



## Fortinet

### NSE5\_EDR-5.0 Exam

Fortinet NSE 5 - FortiEDR 5.0 Exam

**Thank you for Downloading NSE5\_EDR-5.0 exam PDF Demo**

You can also try our NSE5\_EDR-5.0 practice exam software

**Download Free Demo**

[https://prepbolt.com/NSE5\\_EDR-5.0.html](https://prepbolt.com/NSE5_EDR-5.0.html)

QUESTIONS & ANSWERS  
**DEMO VERSION**  
*(LIMITED CONTENT)*

# 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?

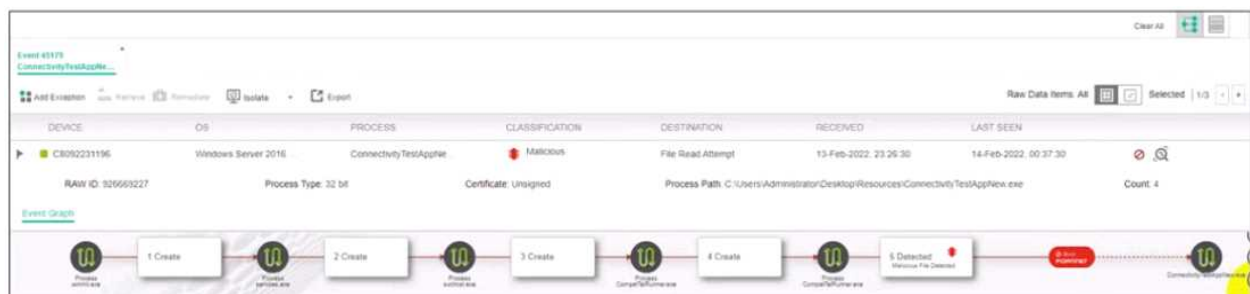
- A. By preventing data exfiltration or encryption even after a breach occurs
- B. By using methods used by traditional EDR
- C. By insurance against ransomware
- D. By real-time filtering to prevent malware from executing

**Answer: D**

Explanation:

## Question: 3

Exhibit.



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.

The screenshot displays the 'CLASSIFICATION DETAILS' for a security event. It includes a red 'Malicious' icon and the text 'Malicious by Fortinet'. Below this, it states 'Automated analysis steps completed by Fortinet Details'. The 'History' section shows a dropdown arrow next to a red 'Malicious' icon, followed by the text 'Malicious, by FortinetCloudServices, on 10-Feb-2022, 10:20:25'. A sub-entry indicates 'Device R2D2-kvm63 was moved from collector group Training to collector group High Security Collector Group once'. The 'Triggered Rules' section shows a dropdown arrow next to a green 'Training-eXtended Detection' icon, followed by the text '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**

---

**Thank You for trying NSE5\_EDR-5.0 PDF Demo**

To try our NSE5\_EDR-5.0 practice exam software visit link  
below

[https://prepbolt.com/NSE5\\_EDR-5.0.html](https://prepbolt.com/NSE5_EDR-5.0.html)

**Start Your NSE5\_EDR-5.0  
Preparation**

Use Coupon "SAVE50" for extra 50% discount on the purchase of  
Practice Test Software. Test your NSE5\_EDR-5.0 preparation with  
actual exam questions.

