Free Questions for 500-285 by certsinside

Shared by Heath on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- connection event table view

B- network profile

C- host profile

D- authentication objects

Answer:

C

Question 2

Question Type: MultipleChoice

When configuring FireSIGHT detection, an administrator would create a network discovery policy and set the action to "discover". Which option is a possible type of discovery?

Options:

A- host

B- IPS event

C- anti-malware

D- networks

Answer:

A

Question 3

Question Type: **MultipleChoice**

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

Options:

A- protocol layer

B- application

C- objects

D- devices

Answer:

B

Question 4

Question Type: **MultipleChoice**

Host criticality is an example of which option?

Options:

A- a default whitelist

B- a default traffic profile

C- a host attribute

D- a correlation policy

Answer:

C

Question 5

Question Type: MultipleChoice

FireSIGHT recommendations appear in which layer of the Policy Layers page?

Options:

A- Layer Summary

B- User Layers

C- Built-In Layers

D- FireSIGHT recommendations do not show up as a layer.

Answer:

C

Question 6

Question Type: **MultipleChoice**

When you are editing an intrusion policy, how do you know that you have changes?

Options:

A- The Commit Changes button is enabled.

B- A system message notifies you.

C- You are prompted to save your changes on every screen refresh.

D- A yellow, triangular icon displays next to the Policy Information option in the navigation panel.

Answer:

D

Question 7

Question Type: MultipleChoice

Which option is used to implement suppression in the Rule Management user interface?

Options:

A- Rule Category

B- Global

C- Source

D- Protocol

Answer:

C

20%
DISCOUNT