Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

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

NEW QUESTION 1
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 2
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

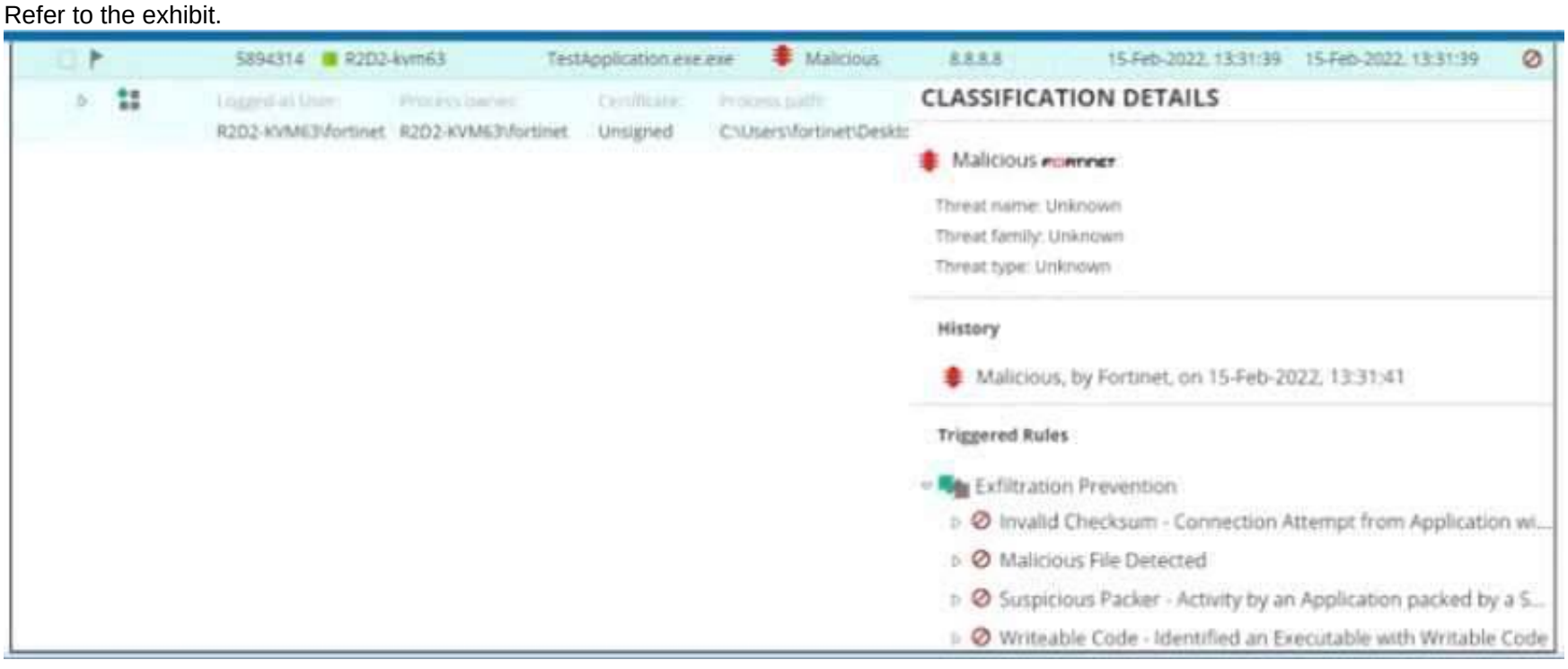
Answer: A

NEW QUESTION 3
Which FortiEDR component is required to find malicious files on the entire network of an organization?

A. FortiEDR Aggregator
B. FortiEDR Central Manager
C. FortiEDR Threat Hunting Repository
D. FortiEDR Core

Answer: A

NEW QUESTION 4
Refer to the exhibit.

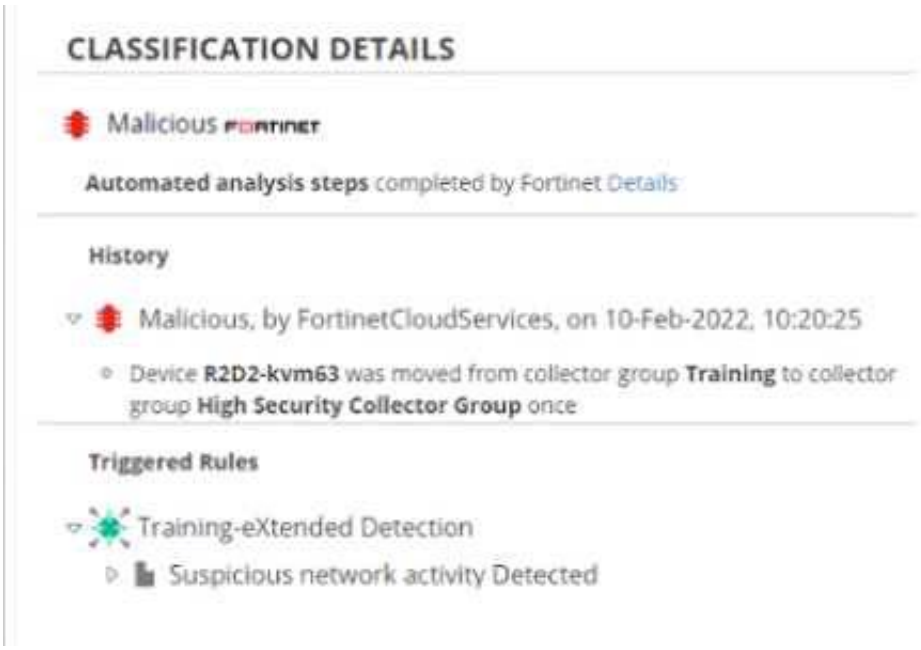


Based on the event shown in the exhibit, which two statements about the event are true? (Choose two.)

