

Real4Test

Real4test

Latest updated materials, Daily Updates!



ORACLE®



<http://www.real4test.com>

Real IT Certification Exam Study materials/Braindumps

Exam : **500-275**

Title : Securing Cisco Networks with Sourcefire FireAMP Endpoints

Vendor : Cisco

Version : DEMO

NO.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.

Answer: B

NO.2 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.

Answer: D

NO.3 Incident responders use which policy mode for outbreak control?

- A. Audit
- B. Protect
- C. Triage
- D. Emergency

Answer: C

NO.4 How many days' worth of data do the widgets on the dashboard page display?

- A. the previous 5 days of data
- B. the previous 6 days of data
- C. the previous 7 days of data
- D. the number of days you set in the dashboard configuration

Answer: C

NO.5 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.

Answer: B

NO.6 Which type of activity is shown in the Device Trajectory page?

- A. the IP addresses of hosts on which a file was seen
- B. the activity of the FireAMP console users
- C. the hosts that are in the same group as the selected host
- D. file creation

Answer: D