



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.pass4itsure.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**


Exhibit.

CLASSIFICATION DETAILS

 Malicious **FORTINET**

Automated analysis steps completed by Fortinet [Details](#)

History

- ▼  Malicious, by FortinetCloudServices, on 10-Feb-2022, 10:20:25
 - Device **R2D2-kvm63** was moved from collector group **Training** to collector group **High Security Collector Group** once
-

Triggered Rules

- ▼  Training-eXtended Detection
 - ▷  Suspicious network activity Detected

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

- A. The device is moved to isolation.
- B. Playbooks is configured for this event.
- C. The event has been blocked
- D. The policy is in simulation mode

Correct Answer: BD

QUESTION 2

Which statement is true about the flow analyzer view in forensics?

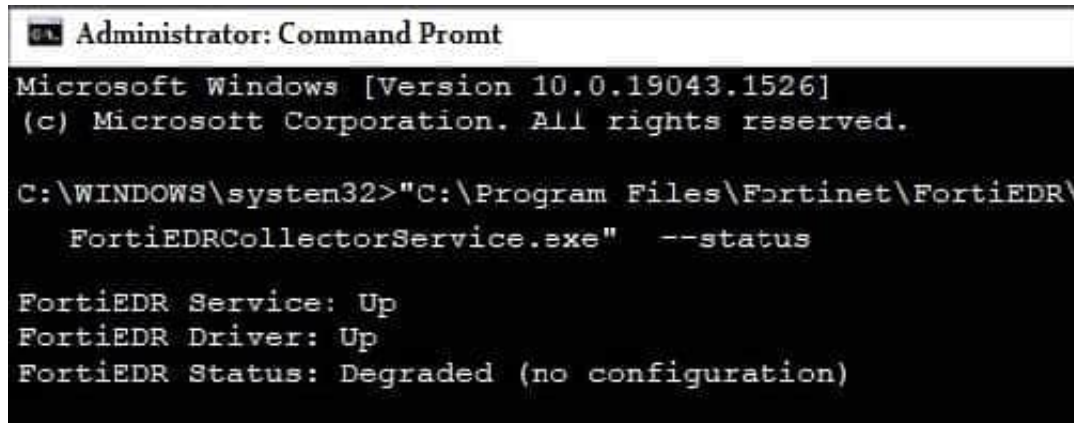
- A. It displays a graphic flow diagram.
- B. Two events can be compared side-by-side.
- C. It shows details about processes and sub processes.
- D. The stack memory of a specific device can be retrieved



Correct Answer: A

QUESTION 3

Refer to the exhibit.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.1526]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>"C:\Program Files\Fortinet\FortiEDR\FortiEDRCollectorService.exe" --status

FortiEDR Service: Up
FortiEDR Driver: Up
FortiEDR Status: Degraded (no configuration)
```

Based on the FortiEDR status output shown in the exhibit, which two statements about the FortiEDR collector are true? (Choose two.)

- A. The collector device has windows firewall enabled
- B. The collector has been installed with an incorrect port number
- C. The collector has been installed with an incorrect registration password
- D. The collector device cannot reach the central manager

Correct Answer: BC

QUESTION 4

Which threat hunting profile is the most resource intensive?

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

Correct Answer: A

QUESTION 5

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

[NSE5_EDR-5.0 Study Guide](#)

[NSE5_EDR-5.0 Exam Questions](#)

[NSE5_EDR-5.0 Braindumps](#)