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.

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

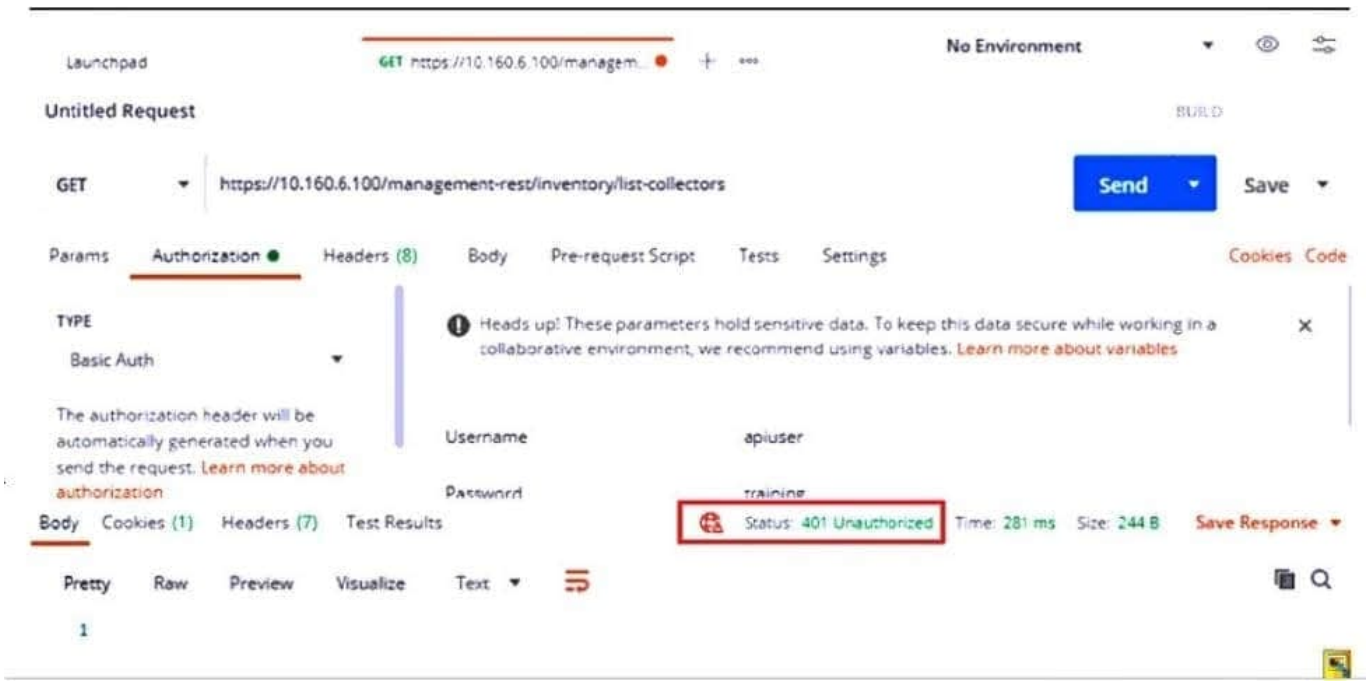
C. A collector records applications that communicate externally

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

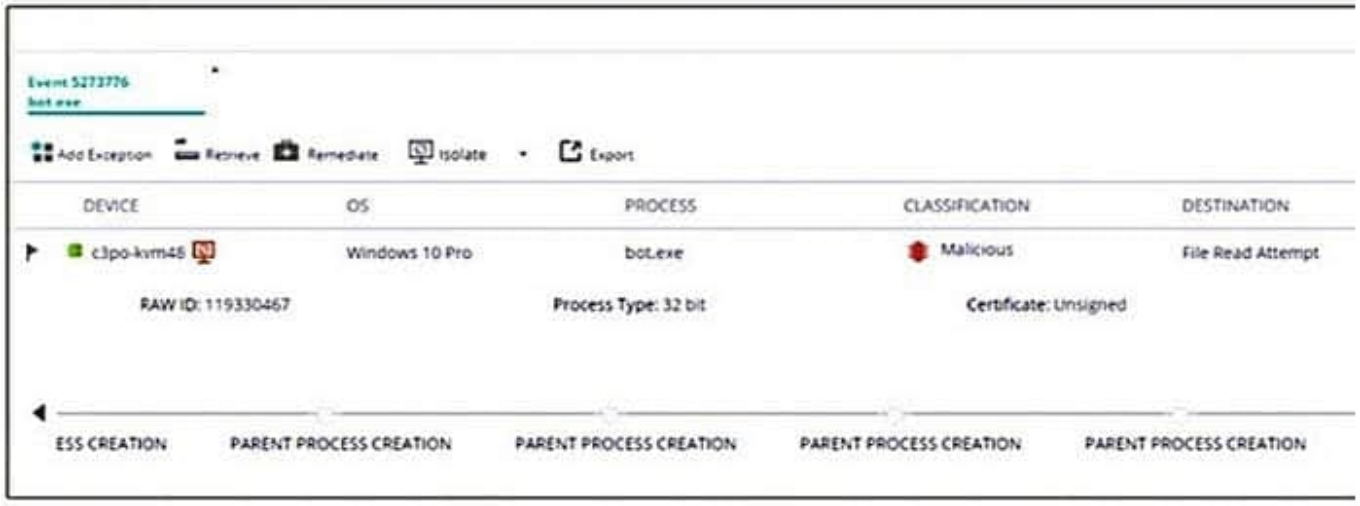
B. HTTP sessions

C. ICMP sessions D. Incoming RDP connections

Correct Answer: CD

QUESTION 9

Exhibit.



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 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