Vendor: Cisco

Exam Code:500-275

Exam Name: Securing Cisco Networks with Sourcefire FireAMP Endpoints (SSFAMP)

Version: Demo

QUESTION 1

When you are viewing information about a computer, what is displayed?

A. the type of antivirus software that is installed

B. the internal IP address

C. when the operating system was installed

D. the console settings

Correct Answer: B

QUESTION 2

For connector-to-FireAMP Private Cloud communication, which port number is used for lower- overhead communication?

A. 22

B. 80

C. 443

D. 32137

Correct Answer: D

QUESTION 3

In a FireAMP Private Cloud installation, an administrator uses which server to configure the FireAMP Private Cloud properties?

A. opadmin..com

B. console..com

C. cloud..com

D. aws..com

Correct Answer: A

QUESTION 4

In a FireAMP Private Cloud installation, deployed connectors communicate with which server?

A. opadmin..com

B. console..com

C. cloud..com

D. aws..com

Correct Answer: C

QUESTION 5

How does application blocking enhance security?

A. It identifies and logs usage.

B. It tracks application abuse.

C. It deletes identified applications.

D. It blocks vulnerable applications from running, until they are patched.

Correct Answer: D

QUESTION 6

How can customers feed new intelligence such as files and hashes to FireAMP?

A. by uploading it to the FTP server

B. from the connector

C. through the management console

D. by sending it via email

Correct Answer: C

QUESTION 7

Which hosts merit special consideration for crafting a policy?

A. end-user hosts

B. domain controllers

C. Linux servers

D. none, because all hosts should get equal consideration

Correct Answer: B

QUESTION 8

The FireAMP connector supports which proxy type?

A. SOCKS6

B. HTTP_proxy

C. SOCKS5_filename

D. SOCKS7

Correct Answer: B

QUESTION 9

Which action can you take from the Detections/Quarantine screen?

A. Create a policy.

B. Restore the detected file.

C. Run a report.

D. Change computer group membership.

Correct Answer: B

QUESTION 10

Where is the File Fetch context menu option available?

A. anywhere a filename or SHA-256 hash is displayed

B. only from the Filter Event View page

C. from the Audit Event page

D. from the configuration in the Business Defaults page

Correct Answer: A

QUESTION 11

Which pair represents equivalent processes whose names differ, depending on the connector version that you are running?

A. immunet_protect and iptray

B. agent.exe and sfc.exe

C. TETRA and SPERO

D. ETHOS and SPERO

Correct Answer: B

QUESTION 12

What do policies enable you to do?

A. specify a custom whitelist

B. specify group membership

C. specify hosts to include in reports

D. specify which events to view

Correct Answer: A