



Pass4IT

Cisco
500-275

QUESTIONS AND ANSWERS

FREE VERSION

(LIMITED CONTENT)

Thank you for downloading our reliable exam questions
for more exams you can visit:

<https://www.pass4it.com/all-vendors>

Dumps Questions 500-275

Exam Name: Securing Cisco Networks with Sourcefire FireAMP Endpoints

Certification Provider: Cisco

Exam: Securing Cisco Networks with Sourcefire FireAMP Endpoints

Question #1

Incident responders use which policy mode for outbreak control?

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

Correct Answer: C

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

fit answer.

Question #3

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

Question #4

What is the first system that is infected with a particular malware called?

A. Patient Zero

B. Source

C. Infector

D. Carrier

Correct Answer: A

Question #5

Which information does the File Trajectory feature show?

A. the time that the scan was run

B. the name of the file

C. the hosts on which the file was seen and points in time where events occurred

D. the protocol

Correct Answer: C

verified answer.