NSE5_EDR-5.0^{Q&As}

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

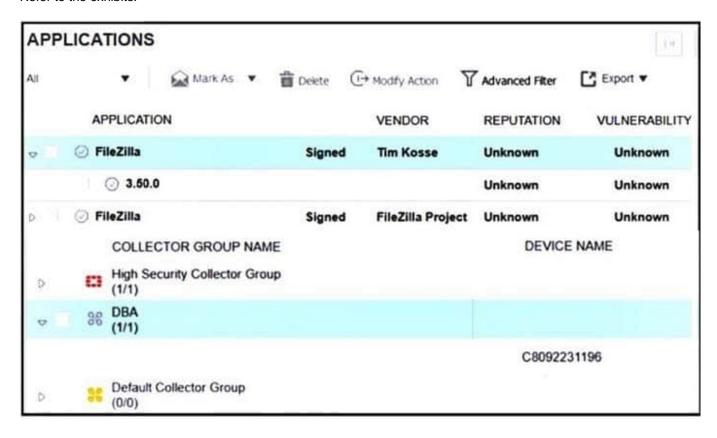Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibits.

APPLICATION			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)	
		C8092231196
▷	Default Collector Group (0/0)	

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

Which three steps does FortiXDR perform to find and prevent cyberattacks? (Choose three.)

A. Extended analysis

B. Extended detection

C. Extended discovery

D. Extended investigation

E. Extended response

Correct Answer: BDE

QUESTION 3

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 4

Which two events can trigger FortiEDR NGAV policy violations? (Choose two.)

A. When a malicious file attempts to communicate externally

B. When a malicious file is executed

C. When a malicious file is read

D. When a malicious file attempts to access data

Correct Answer: BC

NGAV reacts when a file is Saved, Read, or Executed Page 79 of the guide

---

QUESTION 5

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