# 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.certbus.com/500-275.html**

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

**QUESTION 1**

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 2**

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 3**

Custom whitelists are used for which purpose?

A. to specify which files to alert on

B. to specify which files to delete

C. to specify which files to ignore

D. to specify which files to sandbox

Correct Answer: C

**QUESTION 4**

What is a valid data source for DFC Windows connector policy configuration?

A. SANS

B. NIST

C. Emerging Threats

D. Custom and Sourcefire

Correct Answer: D

**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**

If a file\\'s SHA-256 hash is sent to the cloud, but the cloud has never seen the hash before, which disposition is returned?

A. Clean

B. Neutral

C. Malware

D. Unavailable

Correct Answer: B

**QUESTION 7**

Which statement is true about the Device Trajectory feature?

A. It shows where the endpoint devices have moved in your environment by displaying each IP address that a device has had over time.

B. A "plus" sign on the File Trajectory map indicates that you can execute the file inside FireAMP.

C. In the File Trajectory map, you can view the parent process for a file by selecting the infected system.

D. It shows hosts that display Indications of Compromise.

Correct Answer: C

**QUESTION 8**

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 9**

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 10**

In a FireAMP Private Cloud installation, which server does an administrator use to manage connector policy and view events?

A. opadmin..com

B. console..com

C. cloud..com

D. aws..com

Correct Answer: B