

# 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.pass2lead.com/nse5\\_edr-5-0.html](https://www.pass2lead.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 connectors can you use for the FortiEDR automated incident response? (Choose two.)

- A. FortiNAC
- B. FortiGate
- C. FortiSiem
- D. FortiSandbox

Correct Answer: AB

---

**QUESTION 2**

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 3**

Which scripting language is supported by the FortiEDR action managed?

- A. TCL
- B. Python
- C. Perl
- D. Bash

Correct Answer: B

---

**QUESTION 4**

Exhibit.

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
C8092231196	Windows Server 2016	ConnectivityTestAppNe...	Malicious	File Read Attempt	13-Feb-2022 23:26:30	14-Feb-2022 00:37:30

RAW ID: 526669227      Process Type: 32 bit      Certificate: Unsigned      Process Path: C:\Users\Administrator\Desktop\Resources\ConnectivityTestAppNew.exe      Count: 4

DEVICE	OS	PROCESS	CLASSIFICATION
C8092231196	Windows Server 2016	ConnectivityTestAppNe...	Malicious

RAW ID: 526669227      Process Type: 32 bit      Certificate: Unsigned

DESTINATION	RECEIVED	LAST SEEN
File Read Attempt	13-Feb-2022 23:26:30	14-Feb-2022 00:37:30

Process Path: C:\Users\Administrator\Desktop\Resources\ConnectivityTestAppNew.exe      Count: 4

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

A. The device cannot be remediated

- B. The event was blocked because the certificate is unsigned
- C. Device C8092231196 has been isolated
- D. The execution prevention policy has blocked this event.

Correct Answer: AD

---

#### QUESTION 5

Which FortiEDR component is required to find malicious files on the entire network of an organization?

- A. FortiEDR Aggregator
- B. FortiEDR Central Manager
- C. FortiEDR Threat Hunting Repository
- D. FortiEDR Core

Correct Answer: C

[NSE5\\_EDR-5.0 PDF Dumps](#)

[NSE5\\_EDR-5.0 Study Guide](#)

[NSE5\\_EDR-5.0 Braindumps](#)