

# 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.leads4pass.com/nse5\\_edr-5-0.html](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

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



## QUESTION 1

Refer to the exhibit.

**Process Creation**

Summary    cmd.exe    PING.EXE    14-Feb-2022 12:33

**Host:** R2R2-kmv63    **Status:** Running    **Internal IP:** 10.122.0.160  
**Up time:** 6min, 6sec

**Process:** cmd.exe    **PID:** 8180    **TID:** 8184    **Architecture:** 64 bit

**Path:** C:\Windows\System32\cmd.exe

**Executing user:** R2D2-KVM63\fortinet

**Product:** Microsoft Windows Operating System, v10.0.19041.746

**SHA1:** F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D

**Process Creation**

**Process:** PING.EXE    **PID:** 5764    **Architecture:** 64 bit

**Path:** C:\Windows\System32\PING.EXE

**Executing user:** R2D2-KVM63\fortinet

**Parent:** \Device\HarddiskVolume2\Windows\System32\cmd.exe ID-8180

**Product:** Microsoft Windows Operating System, v10.0.19041.1

**SHA1:** 9C13C854A4EF98879D0CA880EF679B4C4ECCF518

**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

Correct Answer: BD

---

## QUESTION 2

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 3

The FortiEDR axe classified an event as inconclusive, out a few seconds later FCS revised the classification to malicious.

What playbook actions ate applied to the event?

- A. Playbook actions applied to inconclusive events
- B. Playbook actions applied to handled events
- C. Playbook actions applied to suspicious events
- D. Playbook actions applied to malicious events

Correct Answer: D

---

## QUESTION 4

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 5

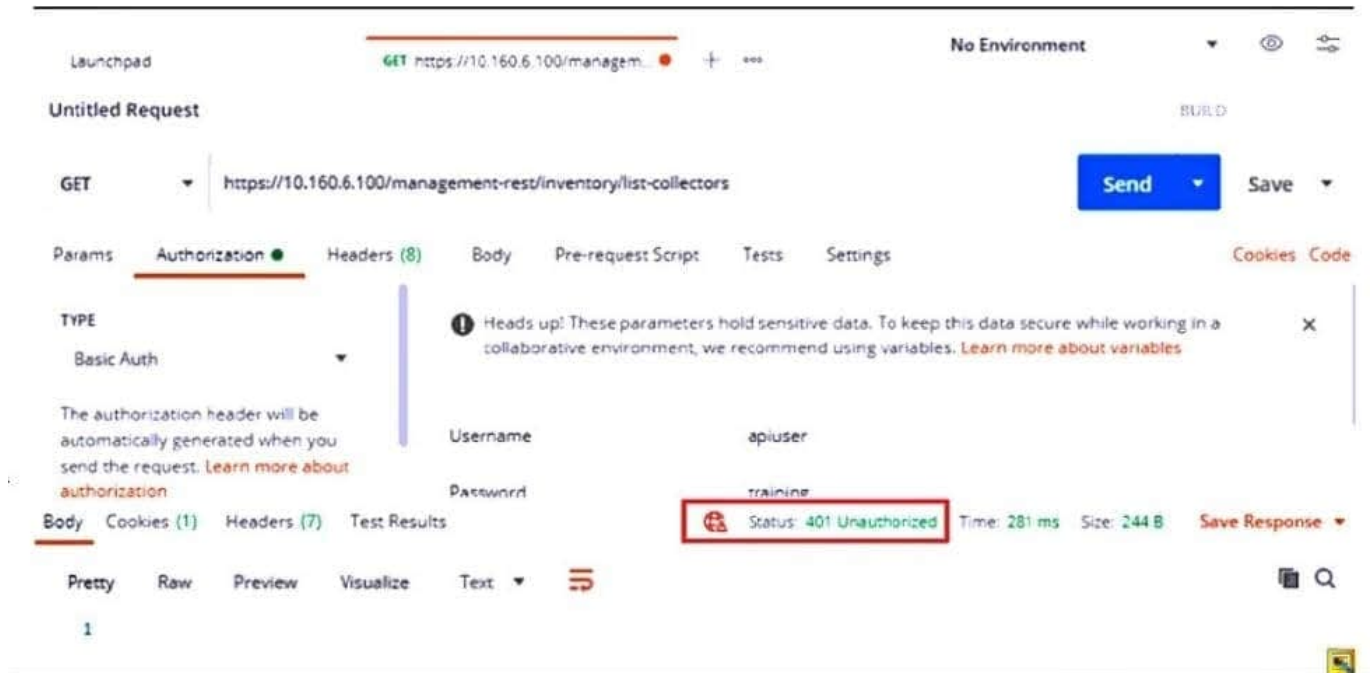
What is the role of a collector in the communication control policy?

- A. A collector blocks unsafe applications from running
- B. A collector is used to change the reputation score of any application that collector runs
- C. A collector records applications that communicate externally
- D. A collector can quarantine unsafe applications from communicating

Correct Answer: C

## QUESTION 6

Refer to the exhibit.



Based on the postman output shown in the exhibit why is the user getting an unauthorized error?

- A. The user has been assigned Admin and Rest API roles
- B. FortiEDR requires a password reset the first time a user logs in
- C. Postman cannot reach the central manager

D. API access is disabled on the central manager

Correct Answer: B

---

## QUESTION 7

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 8

Which two types of traffic are allowed while the device is in isolation mode? (Choose two.)

- A. Outgoing SSH connections
- B. HTTP sessions
- C. ICMP sessions
- D. Incoming RDP connections

Correct Answer: CD

---

## QUESTION 9

Exhibit.

Event 5273776  
bot.exe

Raw Data Items: All ☒ Selected | 1/1

DEVICE	OS	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

RAW ID: 119330467 Process Type: 32 bit Certificate: Unsigned Process Path: C:\Users\fortinet\Desktop\bot.exe Count: 135

ESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION FILE READ ATTEMPT PRE EXECUTE

Event 5273776  
bot.exe

Raw Data Items: All ☒ Selected | 1/1

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION
c3po-kvm48	Windows 10 Pro	bot.exe	Malicious	File Read Attempt

RAW ID: 119330467 Process Type: 32 bit Certificate: Unsigned

ESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION PARENT PROCESS CREATION

Raw Data Items: All ☒ Selected | 1/1

RECEIVED	LAST SEEN
01-Jan-2022, 04:33:09	04-Jan-2022, 13:16:16

Process Path: C:\Users\fortinet\Desktop\bot.exe Count: 135

PARENT PROCESS CREATION FILE READ ATTEMPT PRE EXECUTE

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

Correct Answer: BC

## QUESTION 10

What is the benefit of using file hash along with the file name in a threat hunting repository search?

- A. It helps to make sure the hash is really a malware
- B. It helps to check the malware even if the malware variant uses a different file name
- C. It helps to find if some instances of the hash are actually associated with a different file
- D. It helps locate a file as threat hunting only allows hash search

Correct Answer: B

[NSE5\\_EDR-5.0 PDF Dumps](#)

[NSE5\\_EDR-5.0 VCE Dumps](#)

[NSE5\\_EDR-5.0 Braindumps](#)