



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 Guarantee

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

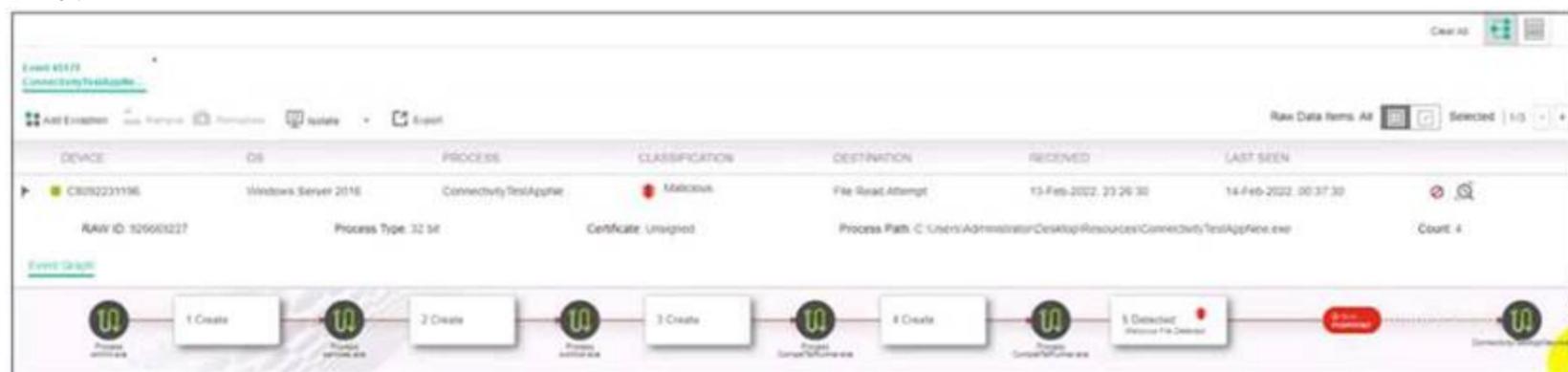
An administrator finds a third party free software on a user's computer that does not appear in the application list in the communication control console. Which two statements are true about this situation? (Choose two)

- 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

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: BC

NEW QUESTION 4

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

NEW QUESTION 5

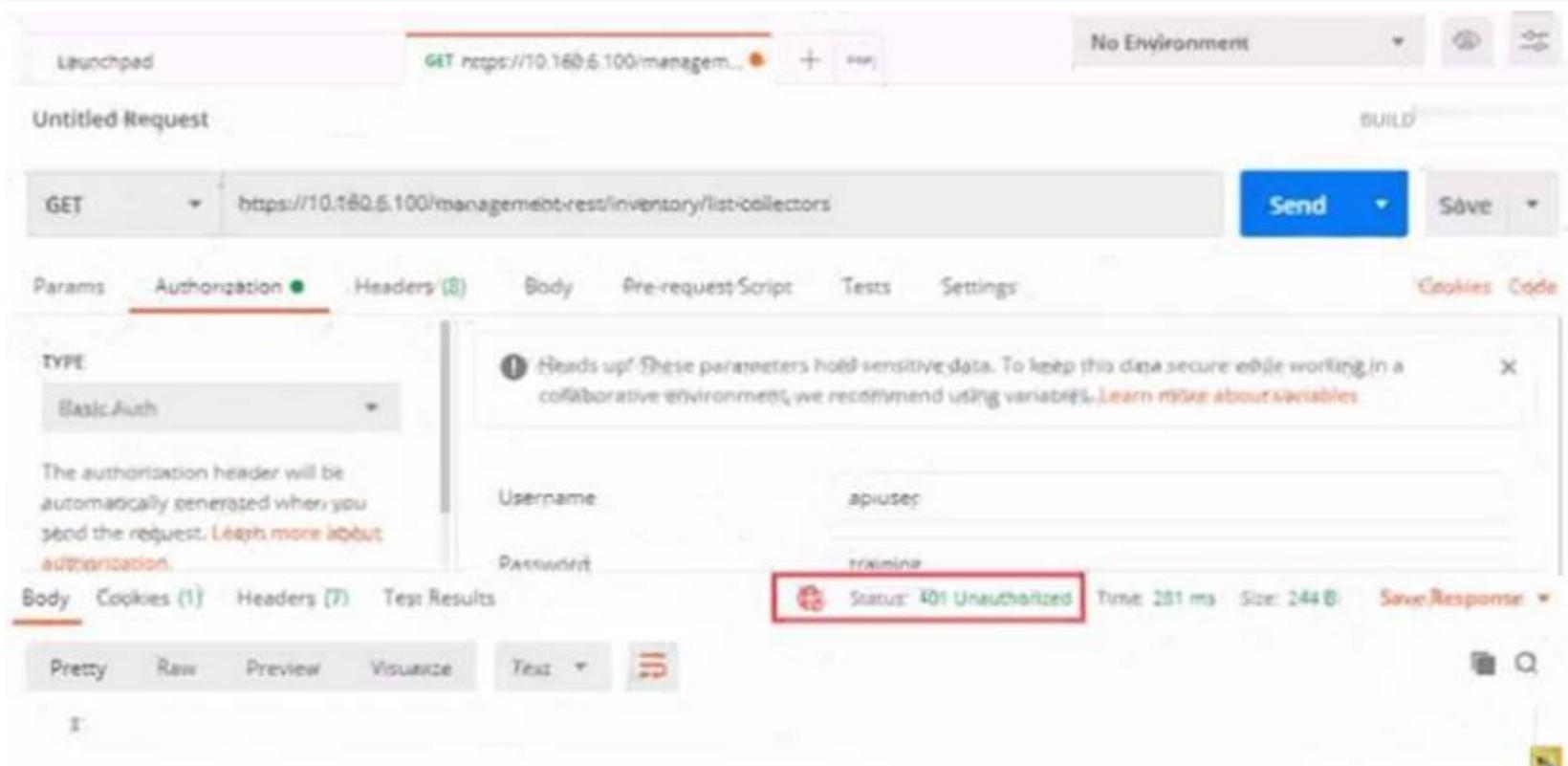
What is the role of a collector in the communication control policy?

