

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.leads4pass.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

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 2

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 3

An administrator needs to restrict access to the ADMINISTRATION tab in the central manager for a specific account.

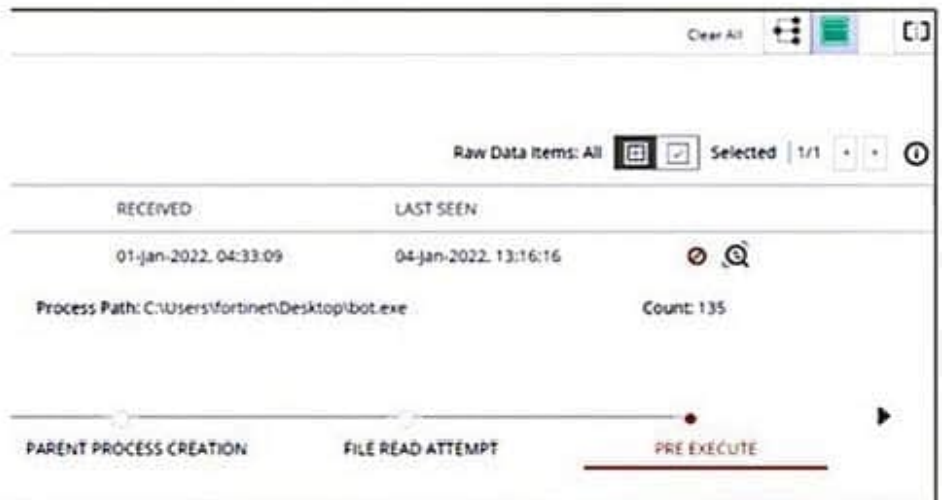
What role should the administrator assign to this account?

- A. Admin
- B. User
- C. Local Admin
- D. REST API

Correct Answer: B

QUESTION 4

Exhibit.



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

- A. An exception has been created for this event
- B. The forensics data is displayed in the stacks view
- C. The device has been isolated
- D. The exfiltration prevention policy has blocked this event

Correct Answer: BC

QUESTION 5

Refer to the exhibit.

The exhibit shows an event viewer.

| All | ID | DEVICE | PROCESS |
|---|------|-------------|---------------------|
| Payroll Manager.exe (3 events) | | | |
| <input type="checkbox"/> | 9715 | cwinserv-32 | Payroll Manager.exe |
| User: CWINSERV-32\Administrator Certificate: Unsigned Process path: | | | |
| <input type="checkbox"/> | 9695 | cwinserv-32 | Payroll Manager.exe |
| <input type="checkbox"/> | 8878 | cwinserv-32 | Payroll Manager.exe |
| CryptoLocker2.exe (1 event) | | | |

| CLASSIFICATION | DESTINATIONS | RECEIVED | LAST UPDATED |
|---|---------------|-----------------------|-----------------------|
| Suspicious | | 25-Nov-2020, 06:09:07 | |
| Suspicious | 74.125.235.20 | 25-Nov-2020, 06:09:07 | 25-Nov-2020, 06:09:07 |
| ..inistrator\Downloads\Resources\TestFiles\Fake Malware\Payroll Manager.exe | | Raw data items: 1 | |
| Suspicious | 74.125.235.20 | 25-Nov-2020, 06:07:43 | 25-Nov-2020, 06:07:43 |
| Suspicious | 74.125.235.20 | 21-Sep-2020, 06:45:53 | 21-Sep-2020, 11:21:11 |
| Malicious | | 28-Sep-2020, 05:46:35 | |

What is true about the Payroll Manager.exe event?

- A. An event has not been handled by a console admin
- B. An event has been deleted
- C. A rule assigned action is set to block but the policy is in simulation mode
- D. An event has been handled by the communication control policy

Correct Answer: C

[Latest NSE5_EDR-5.0 Dumps](#)

[NSE5_EDR-5.0 PDF Dumps](#)

[NSE5_EDR-5.0 VCE Dumps](#)