Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

https://www.2passeasy.com/dumps/NSE5_EDR-5.0/

NEW QUESTION 1
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

Answer: B

NEW QUESTION 2
Exhibit.

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.

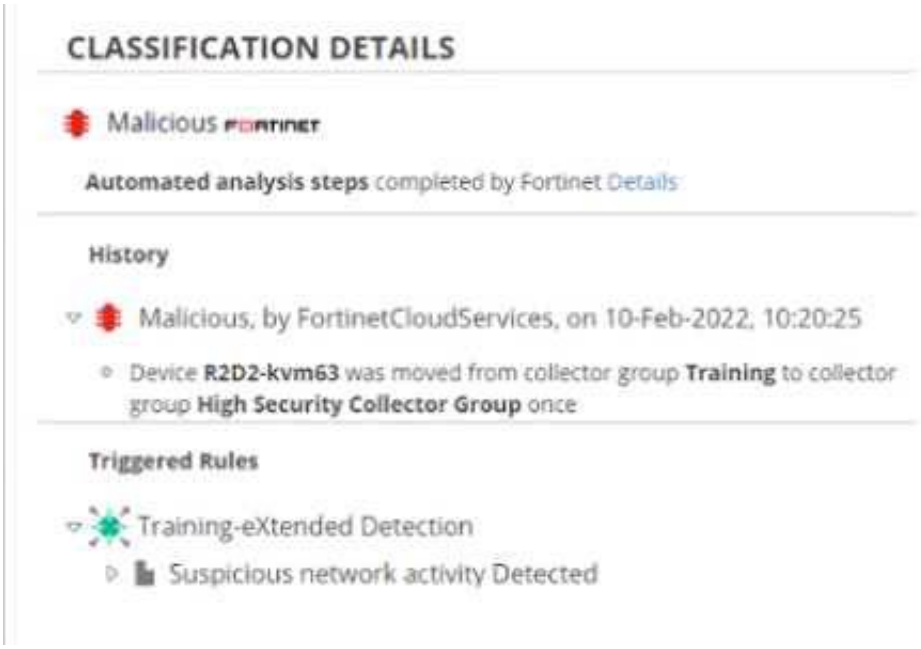
Answer: BC

NEW QUESTION 3
An administrator needs to restrict access to the ADMINISTRATION tab inthe central manager for a specific account.
What role should the administrator assign to this account?

A. Admin
B. User
C. Local Admin
D. REST API

Answer: C

NEW QUESTION 4
Exhibit.



