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.leads4pass.com/nse5_edr-5-0.html

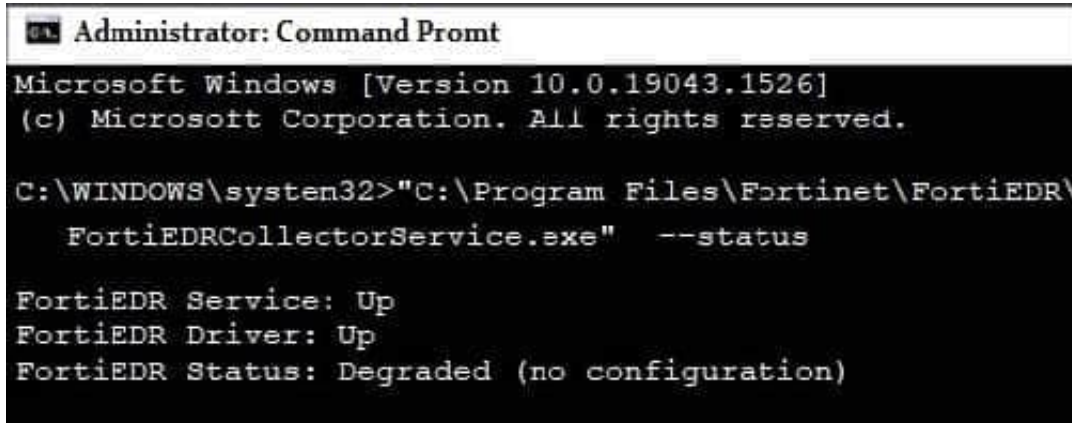## 100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibit.


```
Administrator: Command Promt

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 2

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 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

Which two statements are true about the remediation function in the threat hunting module? (Choose two.)

A. The file is removed from the affected collectors

B. The threat hunting module sends the user a notification to delete the file

C. The file is quarantined

D. The threat hunting module deletes files from collectors that are currently online.

Correct Answer: AD

QUESTION 5

Refer to the exhibit.

Save Query

Query Name | Query profile

Description

Tags | +

Full Query

Category | Device
All Categories | C8092231196

RemotePort3389

Community Query ⓘ
✓ Scheduled Query ⓘ

Classification ⓘ | Suspicious

Repeat every | 15 | Minutes

Save | Cancel

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 6

Which two events can trigger FortiEDR NGAV policy violations? (Choose two.)

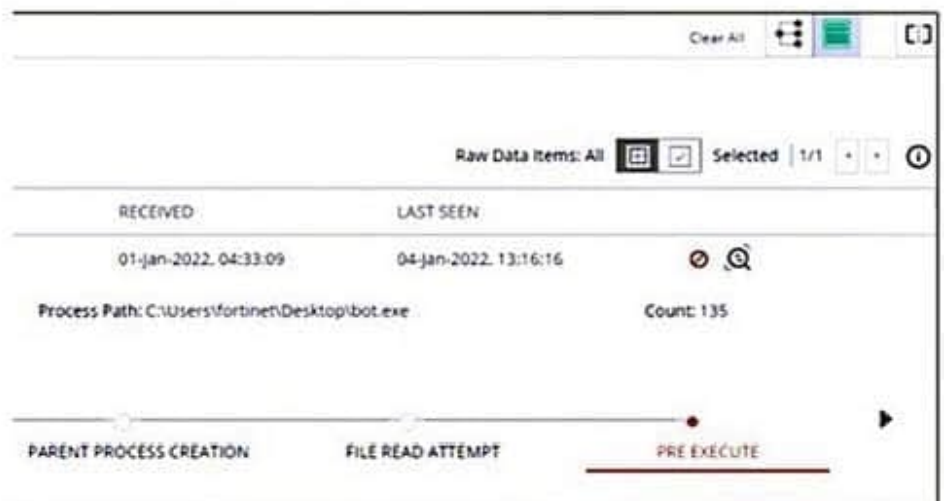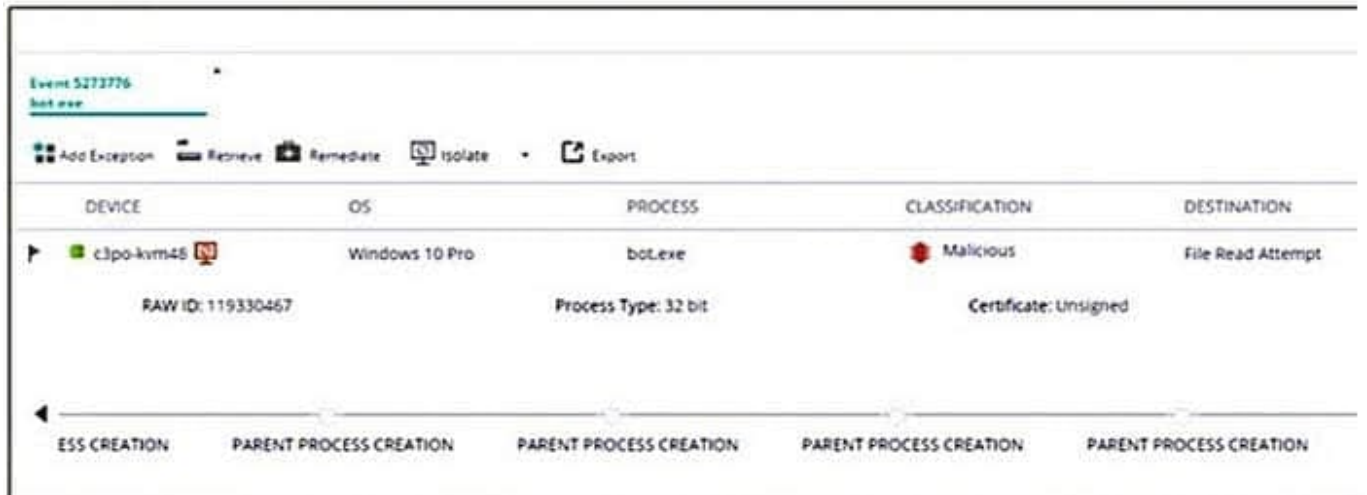A. When a malicious file attempts to communicate externally

B. When a malicious file is executed

C. When a malicious file is read

D. When a malicious file attempts to access data

Correct Answer: BC

NGAV reacts when a file is Saved, Read, or Executed Page 79 of the guide

---

QUESTION 7

Exhibit.

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

Correct Answer: BC

QUESTION 8

Which two criteria are requirements of integrating FortiEDR into the Fortinet Security Fabric? (Choose two.)

A. Core with Core only functionality

B. A Forensics add-on license

C. Central Manager connected to FCS

D. A valid API user with access to connectors

Correct Answer: CD

QUESTION 9

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 10

Exhibit.

CLASSIFICATION DETAILS

🐞 Malicious **FォRTINET**

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

[Latest NSE5_EDR-5.0 Dumps](#)

[NSE5_EDR-5.0 VCE Dumps](#)

[NSE5_EDR-5.0 Practice Test](#)