

Fortinet

NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0 Exam

Questions And Answers PDF Format:

For More Information – Visit link below:

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

Version = Product



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

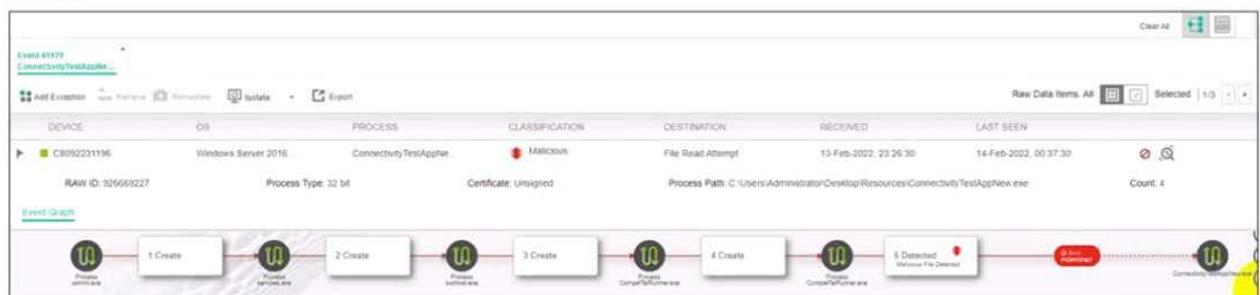
How does FortiEDR implement post-infection protection?

- 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.

The screenshot displays the 'CLASSIFICATION DETAILS' for a security event. At the top, it is labeled 'Malicious Fortinet'. Below this, it states 'Automated analysis steps completed by Fortinet Details'. The 'History' section shows a single event: 'Malicious, by FortinetCloudServices, on 10-Feb-2022, 10:20:25'. A sub-entry indicates that 'Device R2D2-kvm63 was moved from collector group Training to collector group High Security Collector Group once'. The 'Triggered Rules' section shows 'Training-eXtended Detection' with a sub-entry '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

For More Information – **Visit link below:**
<http://www.certsgrade.com/>

PRODUCT FEATURES

-  **100% Money Back Guarantee**
-  **90 Days Free updates**
-  **Special Discounts on Bulk Orders**
-  **Guaranteed Success**
-  **50,000 Satisfied Customers**
-  **100% Secure Shopping**
-  **Privacy Policy**
-  **Refund Policy**

Discount Coupon Code: **CERTSGRADE10**

