



# 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

Refer to the exhibits.

APPLICATIONS

All

Mark As

Delete

Modify Action

Advanced Filter

Export

APPLICATION		VENDOR	REPUTATION	VULNERABILITY
<div><div></div><div></div></div>	<div><div></div><div>FileZilla</div><div>Signed</div></div>	Tim Kosse	Unknown	Unknown
	<div><div></div><div>3.50.0</div></div>		Unknown	Unknown
<div><div></div><div></div></div>	<div><div></div><div>FileZilla</div><div>Signed</div></div>	FileZilla Project	Unknown	Unknown
COLLECTOR GROUP NAME		DEVICE NAME		
<div><div></div><div></div></div>	<div><div></div><div>High Security Collector Group (1/1)</div></div>			
<div><div></div><div></div></div>	<div><div></div><div>DBA (1/1)</div></div>			
		C8092231196		
<div><div></div><div></div></div>	<div><div></div><div>Default Collector Group (0/0)</div></div>			



## 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 2

Refer to the exhibit.

The exhibit shows an event viewer.



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

When installing a FortiEDR collector, why is a 'Registration Password' for collectors needed?

- A. To restrict installation and uninstallation of collectors
- B. To verify Fortinet support request
- C. To restrict access to the management console
- D. To verify new group assignment



Correct Answer: A

---

#### QUESTION 4

What is the purpose of the Threat Hunting feature?

- A. Delete any file from any collector in the organization
- B. Find and delete all instances of a known malicious file or hash in the organization
- C. Identify all instances of a known malicious file or hash and notify affected users
- D. Execute playbooks to isolate affected collectors in the organization

Correct Answer: B

"Threat hunting allows management console users to find and remediate dormant threats before they execute. Essentially it's a search and destroy operation."

---

#### QUESTION 5

Which FortiEDR component must have JumpBox functionality to connect with FortiAnalyzer?

- A. Collector
- B. Core
- C. Central manager
- D. Aggregator

Correct Answer: B

You need an on premise CORE , with jump box functionality and valid API access, to Gate, Analyzer, NAC and or Sandbox.

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

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

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