ISLEVER

500-275

Securing Cisco Networks with Sourcefire FireAMP Endpoints

DEMO

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
Explanation:

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
Explanation:

QUESTION NO: 3

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

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

Answer: C
Explanation:

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
Explanation:

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
Explanation:

QUESTION NO: 6

Which feature allows retrospective detection?

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

Answer: B
Explanation:

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.
D. High-speed analytical engines on the endpoint limit the amount of work the cloud must perform.

Answer: B
Explanation:

QUESTION NO: 8

Which option is a detection technology that is used by FireAMP?

A. fuzzy matching
B. Norton AntiVirus
C. network scans
D. Exterminator

Answer: A
Explanation:

QUESTION NO: 9

File information is sent to the Sourcefire Collective Security Intelligence Cloud using which format?

A. MD5
B. SHA-1
C. filenames
D. SHA-256

Answer: D
Explanation:

QUESTION NO: 10

When discussing the FireAMP product, which term does the acronym DFC represent?

A. It means Detected Forensic Cause.
B. It means Duplicate File Contents.