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.passapply.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

FortiXDR relies on which feature as part of its automated extended response?

A. Playbooks

B. Security Policies

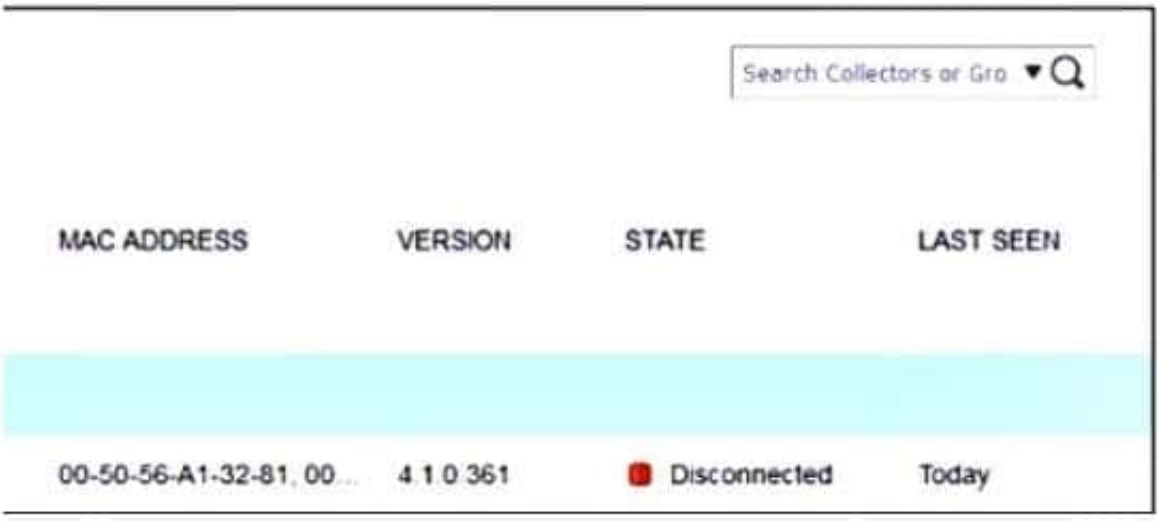
C. Forensic

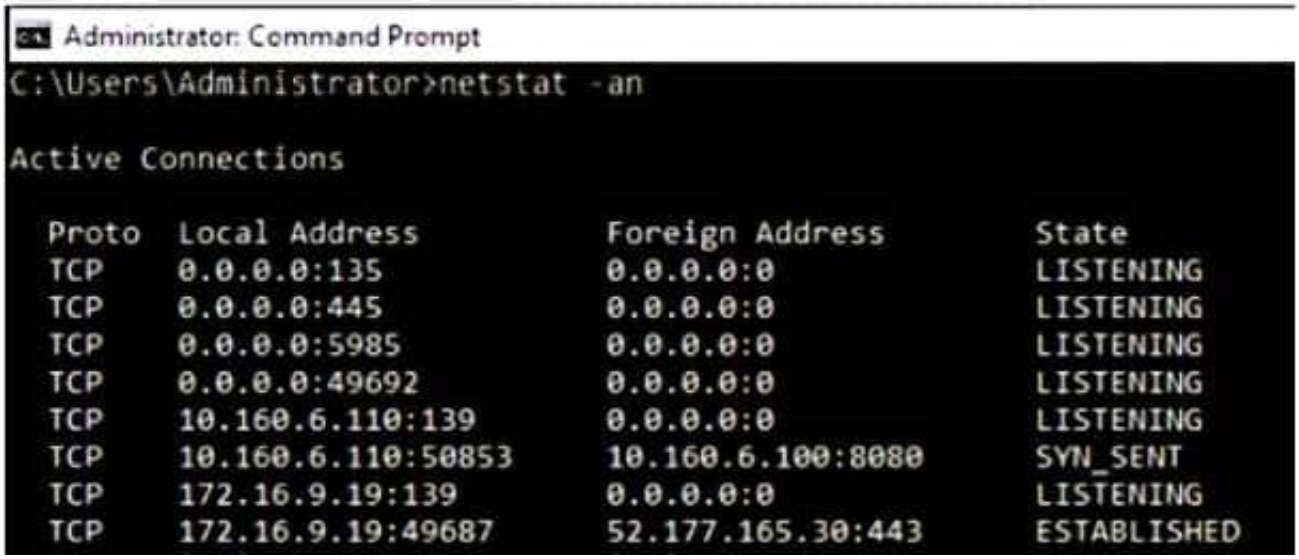
D. Communication Control

Correct Answer: A

QUESTION 2

Refer to the exhibits.





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 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

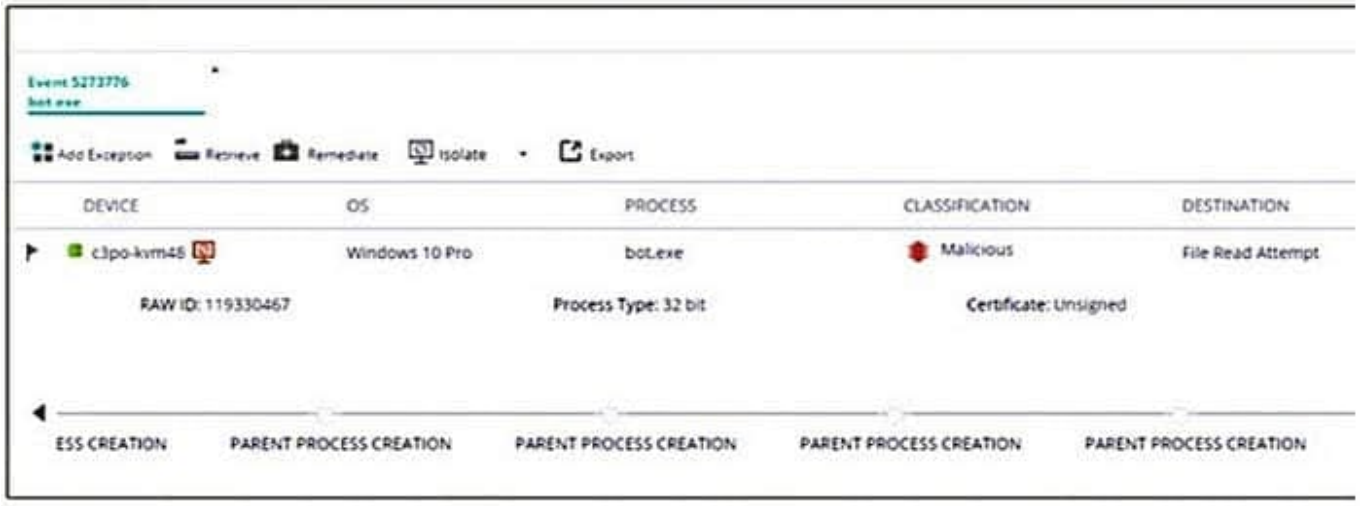
D. Execute playbooks to isolate affected collectors in the organization

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

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 5

An administrator finds a third party free software on a user\\'s computer mat does not appear in me application list in the communication control console

Which two statements are true about this situation? (Choose two)

A. The application is allowed in all communication control policies

B. The application is ignored as the reputation score is acceptable by the security policy

C. The application has not made any connection attempts

D. The application is blocked by the security policies

Correct Answer: CD