- 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 6

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

Answer: A

NEW QUESTION 7

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 8

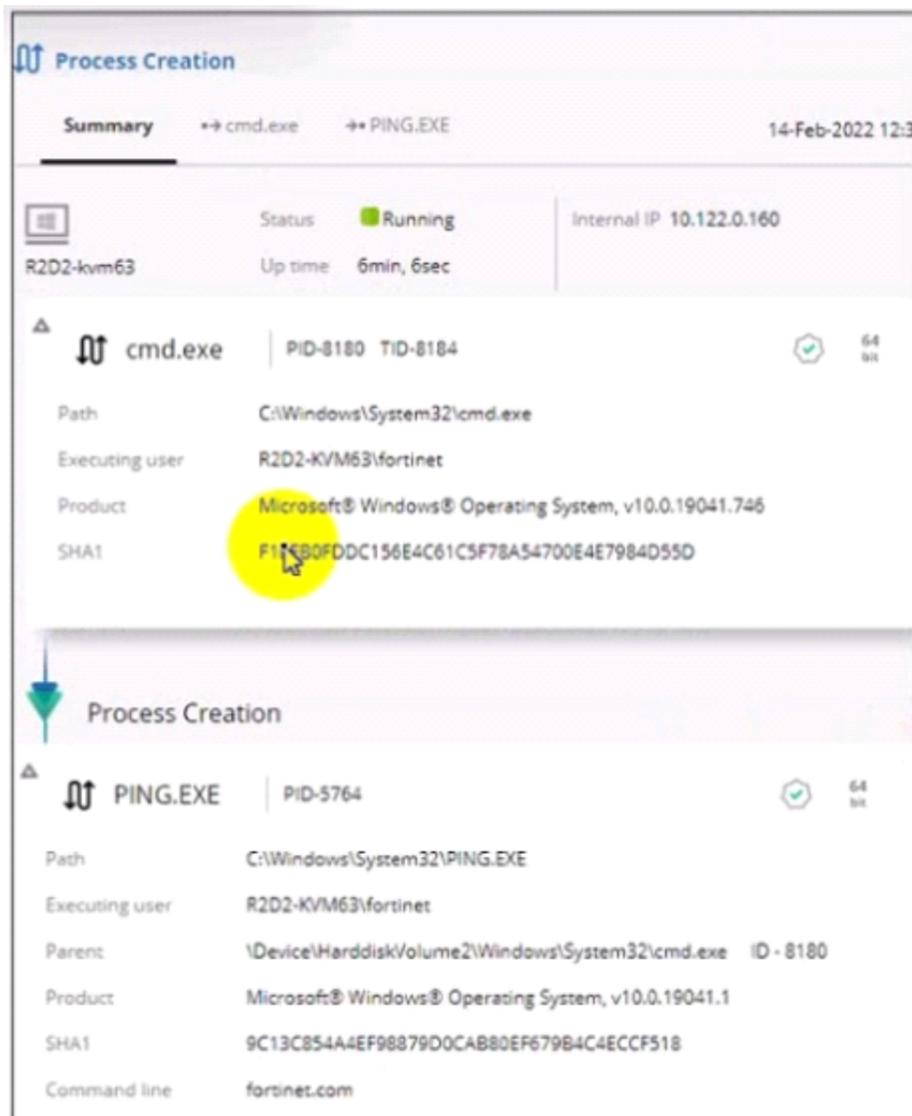
What is true about classifications assigned by Fortinet Cloud Sen/ice (FCS)?

- 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 9

Refer to the exhibit.



Based on the threat hunting event details shown in the exhibit, which two statements about the event are true? (Choose two.)

- A. The PING EXE process was blocked
- B. The user fortinet has executed a ping command
- C. The activity event is associated with the file action
- D. There are no MITRE details available for this event

Answer: AD

NEW QUESTION 10

FortiXDR relies on which feature as part of its automated extended response?

- A. Playbooks
- B. Security Policies
- C. Forensic
- D. Communication Control

Answer: B

NEW QUESTION 10

Which threat hunting profile is the most resource intensive?

- A. Comprehensive
- B. Inventory
- C. Default
- D. Standard Collection

Answer: A

NEW QUESTION 15

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 20

Which scripting language is supported by the FortiEDR action managed?

- A. TCL
- B. Python

- C. Perl
- D. Bash

Answer: A

NEW QUESTION 23

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 point-to-point protection

Answer: AD

NEW QUESTION 26

.....

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/>