Free Questions for 500-285 by certscare

Shared by Mcfadden on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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 2

Question Type: MultipleChoice

Which statement is true when network traffic meets the criteria specified in a correlation rule?

Options:

A- Nothing happens, because you cannot assign a group of rules to a correlation policy.

B- The network traffic is blocked.

C- The Defense Center generates a correlation event and initiates any configured responses.

D- An event is logged to the Correlation Policy Management table.

Answer:

C

Question 3

Question Type: **MultipleChoice**

Stacking allows a primary device to utilize which resources of secondary devices?

Options:

A- interfaces, CPUs, and memory

B- CPUs and memory

C- interfaces, CPUs, memory, and storage

D- interfaces and storage

Answer:

B

Question 4

Question Type: **MultipleChoice**

Which interface type allows for bypass mode?

Options:

A- inline

B- switched

C- routed

D- grouped

Answer:

A

Question 5

Question Type: MultipleChoice

The gateway VPN feature supports which deployment types?

Options:

A- SSL and HTTPS

B- PPTP and MPLS

C- client and route-based

D- point-to-point, star, and mesh

Answer:

D

Question 6

Question Type: MultipleChoice

Which mechanism should be used to write an IPS rule that focuses on the client or server side of a TCP communication?

Options:

A- the directional operator in the rule header

B- the 'flow' rule option

C- specification of the source and destination ports in the rule header

D- The detection engine evaluates all sides of a TCP communication regardless of the rule options.

Answer:

B

Question 7

Question Type: MultipleChoice

Which option describes the two basic components of Sourcefire Snort rules?

Options:

A- preprocessor configurations to define what to do with packets before the detection engine sees them, and detection engine configurations to define exactly how alerting is to take place

B- a rule statement characterized by the message you configure to appear in the alert, and the rule body that contains all of the matching criteria such as source, destination, and protocol

C- a rule header to define source, destination, and protocol, and the output configuration to determine which form of output to produce if the rule triggers

D- a rule body that contains packet-matching criteria or options to define where to look for content in a packet, and a rule header to define matching criteria based on where a packet originates, where it is going, and over which protocol

Answer:

D