

# 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.certbus.com/nse5\\_edr-5-0.html](https://www.certbus.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 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 2**

Refer to the exhibit.

The exhibit shows an event viewer.

All	ID	DEVICE	PROCESS
Payroll Manager.exe (3 events)			
<input type="checkbox"/>	9715	cwinserv-32	Payroll Manager.exe
User: CWINSERV-32\Administrator Certificate: Unsigned Process path:			
<input type="checkbox"/>	9695	cwinserv-32	Payroll Manager.exe
<input type="checkbox"/>	8878	cwinserv-32	Payroll Manager.exe
CryptoLocker2.exe (1 event)			

CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
Suspicious		25-Nov-2020, 06:09:07	
Suspicious	74.125.235.20	25-Nov-2020, 06:09:07	25-Nov-2020, 06:09:07
..inistrator\Downloads\Resources\TestFiles\Fake Malware\Payroll Manager.exe		Raw data items: 1	
Suspicious	74.125.235.20	25-Nov-2020, 06:07:43	25-Nov-2020, 06:07:43
Suspicious	74.125.235.20	21-Sep-2020, 06:45:53	21-Sep-2020, 11:21:11
Malicious		28-Sep-2020, 05:46:35	

What is true about the Payroll Manager.exe event?

- A. An event has not been handled by a console admin
- B. An event has been deleted
- C. A rule assigned action is set to block but the policy is in simulation mode
- D. An event has been handled by the communication control policy

Correct Answer: C

---

### QUESTION 3

Refer to the exhibit.

TestApplication.exe.exe (3 events) 15-Feb-2022, 13:31:39

5894314 R2D2-kvm63 TestApplication.exe.exe Malicious 8.8.8.8 15-Feb-2022, 13:31:39 15-Feb-2022, 13:31:39

Logged-in User:	Process owner:	Certificate:	Process path:
R2D2-KVM63\fortinet	R2D2-KVM63\fortinet	Unsigned	C:\Users\fortinet\Desktop

### CLASSIFICATION DETAILS

**Malicious**

Threat name: Unknown  
 Threat family: Unknown  
 Threat type: Unknown

#### History

Malicious, by Fortinet, on 15-Feb-2022, 13:31:41

#### Triggered Rules

- Exfiltration Prevention
  - Invalid Checksum - Connection Attempt from Application wi...
  - Malicious File Detected
  - Suspicious Packer - Activity by an Application packed by a S...
  - Writeable Code - Identified an Executable with Writable Code

TestApplication.exe.exe (3 events) Malicious

5894314 R2D2-kvm63 TestApplication.exe.exe Malicious

Logged-in User:	Process owner:	Certificate:	Process path:
R2D2-KVM63\fortinet	R2D2-KVM63\fortinet	Unsigned	C:\Users\fortinet\Desktop

15-Feb-2022, 13:31:39

8.8.8.8 15-Feb-2022, 13:31:39 15-Feb-2022, 13:31:39

### CLASSIFICATION DETAILS

**Malicious**

Threat name: Unknown  
 Threat family: Unknown  
 Threat type: Unknown

#### History

Malicious, by Fortinet, on 15-Feb-2022, 13:31:41

#### Triggered Rules

- Exfiltration Prevention
  - Invalid Checksum - Connection Attempt from Application wi...
  - Malicious File Detected
  - Suspicious Packer - Activity by an Application packed by a S...
  - Writeable Code - Identified an Executable with Writable Code

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

- A. The NGAV policy has blocked TestApplication.exe
- B. TestApplication.exe is sophisticated malware
- C. The user was able to launch TestApplication.exe
- D. FCS classified the event as malicious

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

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 5**

Which threat hunting profile is the most resource intensive?

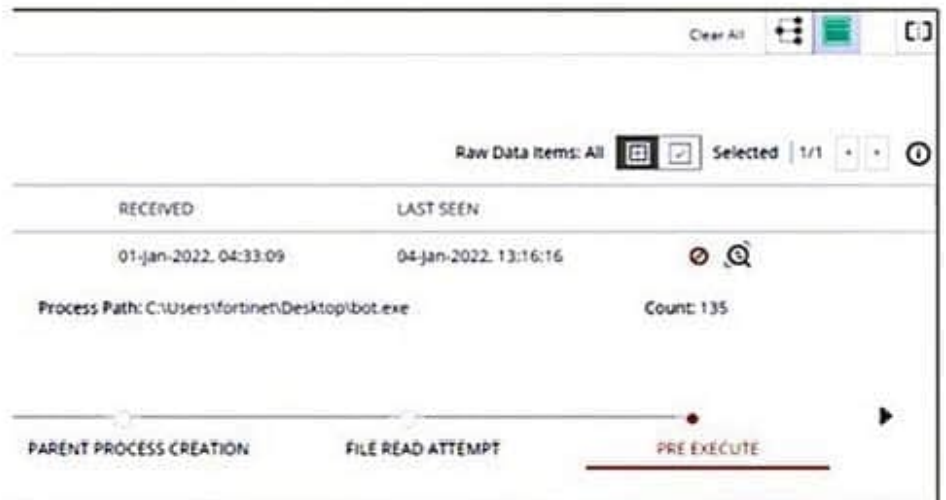
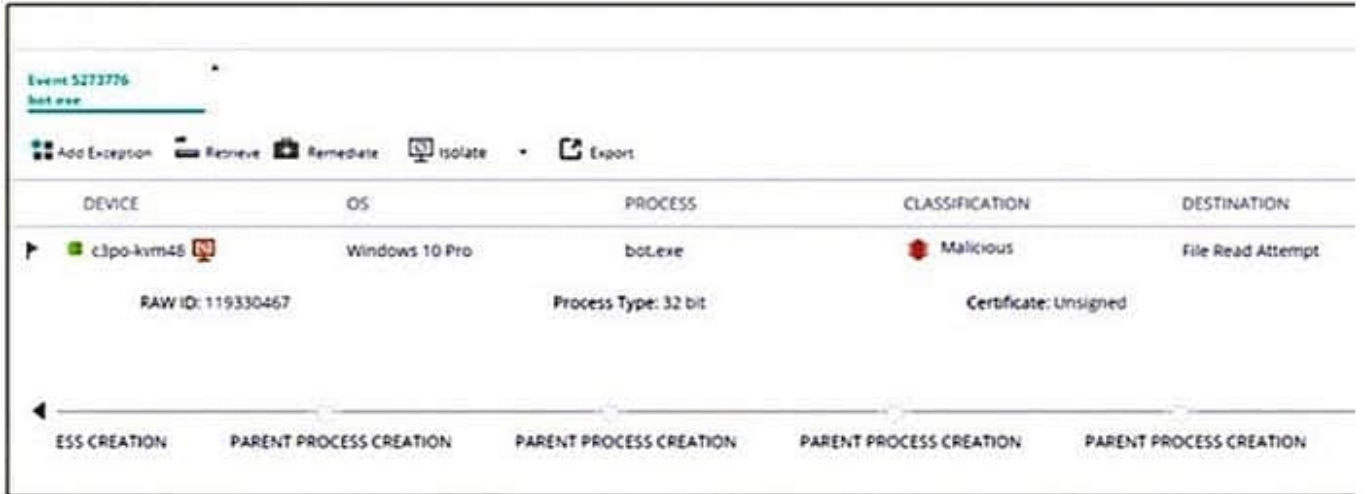
- A. Comprehensive
- B. Inventory
- C. Default
- D. Standard Collection

