

# Fortinet

## NSE5\_EDR-5.0

### Fortinet NSE 5 - FortiEDR 5.0 Exam

For More Information – Visit link below:

<https://www.examsempire.com/>

**Product Version**

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/nse5-edr-5-0>

# Latest Version: 6.0

## 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**

## Question: 2

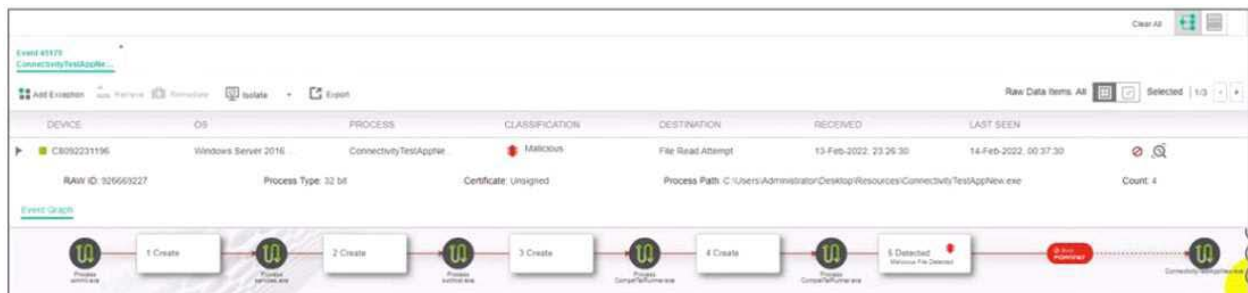
How does FortiEDR implement post-infection protection?

- 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**

## Question: 3

Exhibit.



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**

### 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**

### Question: 5

Exhibit.



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**

**Thank You for Trying Our Product**

**Special 16 USD Discount Coupon: NSZUBG3X**

**Email:** [support@examsempire.com](mailto:support@examsempire.com)

**Check our Customer Testimonials and ratings  
available on every product page.**

**Visit our website.**

**<https://examsempire.com/>**