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

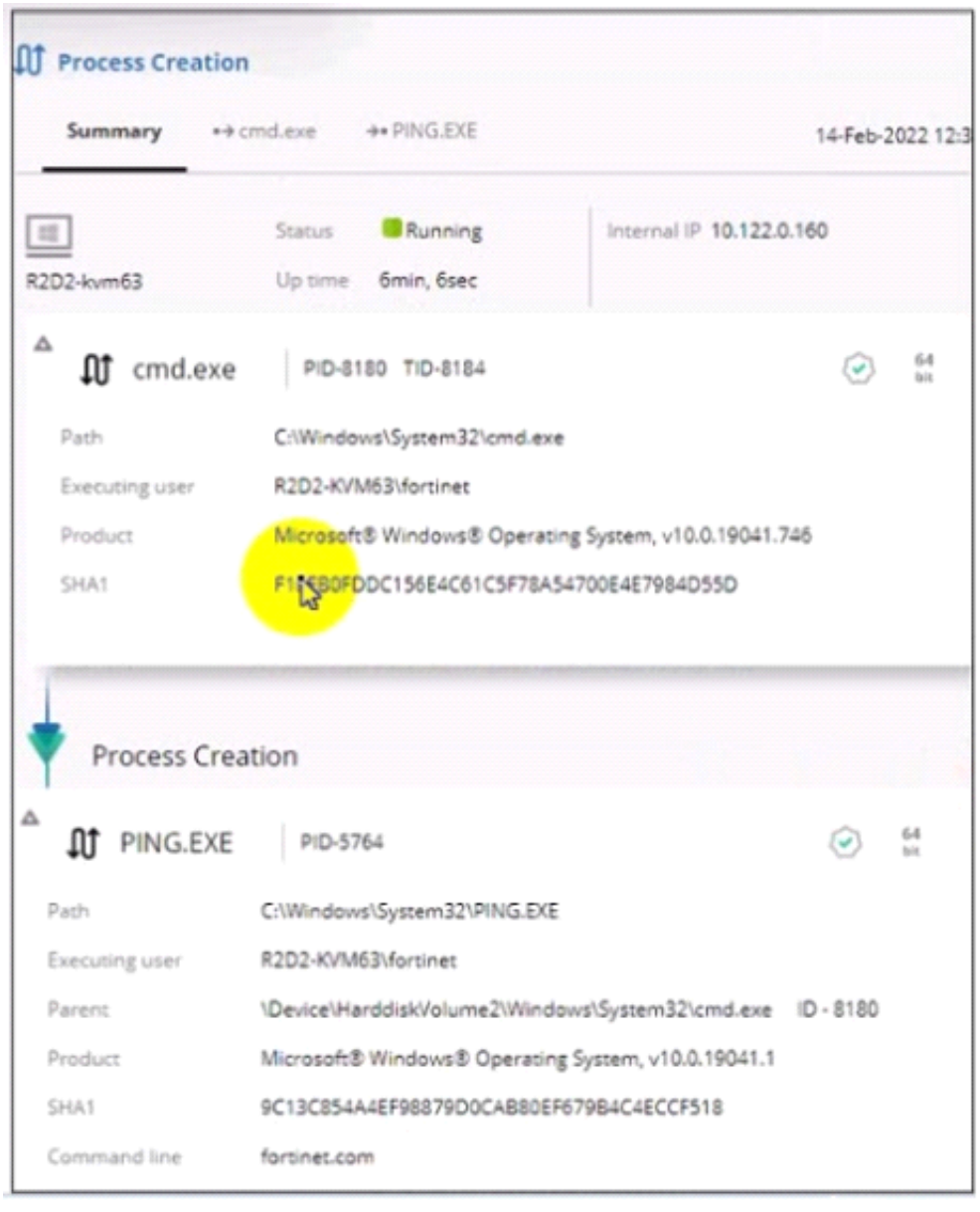
Answer: BD

NEW QUESTION 5
What is true about classifications assigned by Fortinet Cloud Sen/ice (FCS)?

A. The core is responsible for all classifications if FCS playbooks are disabled
B. The core only assigns a classification if FCS is not available
C. FCS revises the classification of the core based on its database
D. FCS is responsible for all classifications

Answer: C

NEW QUESTION 6
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

Answer: AD

NEW QUESTION 7
FortiXDR relies on which feature as part of its automated extended response?

A. Playbooks
B. Security Policies
C. Forensic
D. Communication Control

Answer: B

NEW QUESTION 8
Which connectors can you use for the FortiEDR automated incident response? (Choose two.)

A. FortiNAC
B. FortiGate
C. FortiSiem
D. FortiSandbox

Answer: BC

NEW QUESTION 9
Which scripting language is supported by the FortiEDR action managed?

A. TCL
B. Python
C. Perl
D. Bash

Answer: A

NEW QUESTION 10
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

Answer: D

NEW QUESTION 10
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5_EDR-5.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE5_EDR-5.0 Product From:

https://www.2passeasy.com/dumps/NSE5_EDR-5.0/

Money Back Guarantee

NSE5_EDR-5.0 Practice Exam Features:

* NSE5_EDR-5.0 Questions and Answers Updated Frequently

* NSE5_EDR-5.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_EDR-5.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_EDR-5.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year