Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

NSE5_EDR-5.0 Dumps
NSE5_EDR-5.0 Braindumps
NSE5_EDR-5.0 Real Questions
NSE5_EDR-5.0 Practice Test
NSE5_EDR-5.0 Actual Questions

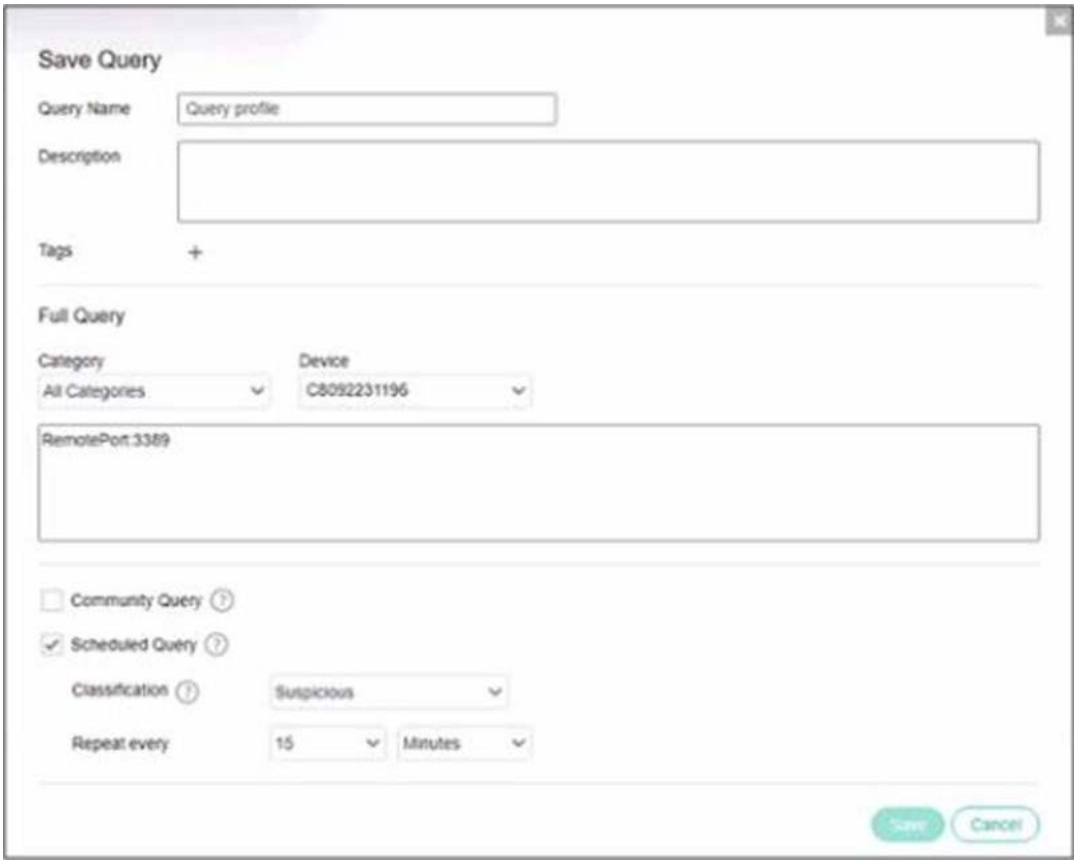
Fortinet

NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

Question: 129

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

Question: 130

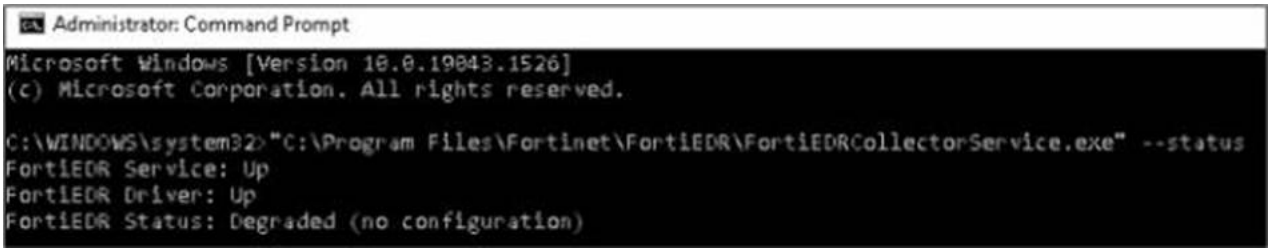
What is the purpose of the Threat Hunting feature?

A. Delete any file from any collector in the organization
B. Find and delete all instances of a known malicious file or hash in the 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

Question: 131

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: A,B,D

Question: 132

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: A,B,C

Question: 133

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: A,C,D

Question: 134

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

Question: 135

Which two types of remote authentication does the FortiEDR management console support? (Choose two.)

A. Radius
B. SAML
C. TACACS
D. LDAP

Answer: A,D

Question: 136

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: A,C

Question: 137

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: A

Question: 138

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

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*