C. A health policy has been disabled on a monitored device.

D. A warning threshold has been exceeded.

ANSWER: A

QUESTION NO: 6

Which option is a remediation module that comes with the Sourcefire System?

A. Cisco IOS Null Route

B. Syslog Route

C. Nmap Route Scan

D. Response Group

ANSWER: A

QUESTION NO: 7

Where do you configure widget properties?

A. dashboard properties

B. the Widget Properties button in the title bar of each widget

C. the Local Configuration page

D. Context Explorer

ANSWER: B

QUESTION NO: 8

FireSIGHT uses three primary types of detection to understand the environment in which it is deployed. Which option is one of the detection types?

A. protocol layer

B. application

C. objects

D. devices

ANSWER: B

QUESTION NO: 9

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

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 NO: 10

Which option is derived from the discovery component of FireSIGHT technology?

A. connection event table view

B. network profile

C. host profile

D. authentication objects

ANSWER: C