



NSE5_EDR-5.0^{Q&As}

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/nse5_edr-5-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Which two statements are true about the remediation function in the threat hunting module? (Choose two.)

- A. The file is removed from the affected collectors
- B. The threat hunting module sends the user a notification to delete the file
- C. The file is quarantined
- D. The threat hunting module deletes files from collectors that are currently online.

Correct Answer: AD

QUESTION 2

Exhibit.

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
NAVIC 30688227	Windows Server 2012	C:\Users\Administrator\Desktop\ConnectivityTestApp.exe	Malicious	Process Path: C:\Users\Administrator\Desktop\Resources\ConnectivityTestApp.exe	11/26/2022 11:35:33	11/26/2022 10:17:30

Event Queue

Timeline: 1 Create, 2 Create, 3 Create, 4 Create, 5 Deleted (Hosted File Location), 6 Deleted



Event 45179
ConnectivityTestAppNe...

Add Exception Retrievs Remediate Isolate Export

DEVICE	OS	PROCESS	CLASSIFICATION
C8092231196	Windows Server 2016	ConnectivityTestAppNe...	Malicious

RAW ID: 926669227 Process Type: 32 bit Certificate: Unsigned

Event Graph

```

graph LR
    P1((Process Initial state)) --> E1[1 Create]
    E1 --> P2((Process Initial state))
    P2 --> E2[2 Create]
    E2 --> P3((Process Initial state))
    P3 --> E3[3 Create]
  
```

Clear All

Raw Data Items: All Selected 1/3

DESTINATION	RECEIVED	LAST SEEN
File Read Attempt	13-Feb-2022, 23:26:30	14-Feb-2022, 00:37:30

Process Path: C:\Users\Administrator\Desktop\Resources\ConnectivityTestAppNew.exe Count: 4

```

graph LR
    P1((Process Computer.exe)) --> E1[4 Create]
    E1 --> P2((Process Computer.exe))
    P2 --> E2[5 Detected Malicious File Detected]
    E2 --> E3[Block Execution]
    E3 -.-> P3((ConnectivityTestAppNew.exe))
  
```

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.

Correct Answer: AD

QUESTION 3



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

Correct Answer: B

QUESTION 4

An administrator finds that a newly installed collector does not display on the INVENTORY tab in the central manager.

What two troubleshooting steps must the administrator perform? (Choose two.)

- A. Export the collector logs from the central manager.
- B. Verify the central manager has connectivity to FCS.
- C. Verify TCP ports 8081 and 555 are open.
- D. Check if the FortiEDR services are running on the collector device.

Correct Answer: CD

QUESTION 5

What is true about classifications assigned by Fortinet Cloud Sentinel (FCS)?

- A. The core is responsible for all classifications if FCS playbooks are disabled
- B. The core only assigns a classification if FCS is not available
- C. FCS revises the classification of the core based on its database
- D. FCS is responsible for all classifications

Correct Answer: C

[Latest NSE5_EDR-5.0 Dumps](#)

[NSE5_EDR-5.0 PDF Dumps](#)

[NSE5_EDR-5.0 Brindumps](#)