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.geekcert.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

Which feature allows retrospective detection?

A. Total Recall

B. Cloud Recall

C. Recall Alert

D. Recall Analysis

Correct Answer: B

QUESTION 2

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 3

Incident responders use which policy mode for outbreak control?

A. Audit

B. Protect

C. Triage

D. Emergency

Correct Answer: C

QUESTION 4

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 5

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

Latest 500-275 Dumps   500-275 VCE Dumps   500-275 Exam Questions