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.passapply.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 statement represents a best practice for deploying on Windows servers?

A. You should treat Windows servers like any other host in the deployment.

B. You should obtain the Microsoft TechNet article that describes the proper exclusions for Windows servers.

C. You should never configure exclusions for Windows servers.

D. You should deploy FireAMP connectors only alongside existing antivirus software on Windows servers.

Correct Answer: B

QUESTION 2

Which option represents a configuration step on first use?

A. Verify, Contain, and Protect

B. User Account Setup

C. System Defaults Configuration

D. Event Filtering

Correct Answer: A

QUESTION 3

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 4

Which tool can you use to query the history.db file?

A. Curl

B. FireAMP_Helper.vbs

C. cscript

D. SQLite

Correct Answer: D Question Set 1

QUESTION 5

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

[500-275 PDF Dumps](#)   [500-275 VCE Dumps](#)   [500-275 Study Guide](#)