Demo Questions

Cisco 500-275 Exam

Securing Cisco Networks with Sourcefire FireAMP Endpoints

Question #1 ***Topic 1***

Incident responders use which policy mode for outbreak control?

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

Correct Answer: *C*

Question #2 ***Topic 1***

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*Topic 1*

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*Topic 1*

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*Topic 1*

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.

Question #6*Topic 1*

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.

Correct Answer: *B*