Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

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

NEW QUESTION 1
Which two statements are true about the remediation function in the threat hunting module? (Choose two.)

A. The file is removed from the affected collectors
B. The threat hunting module sends the user a notification to delete the file
C. The file is quarantined
D. The threat hunting module deletes files from collectors that are currently online.

Answer: BC

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
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 ofa known malicious file or hash inthe 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

Answer: C

NEW QUESTION 4
Refer to the exhibit.

Based on the FortiEDR status output shown in the exhibit, which two statements about the FortiEDR collector are true? (Choose two.)

A. The collector device has windows firewall enabled
B. The collector has been installed with an incorrect port number
C. The collector has been installed with an incorrect registration password
D. The collector device cannot reach the central manager

Answer: BD

NEW QUESTION 5
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 6
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

Answer: CD

NEW QUESTION 7
Refer to the exhibit.

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

A. A partial exception is applied to this event
B. FCS playbooks is enabled by Fortinet support
C. The exception is applied only on device C8092231196
D. The system owner can modify the trigger rules parameters

Answer: AC

NEW QUESTION 8
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 9
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

Answer: D

NEW QUESTION 10
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 10
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 15
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

Answer: C

NEW QUESTION 17
Which two statements about the FortiEDR solution are true? (Choose two.)

A. It provides pre-infection and post-infection protection
B. It is Windows OS only
C. It provides central management
D. It provides pant-to-point protection

Answer: AD

NEW QUESTION 22
.....

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