Fortinet

Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

NEW QUESTION 1
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

Answer: AD

NEW QUESTION 2
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

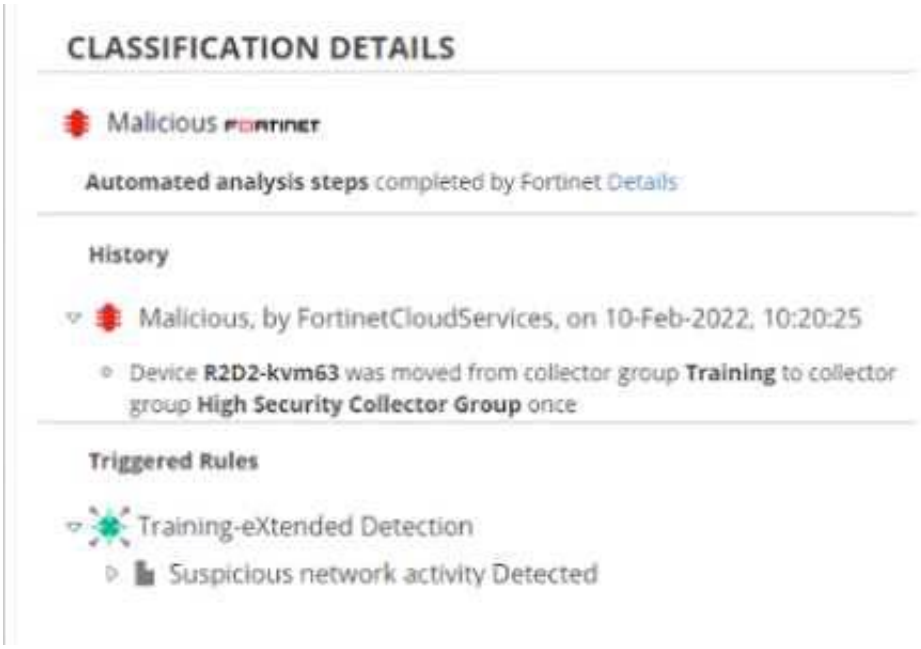
NEW QUESTION 3
Refer to the exhibit.

Based on the threat hunting query shown in the exhibit which of the following is true?

A. RDP connections will be blocked and classified as suspicious
B. A security event will be triggered when the device attempts a RDP connection
C. This query is included in other organizations
D. The query will only check for network category

Answer: B

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
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 7
Which threat hunting profile is the most resource intensive?

A. Comprehensive
B. Inventory
C. Default
D. Standard Collection

Answer: A

NEW QUESTION 10
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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