500-285 Q&As

Securing Cisco Networks with FireSIGHT Intrusion Prevention System (SSFIPS)

Pass Cisco 500-285 Exam with 100% Guarantee

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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.

Correct Answer: B

QUESTION 2

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

A. block traffic

B. determine which users are involved in monitored connections

C. discover information about users

D. route traffic

Correct Answer: B

QUESTION 3

Which option is a valid whitelist evaluation value?

A. pending

B. violation

C. semi-compliant

D. not-evaluated

Correct Answer: D

QUESTION 4

Which option is true regarding the $HOME_NET variable?

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

Correct Answer: C

QUESTION 5

Which interface type allows for VLAN tagging?

A. inline

B. switched

C. high-availability link

D. passive

Correct Answer: B

QUESTION 6

Suppose an administrator is configuring an IPS policy and attempts to enable intrusion rules that require the operation of the TCP stream preprocessor, but the TCP stream preprocessor is turned off. Which statement is true in this situation?

A. The administrator can save the IPS policy with the TCP stream preprocessor turned off, but the rules requiring its operation will not function properly.

B. When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the TCP stream preprocessor will be turned on for the IPS policy.

C. The administrator will be prevented from changing the rule state of the rules that require the TCP stream preprocessor until the TCP stream preprocessor is enabled.

D. When the administrator enables the rules and then attempts to save the IPS policy, the administrator will be prompted to accept that the rules that require the TCP stream preprocessor will be turned off for the IPS policy.

Correct Answer: B

QUESTION 7

Which option describes Spero file analysis?

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

Correct Answer: C

QUESTION 8

Correlation policy rules allow you to construct criteria for alerting on very specific conditions. Which option is an example of such a rule?

A. testing password strength when accessing an application

B. limiting general user access to administrative file shares

C. enforcing two-factor authentication for access to critical servers

D. issuing an alert if a noncompliant operating system is detected or if a host operating system changes to a noncompliant operating system when it was previously profiled as a compliant one

Correct Answer: D

QUESTION 9

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

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

Correct Answer: D

QUESTION 10

Which list identifies the possible types of alerts that the Sourcefire System can generate as notification of events or policy violations?

A. logging to database, SMS, SMTP, and SNMP

B. logging to database, SMTP, SNMP, and PCAP

C. logging to database, SNMP, syslog, and email

D. logging to database, PCAP, SMS, and SNMP

Correct Answer: C