

## **EndExam** QUESTION & ANSWER

Accurate study guides, High passing rate!





We offer free update service for one year! http://www.endexam.com

## Exam : NSE5\_EDR-5.0

# Title:Fortinet NSE 5 - FortiEDR5.0 Exam

### Version : DEMO

#### 1.Refer to the exhibit.

| Save Query<br>Query Name | Query profile |            |    |                                       |  |
|--------------------------|---------------|------------|----|---------------------------------------|--|
| Description              |               |            |    |                                       |  |
| Tags                     | +             |            |    |                                       |  |
| Full Query               |               |            |    |                                       |  |
| Category                 |               | Device     |    |                                       |  |
| All Categories           | ~             | C80922311  | 96 | ~                                     |  |
|                          |               |            |    |                                       |  |
| Community C              |               |            |    |                                       |  |
|                          | wery ⑦        | luspicious |    |                                       |  |
| Scheduled Q              | wery ⑦        |            |    | · · · · · · · · · · · · · · · · · · · |  |

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

Answer: B

2. 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 Answer: C

#### 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

Answer: B,C

4.Exhibit.

| Event 45178 *<br>ConnectivityTestAppNe |                         |                       |                     |                            |   |                       | Ciear Al             |
|--|-------------------------|-----------------------|---------------------|----------------------------|---|-----------------------|----------------------|
| Antheopter To Horses (D) -             | innestato 🖾 Isolate - 🖸 | S Export              |                     |                            |   | Raw Data items: All   | 🖽 📝 Selected   1/3 🔹 |
| DEVICE                                 | 09                      | PROCESS               | CLASSIFICATION      | DESTINATION                | RECEIVED                                | LAST SEEN             |                      |
| C8092231196                            | Windows Server 2016     | ConnectivityTestAppNe | Malicious           | File Read Attempt          | 13-Feb-2022, 23-26-30                   | 14-Feb-2022, 00:37:30 | Ø Q                  |
| RAW ID: 926669227                      | Process Type            | e 32 bit Ge           | rtificate: Unsigned | Process Path. C. Users Adv | meistrator/Desktop/Resources/Connectivi | tyTestAppNew exe      | Count: 4             |
| 1 Creat                                | -                       | 2 Create              | 3 Create            | 4 Create                   | S Defected                              |                       |                      |
| Product                                | Press<br>prosta         |                       |                     |                            | Compatiblicity and                      |                       | Constant Strephen    |

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: A D

5.Exhibit.

| Add Exception    | Remediate Displate • | • C Export           |                     |                   |  | Raw Data Items: Al    | Selected 1/1 |  |
|------------------|----------------------|----------------------|---------------------|-------------------|--|-----------------------|--------------|--|
| DEVICE           | 05                   | PROCESS              | CLASSIFICATION      | DESTINATION       | RECEIVED                               | LAST SEEN             | -            |  |
| • • c3po-kvm48 👰 | Windows 10 Pro       | bot.exe              | Malicious           | File Read Attempt | 01-Jan-2022, 04:33:09                  | 04-jan-2022, 13:16:16 | Ø Q          |  |
| RAW ID: 119330-  | 467                  | Process Type: 32 bit | Certificate: Unsign | ed                | Process Path: C:\Users\fortinet\Deskto | plbot.exe             | Count: 135   |  |
|                  |                      |                      |                     |                   | 0                                      |                       |              |  |

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 m the stacks view
- C. The device has been isolated
- D. The exfiltration prevention policy has blocked this event

Answer: B C