500-275 Q&As

Securing Cisco Networks with Sourcefire FireAMP Endpoints (SSFAMP)

Pass Cisco 500-275 Exam with 100% Guarantee

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

https://www.pass2lead.com/500-275.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

The FireAMP connector supports which proxy type?

A. SOCKS6

B. HTTP_proxy

C. SOCKS5_filename

D. SOCKS7

Correct Answer: B

QUESTION 3

The Update Window allows you to perform which action?

A. identify which hosts need to be updated

B. email the user to download a new client

C. specify a timeframe when an upgrade can be started and stopped

D. update your cloud instance

Correct Answer: C

QUESTION 4

Where does an administrator go to get a copy of a fetched file?

A. the Business Defaults page

B. the File menu, followed by Downloads

C. the File Repository

D. the Search selection in the Analysis menu

Correct Answer: C

QUESTION 5

Which disposition can be returned in response to a malware cloud lookup?

A. Dirty

B. Virus

C. Malware

D. Infected

Correct Answer: C

QUESTION 6

When discussing the FireAMP product, which term does the acronym DFC represent?

A. It means Detected Forensic Cause.

B. It means Duplicate File Contents.

C. It means Device Flow Correlation.

D. It is not an acronym that is associated with the FireAMP product.

Correct Answer: C

QUESTION 7

Which set of actions would you take to create a simple custom detection?

A. Add a SHA-256 value; upload a file to calculate a SHA-256 value; upload a text file that contains SHA256 values.

B. Upload a packet capture; use a Snort rule; use a ClamAV rule.

C. Manually input the PE header data, the MD-5 hash, and a list of MD-5 hashes.

D. Input the file and file name.

Correct Answer: A

QUESTION 8

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 9

Which question should be in your predeployment checklist?

A. How often are backup jobs run?

B. Are any Linux servers being deployed?

C. Who are the users of the hosts on which you will deploy?

D. Which applications are installed on the hosts on which you will deploy?

Correct Answer: D

QUESTION 10

Which FireAMP capability can tell you how malware has spread in a network?

A. File Analysis

B. Threat Root Cause

C. File Trajectory

D. Heat Map

Correct Answer: C