# NSE5_EDR-5.0<sup>Q&As</sup>

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

**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**

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 3**

Which two statements about the FortiEDR solution are true? (Choose two.)

A. It provides pre-infection and post-infection protection

B. It is Windows OS only

C. It provides central management

D. It provides pant-to-point protection

Correct Answer: AC


**QUESTION 4**

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 5

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 6

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 7

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 8**

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

**QUESTION 9**

A company requires a global exception for a FortiEDR multi-tenant environment.

How can the administrator achieve this?

A. The local administrator can create a new exception and share it with other organizations.

B. A user account can create a new exception and share it with other organizations.

C. The administrator can create a new exception and assign it globally to all organizations.

D. The administrator can create a new exception policy for each organization hosted on FortiEDR.

Correct Answer: C

Fortiedr AdminGuide "For a multi-organization FortiEDR system, an Administrator who is assigned to All organizations (see Users) can also specify whether the exception applies to all organizations. The All organizations option applies the exception to all organizations, regardless of whether or not the security event already occurred."

**QUESTION 10**

What is true about classifications assigned by Fortinet Cloud Sen/ice (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 VCE Dumps

NSE5_EDR-5.0 Study Guide