



# 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](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

Which scripting language is supported by the FortiEDR action managed?

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

Correct Answer: B

---

### QUESTION 2

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 3

Exhibit.



Event 5273776  
bot.exe

Add Exception Remove Remediate Isolate Export

Raw Data Items: All Selected 1/1

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
c:\p0-kvm48	Windows 10 Pro	bot.exe	Malicious	File Read Attempt	01-Jan-2022, 04:33:09	04-Jan-2022, 13:16:16

RAW ID: 119330467 Process Type: 32 bit Certificate: Unsigned Process Path: C:\Users\fortinet\Desktop\bot.exe Count: 135

← ESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION FILE READ ATTEMPT PRE EXECUTE →

Event 5273776  
bot.exe

Add Exception Remove Remediate Isolate Export

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION
c:\p0-kvm48	Windows 10 Pro	bot.exe	Malicious	File Read Attempt

RAW ID: 119330467 Process Type: 32 bit Certificate: Unsigned

← ESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION →

Clear All

Raw Data Items: All Selected 1/1

RECEIVED	LAST SEEN
01-Jan-2022, 04:33:09	04-Jan-2022, 13:16:16

Process Path: C:\Users\fortinet\Desktop\bot.exe Count: 135

PARENT PROCESS CREATION FILE READ ATTEMPT PRE EXECUTE

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

- A. An exception has been created for this event
- B. The forensics data is displayed in the stacks view
- C. The device has been isolated
- D. The exfiltration prevention policy has blocked this event

Correct Answer: BC



#### 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

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

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

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

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