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 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 2

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 3

Incident responders use which policy mode for outbreak control?

A. Audit

B. Protect

C. Triage

D. Emergency

Correct Answer: C

QUESTION 4

From the Deployment screen, you can deploy agents via which mechanism?

A. push to client

B. .zip install file

C. user download from Sourcefire website or email

D. precompiled RPM package

Correct Answer: C

QUESTION 5

FireAMP reports can be distributed by which mechanism?

A. email

B. cloud sync

C. Windows file share

D. a Crystal Reports subscription

Correct Answer: A

Latest 500-275 Dumps   500-275 Practice Test   500-275 Braindumps