NSE5_EDR-5.0 Q&As

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/nse5_edr-5-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: B

"Threat hunting allows management console users to find and remediate dormant threats before they execute. Essentially it\\'s a search and destroy operation."

QUESTION 2

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

A. FortiEDR Aggregator

B. FortiEDR Central Manager

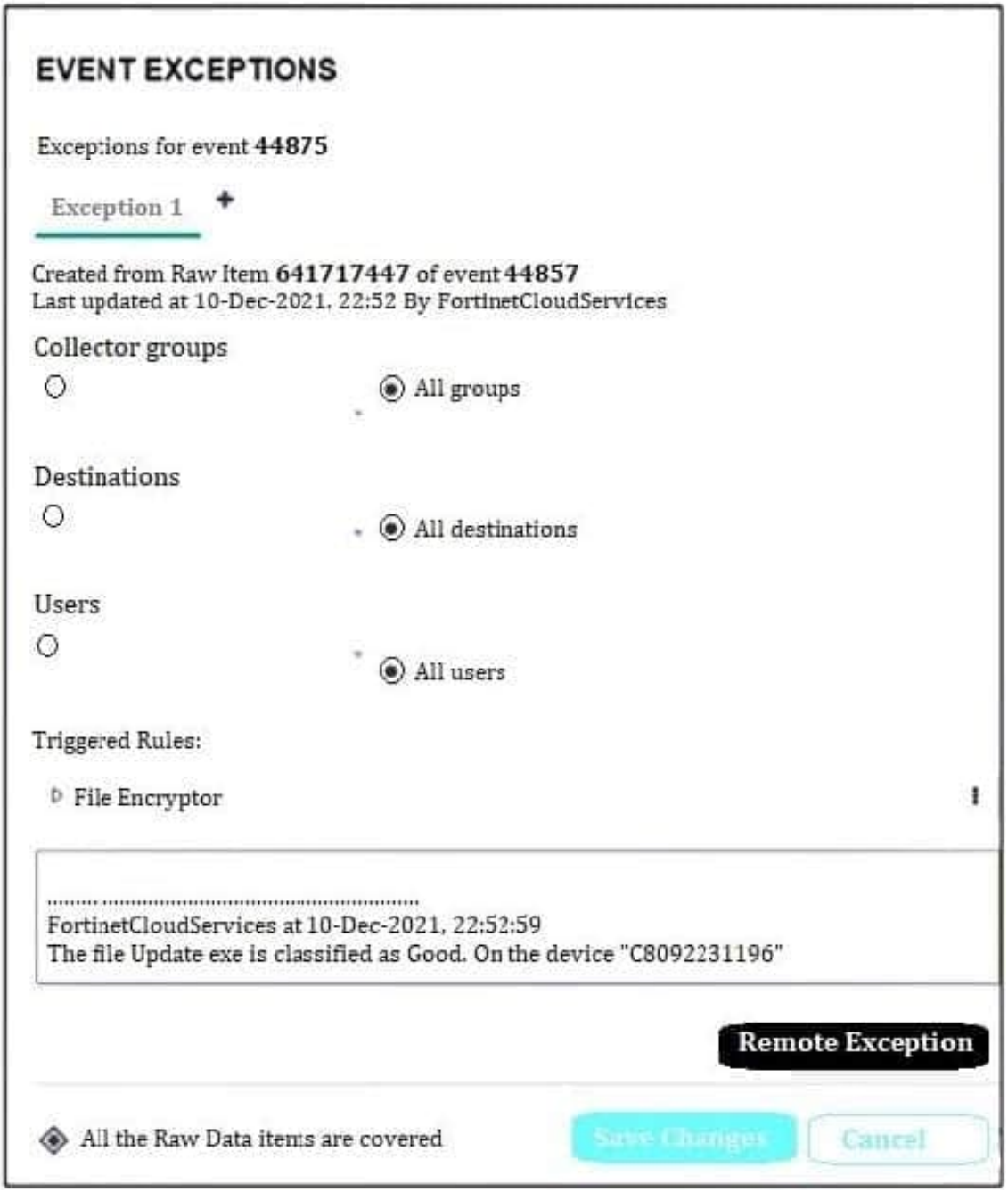
C. FortiEDR Threat Hunting Repository

D. FortiEDR Core

Correct Answer: C

QUESTION 3

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

