Fortinet

Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

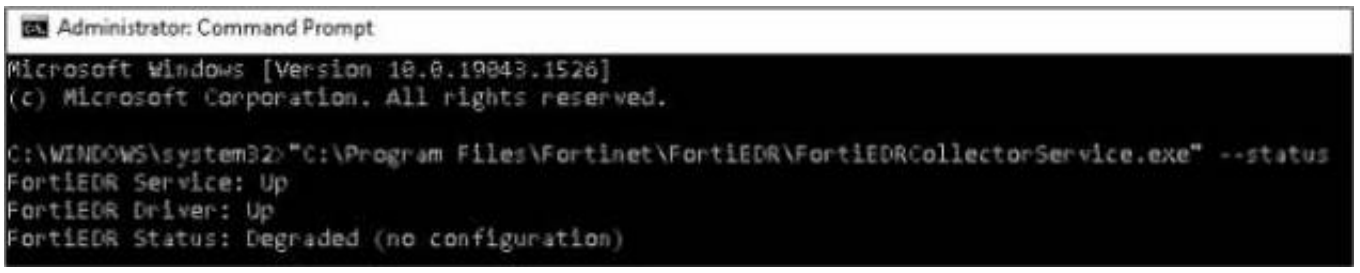
Answer: C

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
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

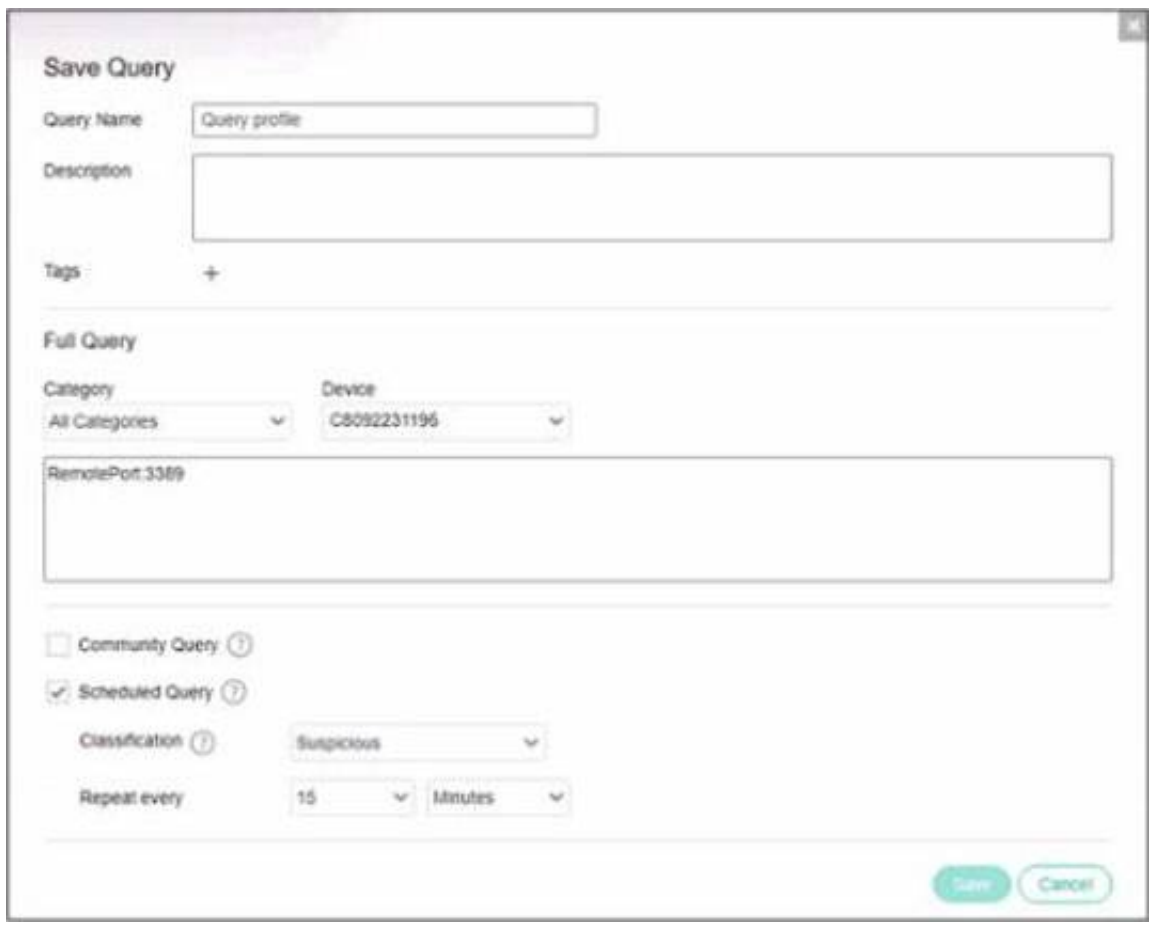
Answer: BD

NEW QUESTION 4
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 5
Refer to the exhibit.

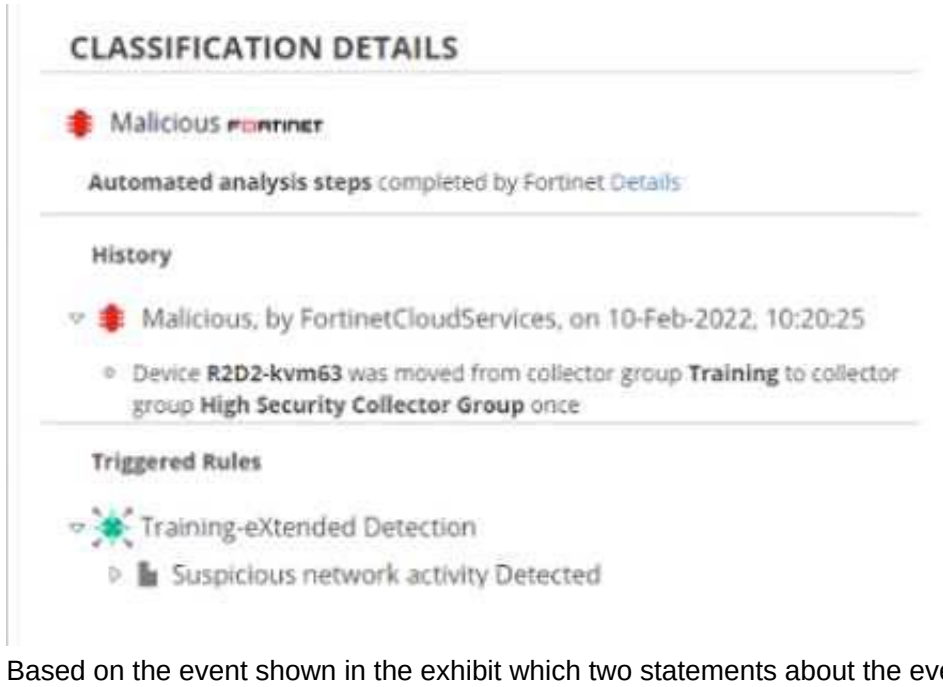


Based on the threat hunting query shown in the exhibit which of the following is true?

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 6
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 7
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 8
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 9
Which scripting language is supported by the FortiEDR action managed?

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

Answer: A

NEW QUESTION 10
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 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 15
.....

Relate Links

100% Pass Your NSE5_EDR-5.0 Exam with Exambible Prep Materials

https://www.exambible.com/NSE5_EDR-5.0-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/