500-285 Q&As

Securing Cisco Networks with FireSIGHT Intrusion Prevention System (SSFIPS)

Pass Cisco 500-285 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/500-285.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

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

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.

Correct Answer: C

QUESTION 3

The collection of health modules and their settings is known as which option?

A. appliance policy

B. system policy

C. correlation policy

D. health policy

Correct Answer: D

QUESTION 4

Which option is a valid whitelist evaluation value?

A. pending

B. violation

C. semi-compliant

D. not-evaluated

Correct Answer: D

QUESTION 5

Which Sourcefire feature allows you to send traffic directly through the device without inspecting it?

A. fast-path rules

B. thresholds or suppressions

C. blacklist

D. automatic application bypass

Correct Answer: A