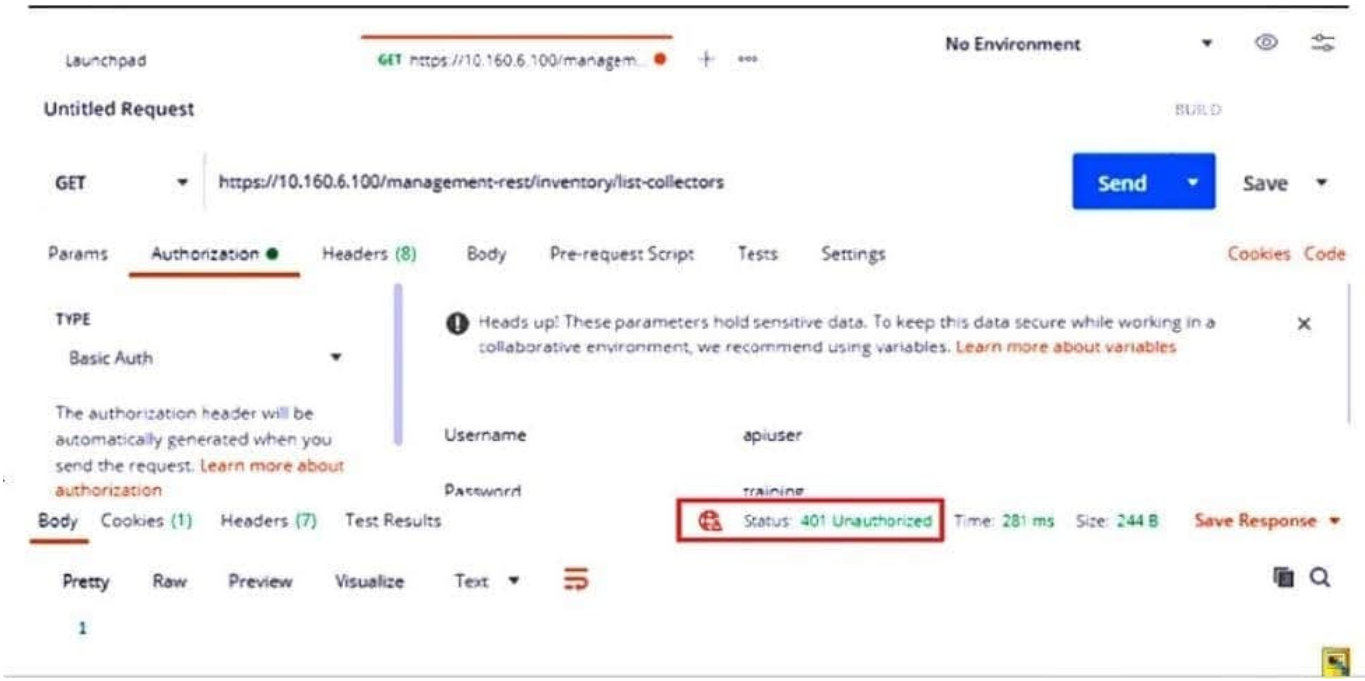
C. The exception is applied only on device C8092231196

D. The system owner can modify the trigger rules parameters

Correct Answer: AC

QUESTION 4

Refer to the exhibit.



Based on the postman output shown in the exhibit why is the user getting an unauthorized error?

A. The user has been assigned Admin and Rest API roles

B. FortiEDR requires a password reset the first time a user logs in

C. Postman cannot reach the central manager

D. API access is disabled on the central manager

Correct Answer: B

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

Correct Answer: C