

## Exam Questions NSE5\_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

[https://www.2passeasy.com/dumps/NSE5\\_EDR-5.0/](https://www.2passeasy.com/dumps/NSE5_EDR-5.0/)



**NEW QUESTION 1**

Refer to the exhibits.

DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
C8092231196	...1196\Administrator	Windows Server 2016 Standard Evaluation	10.160.6.110	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

**Answer: B**

**NEW QUESTION 2**

Exhibit.

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

- A. The device cannot be remediated
- B. The event was blocked because the certificate is unsigned
- C. Device C8092231196 has been isolated
- D. The execution prevention policy has blocked this event.

**Answer: BC**

**NEW QUESTION 3**

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

**Answer: C**

**NEW QUESTION 4**

Exhibit.

**CLASSIFICATION DETAILS**

Malicious **runner**

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

**Answer: BD**

**NEW QUESTION 5**

What is true about classifications assigned by Fortinet Cloud Service (FCS)?

- A. The core is responsible for all classifications if FCS playbooks are disabled
- B. The core only assigns a classification if FCS is not available
- C. FCS revises the classification of the core based on its database
- D. FCS is responsible for all classifications

**Answer: C**

**NEW QUESTION 6**

Refer to the exhibit.

The screenshot shows the 'Process Creation' window in the Fortinet EDR console. It displays two processes:

- cmd.exe** (PID-8180, TID-8184):
  - Status: Running
  - Internal IP: 10.122.0.160
  - Up time: 6min, 6sec
  - Path: C:\Windows\System32\cmd.exe
  - Executing user: R2D2-KVM63\fortinet
  - Product: Microsoft® Windows® Operating System, v10.0.19041.746
  - SHA1: F115B0FD0DC156E4C61C5F78A54700E4E7984D55D
- PING.EXE** (PID-5764):
  - Path: C:\Windows\System32\PING.EXE
  - Executing user: R2D2-KVM63\fortinet
  - Parent: \Device\Harddisk\Volume2\Windows\System32\cmd.exe ID - 8180
  - Product: Microsoft® Windows® Operating System, v10.0.19041.1
  - SHA1: 9C13C854A4EF98879D0CAB80EF679B4C4ECCF518
  - Command line: fortinet.com

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

- A. The PING EXE process was blocked
- B. The user fortinet has executed a ping command
- C. The activity event is associated with the file action
- D. There are no MITRE details available for this event

**Answer:** AD

**NEW QUESTION 7**

FortiXDR relies on which feature as part of its automated extended response?

- A. Playbooks
- B. Security Policies
- C. Forensic
- D. Communication Control

**Answer:** B

**NEW QUESTION 8**

Which connectors can you use for the FortiEDR automated incident response? (Choose two.)

- A. FortiNAC
- B. FortiGate
- C. FortiSiem
- D. FortiSandbox

**Answer:** BC

**NEW QUESTION 9**

Which scripting language is supported by the FortiEDR action managed?

- A. TCL
- B. Python
- C. Perl
- D. Bash

**Answer:** A

**NEW QUESTION 10**

How does FortiEDR implement post-infection protection?

- A. By preventing data exfiltration or encryption even after a breach occurs
- B. By using methods used by traditional EDR
- C. By insurance against ransomware
- D. By real-time filtering to prevent malware from executing

**Answer:** D

**NEW QUESTION 10**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5\_EDR-5.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE5\_EDR-5.0 Product From:

[https://www.2passeasy.com/dumps/NSE5\\_EDR-5.0/](https://www.2passeasy.com/dumps/NSE5_EDR-5.0/)

## Money Back Guarantee

### **NSE5\_EDR-5.0 Practice Exam Features:**

- \* NSE5\_EDR-5.0 Questions and Answers Updated Frequently
- \* NSE5\_EDR-5.0 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE5\_EDR-5.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE5\_EDR-5.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year