Correct Answer: A

---

**QUESTION 6**

Exhibit.



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 7**

Refer to the exhibits.

Enable/Disable ▾ Isolate ▾ Export ▾ Uninstall

DEVICE NAME	LAST LOGGED	OS	IP
C8092231196	... 1196\Administrator	Windows Server 2016 Standard Evaluation	10.160.6.110

Search Collectors or Gro ▾ Q

MAC ADDRESS	VERSION	STATE	LAST SEEN
00-50-56-A1-32-81, 00...	4.1.0.361	Disconnected	Today

```
Administrator: Command Prompt
C:\Users\Administrator>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
TCP   0.0.0.0:5985             0.0.0.0:0               LISTENING
TCP   0.0.0.0:49692            0.0.0.0:0               LISTENING
TCP   10.160.6.110:139         0.0.0.0:0               LISTENING
TCP   10.160.6.110:50853      10.160.6.100:8080      SYN_SENT
TCP   172.16.9.19:139         0.0.0.0:0               LISTENING
TCP   172.16.9.19:49687      52.177.165.30:443      ESTABLISHED
```

The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address 10.160.6.100 using default port. Based on the netstat command output what must you do to resolve the connectivity issue?

- A. Reinstall collector agent and use port 443
- B. Reinstall collector agent and use port 8081
- C. Reinstall collector agent and use port 555
- D. Reinstall collector agent and use port 6514

Correct Answer: B

**QUESTION 8**

Refer to the exhibits.

The screenshot shows a web interface titled 'APPLICATIONS'. At the top, there are navigation options: 'All', 'Mark As', 'Delete', 'Modify Action', 'Advanced Filter', and 'Export'. Below this is a table with columns: APPLICATION, SIGNED, VENDOR, REPUTATION, and VULNERABILITY. The table lists two FileZilla entries. The first entry is for FileZilla 3.50.0, signed by Tim Kosse, with an unknown reputation and vulnerability. The second entry is for FileZilla, signed by FileZilla Project, also with an unknown reputation and vulnerability. Below the table, there are sections for 'COLLECTOR GROUP NAME' and 'DEVICE NAME'. Under 'COLLECTOR GROUP NAME', there are three groups: 'High Security Collector Group (1/1)', 'DBA (1/1)', and 'Default Collector Group (0/0)'. Under 'DEVICE NAME', the value 'C8092231196' is listed.

APPLICATION	SIGNED	VENDOR	REPUTATION	VULNERABILITY
FileZilla	Signed	Tim Kosse	Unknown	Unknown
3.50.0			Unknown	Unknown
FileZilla	Signed	FileZilla Project	Unknown	Unknown

COLLECTOR GROUP NAME	DEVICE NAME
High Security Collector Group (1/1)	
DBA (1/1)	
Default Collector Group (0/0)	C8092231196

### APPLICATION DETAILS

FileZilla

**Policies**

Policy	Action
Default Communication Control ... <b>FORTINET</b>	<b>Allow</b> According to policy
Servers Policy <b>FORTINET</b>	<b>Deny</b> According to policy
Finance Policy	<b>Deny</b> <i>Manually</i>
Simulation Communication Control Policy	<b>Allow</b> According to policy
Isolation Policy <b>FORTINET</b>	<b>Deny</b> According to policy

### ASSIGNED COLLECTOR GROUPS

**Finance Policy**

- Unassign Group

The exhibits show application policy logs and application details Collector C8092231196 is a member of the Finance group What must an administrator do to block the FileZilla application?

- A. Deny application in Finance policy
- B. Assign Finance policy to DBA group
- C. Assign Finance policy to Default Collector Group
- D. Assign Simulation Communication Control Policy to DBA group

Correct Answer: B

### QUESTION 9

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 10

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

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

[NSE5\\_EDR-5.0 Practice Test](#)

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