



# 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.pass4itsure.com/nse5\\_edr-5-0.html](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

Which threat hunting profile is the most resource intensive?

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

Correct Answer: A

---

### QUESTION 2

Refer to the exhibit.



### Save Query

Query Name

Description

Tags

### Full Query

Category

Device

Community Query

Scheduled Query

Classification

Repeat every

Based on the threat hunting query shown in the exhibit which of the following is true?

- A. RDP connections will be blocked and classified as suspicious
- B. A security event will be triggered when the device attempts a RDP connection
- C. This query is included in other organizations
- D. The query will only check for network category

Correct Answer: B

### QUESTION 3

Which two types of remote authentication does the FortiEDR management console support? (Choose two.)

- A. Radius



B. SAML

C. TACACS D. LDAP

Correct Answer: BD

---

#### QUESTION 4

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 5

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

A. FortiNAC

B. FortiGate

C. FortiSiem

D. FortiSandbox

Correct Answer: AB

---

#### QUESTION 6

Which FortiEDR component is required to find malicious files on the entire network of an organization?

A. FortiEDR Aggregator

B. FortiEDR Central Manager

C. FortiEDR Threat Hunting Repository

D. FortiEDR Core

Correct Answer: C

---

#### QUESTION 7



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

---

### QUESTION 8

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

Correct Answer: A

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>

---

### QUESTION 9

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 10

Exhibit.

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
R2D2-KVM63	Windows Server 2016	C:\Windows\System32\cmd.exe	Malicious	Process Path: C:\Users\Administrator\Desktop\resources\ConnectivityTestApp.exe	10 Feb 2022 10:20:25	10 Feb 2022 10:17:30

Event Flow Diagram:

```

    graph LR
      A[1 Create] --> B[2 Create]
      B --> C[3 Create]
      C --> D[4 Create]
      D --> E[5 Detected  
Malicious]
      E --> F[6 Blocked]
  
```



Event 45179  
ConnectivityTestAppNe...

Add Exception | Retrievs | Remediate | Isolate | Export

DEVICE	OS	PROCESS	CLASSIFICATION
C8092231196	Windows Server 2016	ConnectivityTestAppNe...	Malicious

RAW ID: 926669227      Process Type: 32 bit      Certificate: Unsigned

Event Graph

```
graph LR; P1((Process: ConnectivityTestAppNew.exe)) --> A1[1 Create]; A1 --> P2((Process: ConnectivityTestAppNew.exe)); P2 --> A2[2 Create]; A2 --> P3((Process: ConnectivityTestAppNew.exe)); P3 --> A3[3 Create];
```

Clear All

Raw Data Items: All | Selected 1/3

DESTINATION	RECEIVED	LAST SEEN
File Read Attempt	13-Feb-2022, 23:26:30	14-Feb-2022, 00:37:30

Process Path: C:\Users\Administrator\Desktop\Resources\ConnectivityTestAppNew.exe      Count: 4

```
graph LR; P1((Process: ConnectivityTestAppNew.exe)) --> A1[4 Create]; A1 --> P2((Process: ConnectivityTestAppNew.exe)); P2 --> A2[5 Detected Malicious File Detected]; A2 --> A3[Block Execution]; A3 -.-> P3((Process: ConnectivityTestAppNew.exe));
```

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.

Correct Answer: AD