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

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

**Answer:** AD

**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

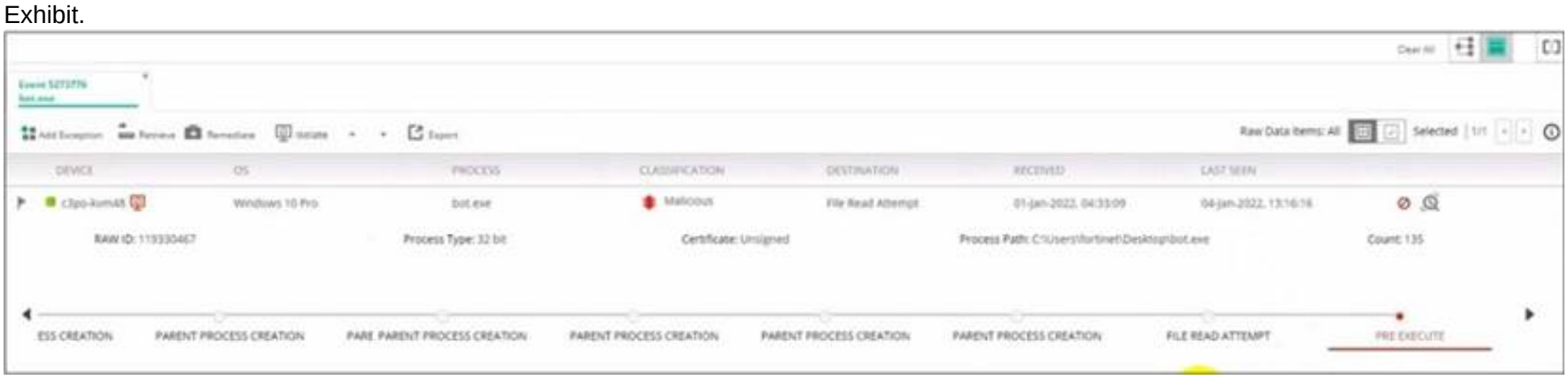
**Answer:** C

**NEW QUESTION 4**
Which FortiEDR component is required to find malicious files on the entire network of an organization?

A. FortiEDR Aggregator
B. FortiEDR Central Manager
C. FortiEDR Threat Hunting Repository
D. FortiEDR Core

**Answer:** A

**NEW QUESTION 5**
Exhibit.

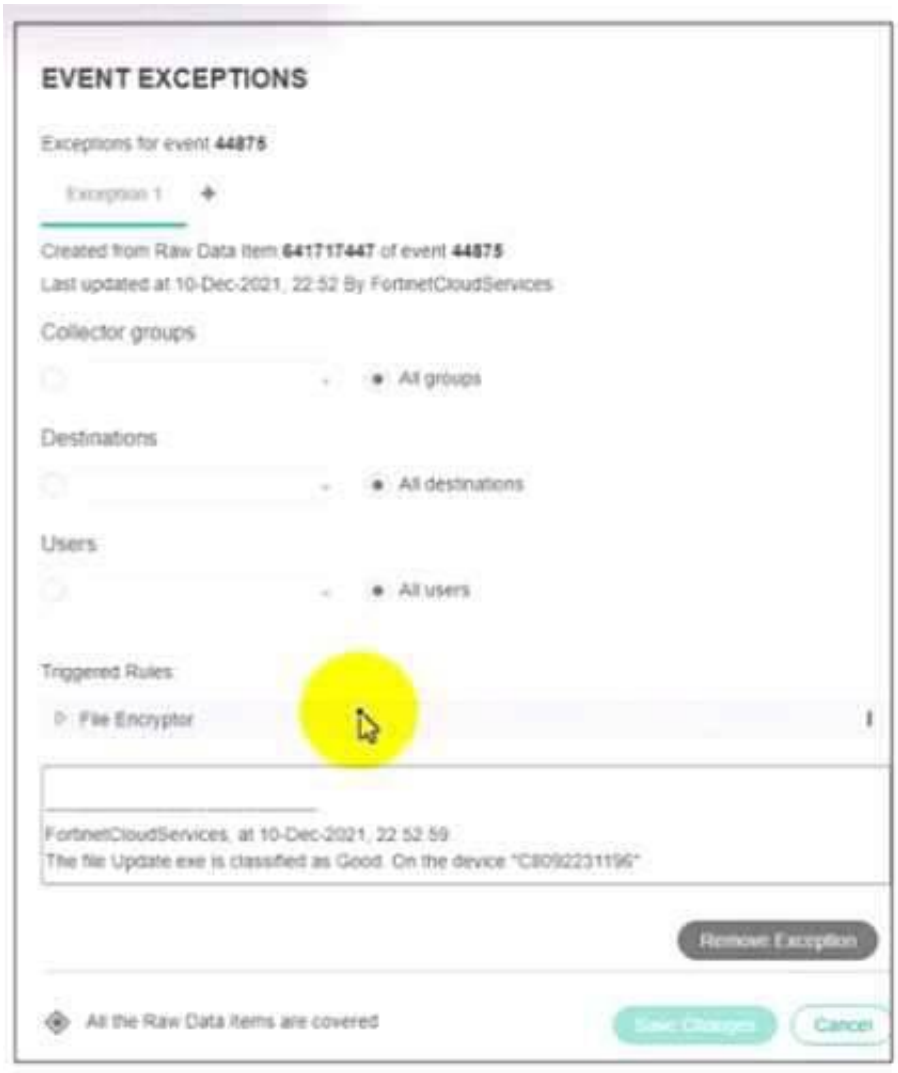



Based on the forensics data shown in the exhibit, which two statements are true? (Choose two.)

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 6**
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 7**
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 10**
.....

# 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/