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.pass2lead.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

A user discovery agent can be installed on which platform?

A. OpenLDAP

B. Windows

C. RADIUS

D. Ubuntu

Correct Answer: B Testlet 1

TESTLET OVERVIEW

Title: Case Study

The following testlet will present a Case Study followed by [count] multiple choice question(s), [count] create a tree question(s), [count] build list and reorder question(s) and [count] drop and connect question (s).

You will have [count] minutes to complete the testlet.

For help on how to answer the questions, click the Instuctions button on the question screen.

QUESTION 2

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

A. the Defense Center

B. FireSIGHT

C. the managed device

D. the host

Correct Answer: C

QUESTION 3

Which statement represents detection capabilities of the HTTP preprocessor?

A. You can configure it to blacklist known bad web servers.

B. You can configure it to normalize cookies in HTTP headers.

C. You can configure it to normalize image content types.

D. You can configure it to whitelist specific servers.

Correct Answer: B

QUESTION 4

When configuring an LDAP authentication object, which server type is available?

A. Microsoft Active Directory

B. Yahoo

C. Oracle

D. SMTP

Correct Answer: A

QUESTION 5

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