



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.passapply.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

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

QUESTION 2

Which threat hunting profile is the most resource intensive?



- A. Comprehensive
- B. Inventory
- C. Default
- D. Standard Collection

Correct Answer: A

QUESTION 3

FortiXDR relies on which feature as part of its automated extended response?

- A. Playbooks
- B. Security Policies
- C. Forensic
- D. Communication Control


Correct Answer: A

QUESTION 4

Exhibit.



CLASSIFICATION DETAILS

 Malicious **FORTINET**

Automated analysis steps completed by Fortinet [Details](#)

History

- Malicious, by FortinetCloudServices, on 10-Feb-2022, 10:20:25
 - Device **R2D2-kvm63** was moved from collector group **Training** to collector group **High Security Collector Group** once

Triggered Rules

-  Training-eXtended Detection
 -  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

Correct Answer: BD

QUESTION 5

The FortiEDR axe classified an event as inconclusive, out a few seconds later FCS revised the classification to malicious.

What playbook actions ate applied to the event?

- A. Playbook actions applied to inconclusive events
- B. Playbook actions applied to handled events
- C. Playbook actions applied to suspicious events
- D. Playbook actions applied to malicious events

Correct Answer: D



[NSE5_EDR-5.0 PDF
Dumps](#)

[NSE5_EDR-5.0 VCE
Dumps](#)

[NSE5_EDR-5.0 Braindumps](#)