210-255$^{\text{Q\&As}}$

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

QUESTION 1

Which of the following are the three broad categories of cybersecurity investigations?

A. Public, private, and individual investigations

B. Judiciary, private, and individual investigations

C. Public, private, and corporate investigations

D. Government, corporate, and private investigations

Correct Answer: A

QUESTION 2

According to NIST SP800-86, which action describes volatile data collection?

A. collection of data before a system reboot

B. collection of data that contains malware

C. collection of data during a system reboot

D. collection of data after a system reboot

Correct Answer: A

QUESTION 3

Which of the following Linux file systems not only supports journaling but also modifies important data structures of the file system, such as the ones destined to store the file data for better performance and reliability?

A. GRUB

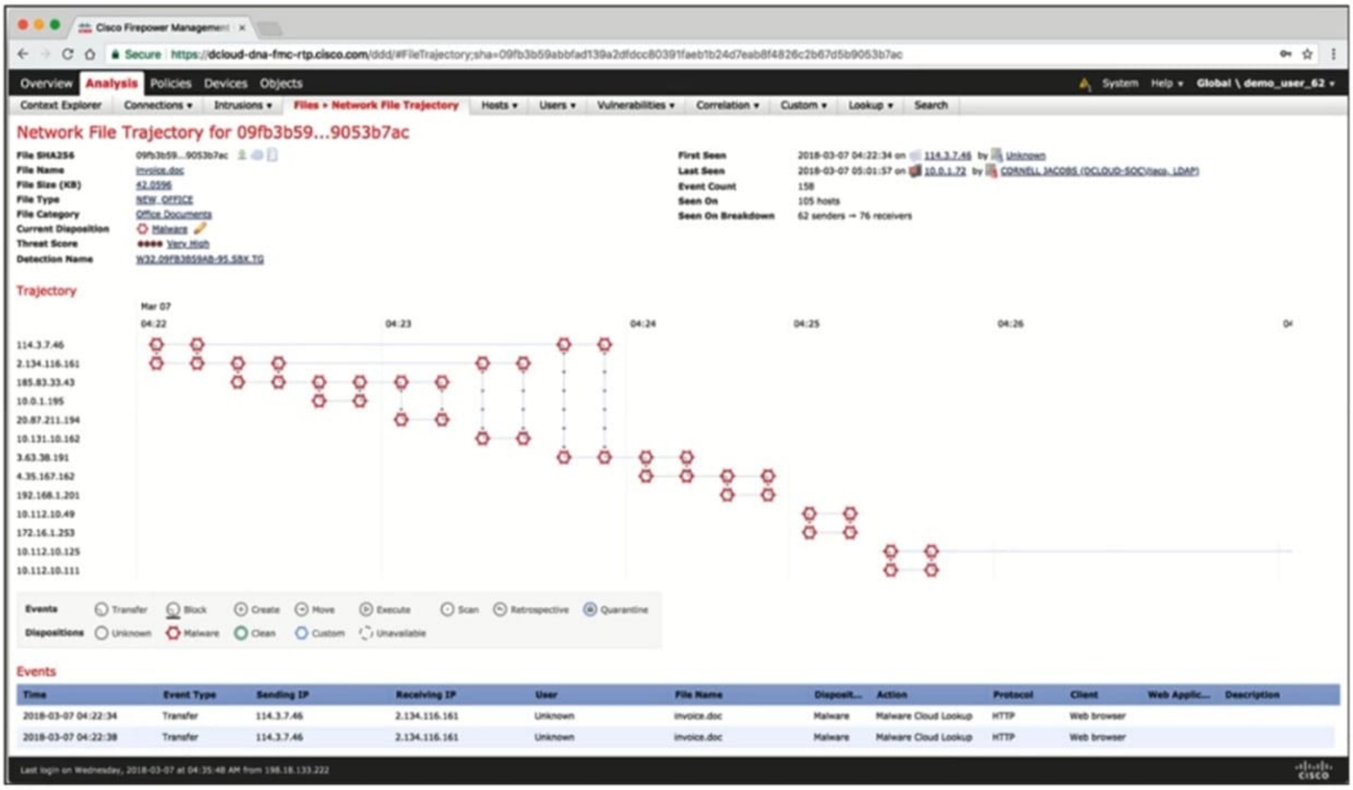
B. LILO

C. Ext4

D. FAT32

Correct Answer: C

QUESTION 4



Network File Trajectory for 09fb3b59...9053b7ac

File SHA256: 09fb3b59...9053b7ac
File Name: invoice.doc
File Size (KB): 42.0596
File Type: NEW_OFFICE
File Category: Office Documents
Current Disposition: Malware
Threat Score: ●●●● Very High
Detection Name: W32.09FB3B59AB-95.SBX.TG

First Seen: 2018-03-07 04:22:34 on 114.3.7.46 by Unknown
Last Seen: 2018-03-07 05:01:57 on 10.0.1.72 by CORNELL JACOBS (DCLOUD-SOC\jaco, LDAP)
Event Count: 158
Seen On: 105 hosts
Seen On Breakdown: 62 senders → 76 receivers

Trajectory

Events

Time	Event Type	Sending IP	Receiving IP	User	File Name	Disposit...	Action	Protocol	Client	Web Applic...	Description
2018-03-07 04:22:34	Transfer	114.3.7.46	2.134.116.161	Unknown	invoice.doc	Malware	Malware Cloud Lookup	HTTP	Web browser		
2018-03-07 04:22:38	Transfer	114.3.7.46	2.134.116.161	Unknown	invoice.doc	Malware	Malware Cloud Lookup	HTTP	Web browser		

Last login on Wednesday, 2018-03-07 at 04:35:48 AM from 198.18.133.222

Refer to the exhibit. Which description of the IP addresses under the Trajectory section is true?

A. victim systems running Microsoft Word

B. spoofed IP addresses

C. victim systems running Adobe Acrobat

D. attackers

Correct Answer: A

QUESTION 5

Which source provides reports of vulnerabilities in software and hardware to a Security Operations Center?

A. Analysis Center

B. National CSIRT

C. Internal CSIRT

D. Physical Security

Correct Answer: C

Latest 210-255 Dumps 210-255 Study Guide 210-255 Braindumps