Fortinet

Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

NEW QUESTION 1
A FortiEDR security event is causing a performance issue with a third-parry application. What must you do first about the event?

A. Contact Fortinet support
B. Terminate the process and uninstall the third-party application
C. Immediately create an exception
D. Investigate the event to verify whether or not the application is safe

Answer: C

NEW QUESTION 2
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

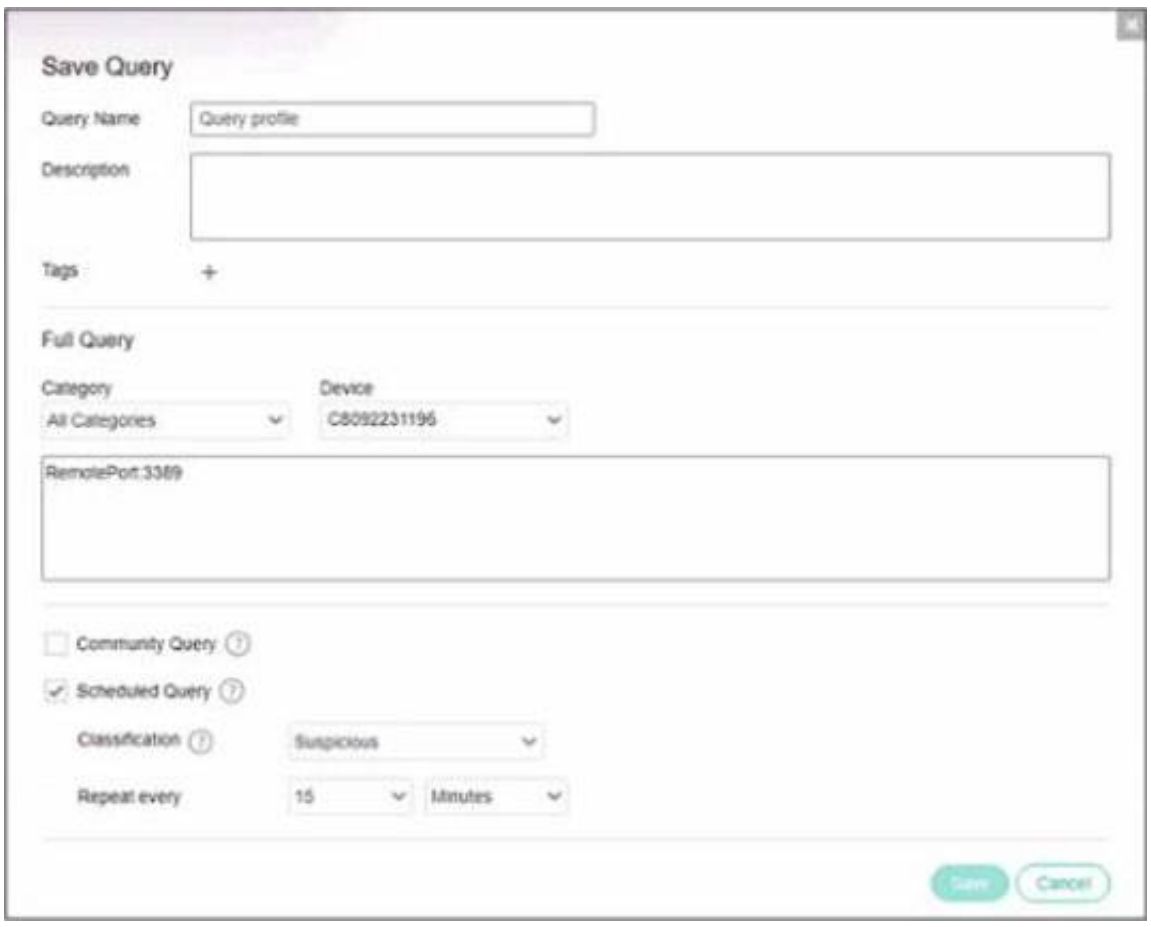
Answer: AD

NEW QUESTION 3
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 4
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

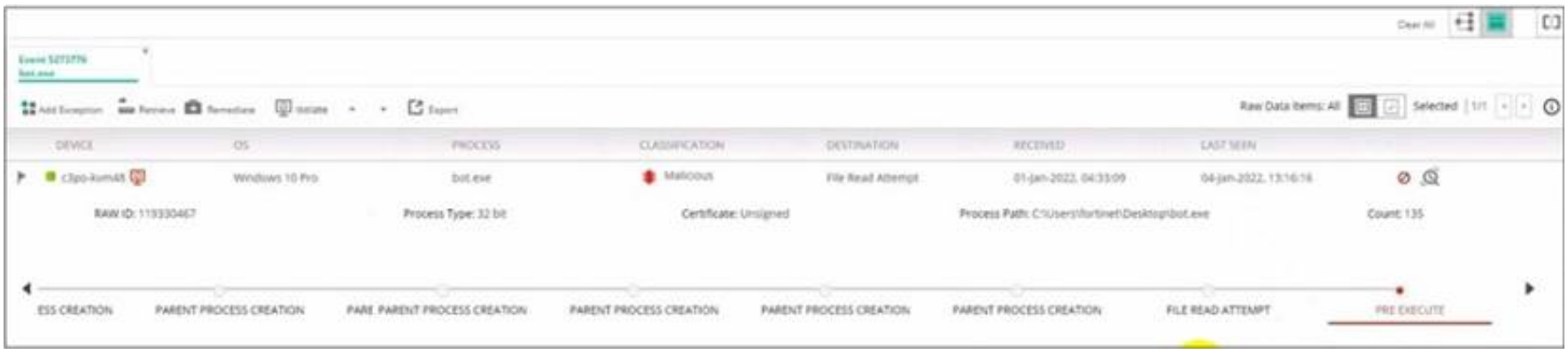
NEW QUESTION 5
Refer to the exhibit.

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.

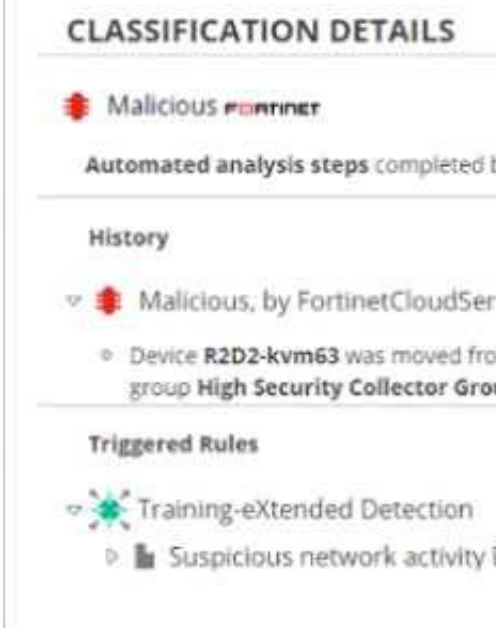


Based on the forensics data shown in the exhibit, which two statements are true? (Choose two.)

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
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 8
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 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
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 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 12
.....

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