A. The NGAV policy has blocked TestApplication exe
B. TestApplication exe is sophisticated malware
C. The user was able to launch TestApplication exe
D. FCS classified the event as malicious

Answer: AB

NEW QUESTION 5
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

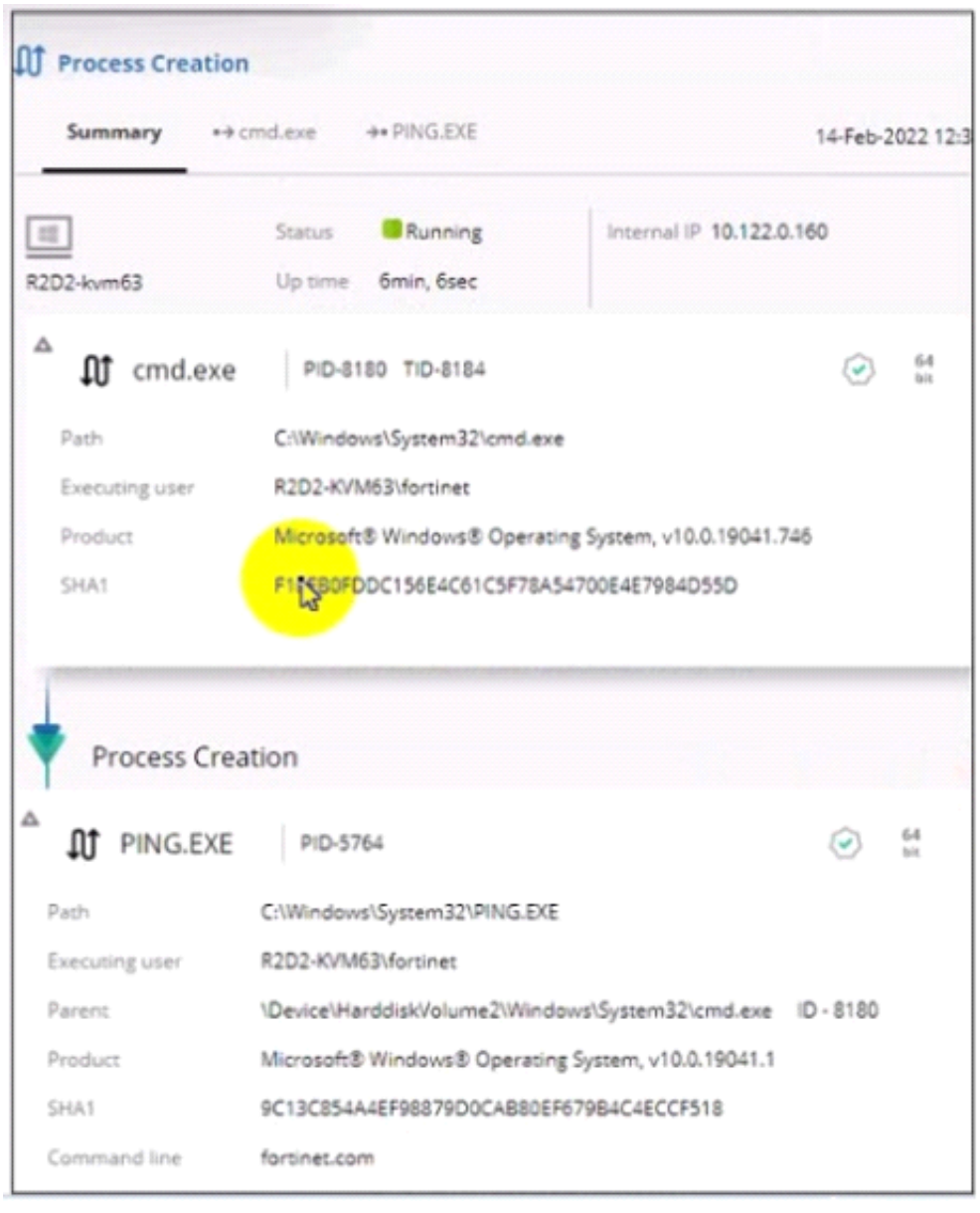
Answer: BD

NEW QUESTION 6
A company requires a global communication policy for a FortiEDR multi-tenant environment. How can the administrator achieve this?

A. An administrator creates a new communication control policy and shares it with other organizations
B. A local administrator creates new a communication control policy and shares it with other organizations
C. A local administrator creates a new communication control policy and assigns it globally to all organizations
D. An administrator creates a new communication control policy for each organization

Answer: C

NEW QUESTION 7
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 8
Which security policy has all of its rules disabled by default?

A. Device Control
B. Ransomware Prevention
C. Execution Prevention
D. Exfiltration Prevention

Answer: B

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