



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.pass4itsure.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

An administrator finds a third party free software on a user's computer that does not appear in the application list in the communication control console

Which two statements are true about this situation? (Choose two)

- A. The application is allowed in all communication control policies
- B. The application is ignored as the reputation score is acceptable by the security policy
- C. The application has not made any connection attempts
- D. The application is blocked by the security policies

Correct Answer: CD

QUESTION 2

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

What playbook actions were 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

QUESTION 3

Refer to the exhibit.



EVENT EXCEPTIONS

Exceptions for event **44875**

Exception 1 +

Created from Raw Item **641717447** of event **44857**
Last updated at 10-Dec-2021, 22:52 By FortinetCloudServices

Collector groups

All groups

Destinations

All destinations

Users

All users

Triggered Rules:

▸ File Encryptor ⓘ

.....
FortinetCloudServices at 10-Dec-2021, 22:52:59
The file Update.exe is classified as Good. On the device "C8092231196"

Remote Exception

◆ All the Raw Data items are covered

Save Changes Cancel

Based on the event exception shown in the exhibit which two statements about the exception are true? (Choose two)

- A. A partial exception is applied to this event
- B. FCS playbooks is enabled by Fortinet support
- C. The exception is applied only on device C8092231196
- D. The system owner can modify the trigger rules parameters

Correct Answer: AC



QUESTION 4

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 5

Which security policy has all of its rules disabled by default?

- A. Device Control
- B. Ransomware Prevention
- C. Execution Prevention
- D. Exfiltration Prevention

Correct Answer: A

[NSE5_EDR-5.0 VCE Dumps](#)

[NSE5_EDR-5.0 Practice Test](#)

[NSE5_EDR-5.0 Exam Questions](#)