



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 three steps does FortiXDR perform to find and prevent cyberattacks? (Choose three.)

- A. Extended analysis
- B. Extended detection
- C. Extended discovery
- D. Extended investigation
- E. Extended response

Correct Answer: BDE

QUESTION 2

Which two criteria are requirements of integrating FortiEDR into the Fortinet Security Fabric? (Choose two.)

- A. Core with Core only functionality
- B. A Forensics add-on license
- C. Central Manager connected to FCS
- D. A valid API user with access to connectors

Correct Answer: CD

QUESTION 3

Which two events can trigger FortiEDR NGAV policy violations? (Choose two.)

- A. When a malicious file attempts to communicate externally
- B. When a malicious file is executed
- C. When a malicious file is read
- D. When a malicious file attempts to access data

Correct Answer: BC

NGAV reacts when a file is Saved, Read, or Executed Page 79 of the guide

QUESTION 4

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

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 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

[Latest NSE5_EDR-5.0
Dumps](#)

[NSE5_EDR-5.0 VCE
Dumps](#)

[NSE5_EDR-5.0 Practice
Test](#)