



# 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

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 2

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 ▾

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&gt;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 3

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 4

Exhibit.



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

Timeline: ESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, FILE READ ATTEMPT, PRE EXECUTE

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

Timeline: ESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION, PARENT PROCESS CREATION

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

Timeline: 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 5**

An administrator finds a third party free software on a user's computer that does not appear in the application list in the communication control console

Which two statements are true about this situation? (Choose two)

- A. The application is allowed in all communication control policies
- B. The application is ignored as the reputation score is acceptable by the security policy
- C. The application has not made any connection attempts
- D. The application is blocked by the security policies

Correct Answer: CD

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

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

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