Fortinet

NSE5_EDR-5.0 Exam

Fortinet NSE 5 - FortiEDR 5.0 Exam

Questions & Answers
Demo

Version: 4.0

Question: 1

What is the purpose of the Threat Hunting feature?

A. Delete any file from any collector in the organization
B. Find and delete all instances of a known malicious file or hash in the organization
C. Identify all instances of a known malicious file or hash and notify affected users
D. Execute playbooks to isolate affected collectors in the organization

Answer: C

Explanation:

Question: 2

How does FortiEDR implement post-infection protection?

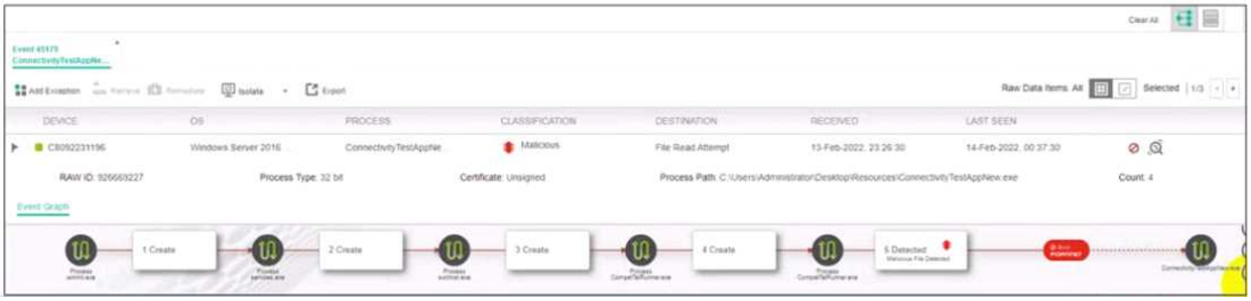
A. By preventing data exfiltration or encryption even after a breach occurs
B. By using methods used by traditional EDR
C. By insurance against ransomware
D. By real-time filtering to prevent malware from executing

Answer: D

Explanation:

Question: 3

Exhibit.



DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
C8092231196	Windows Server 2016	ConnectivityTestAppNe	Malicious	File Read Attempt	13-Feb-2022, 23:26:30	14-Feb-2022, 00:37:30

RAW ID: 926669227 Process Type: 32 bit Certificate: Unsigned Process Path: C:\Users\Administrator\Desktop\Resources\ConnectivityTestAppNew.exe Count: 4

Based on the forensics data shown in the exhibit which two statements are true? (Choose two.)

A. The device cannot be remediated
B. The event was blocked because the certificate is unsigned

C. Device C8092231196 has been isolated
D. The execution prevention policy has blocked this event.

Answer: B, C

Explanation:

Question: 4

What is the benefit of using file hash along with the file name in a threat hunting repository search?

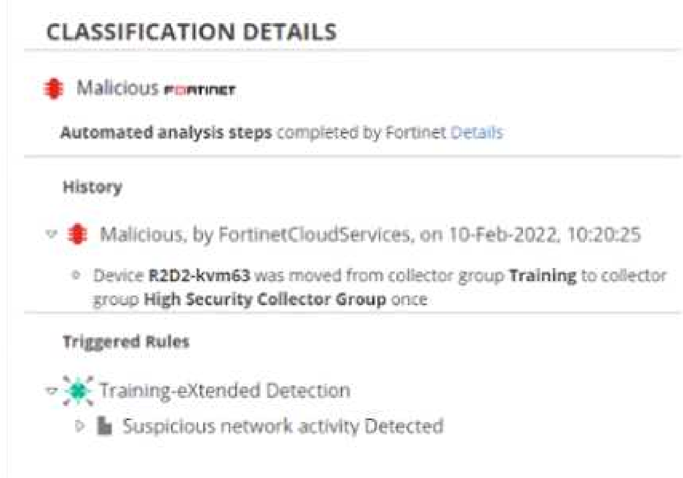
A. It helps to make sure the hash is really a malware
B. It helps to check the malware even if the malware variant uses a different file name
C. It helps to find if some instances of the hash are actually associated with a different file
D. It helps locate a file as threat hunting only allows hash search

Answer: C

Explanation:

Question: 5

Exhibit.



CLASSIFICATION DETAILS

Malicious FORTINET

Automated analysis steps completed by Fortinet Details

History

Malicious, by FortinetCloudServices, on 10-Feb-2022, 10:20:25

Device **R2D2-kvm63** was moved from collector group **Training** to collector group **High Security Collector Group** once

Triggered Rules

Training-eXtended Detection

Suspicious network activity Detected

Based on the event shown in the exhibit which two statements about the event are true? (Choose two.)

A. The device is moved to isolation.
B. Playbooks is configured for this event.
C. The event has been blocked
D. The policy is in simulation mode

Answer: B, D