Cisco

Exam 500-275

Securing Cisco Networks with Sourcefire FireAMP Endpoints

Version: 6.0

[Total Questions: 50]

Question No : 1

The FireAMP connector monitors the system for which type of activity?

A. vulnerabilities
B. enforcement of usage policies
C. file operations
D. authentication activity

Answer: C

Question No : 2

Which disposition can be returned in response to a malware cloud lookup?

A. Dirty
B. Virus
C. Malware
D. Infected

Answer: C

Question No : 3

The FireAMP Mobile endpoint connector currently supports which mobile OS device?

A. Firefox
B. HTML5
C. Android
D. iPhone

Answer: C

Question No : 4

If a file's SHA-256 hash is sent to the cloud, but the cloud has never seen the hash before, which disposition is returned?

A. Clean
B. Neutral
C. Malware
D. Unavailable

Answer: B

Question No : 5

Which statement describes an advantage of the FireAMP product?

A. Signatures are pushed to endpoints more quickly than other antivirus products.
B. Superior detection algorithms on the endpoint limit the amount of work the cloud must perform.
C. It provides enterprise visibility.
D. It relies on sandboxing.

Answer: C

Question No : 6

Which feature allows retrospective detection?

A. Total Recall
B. Cloud Recall
C. Recall Alert
D. Recall Analysis

Answer: B

Question No : 7

Which statement describes an advantage of cloud-based detection?

A. Limited customization allows for faster detection.
B. Fewer resources are required on the endpoint.
C. Sandboxing reduces the overall management overhead of the system.