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
Refer to the exhibits.

The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address 10.160.6.100 using default port.
Based on the netstat command output what must you do to resolve the connectivity issue?

A. Reinstall collector agent and use port 443
B. Reinstall collector agent and use port 8081
C. Reinstall collector agent and use port 555
D. Reinstall collector agent and use port 6514

Answer: B

NEW QUESTION 3
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 4
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

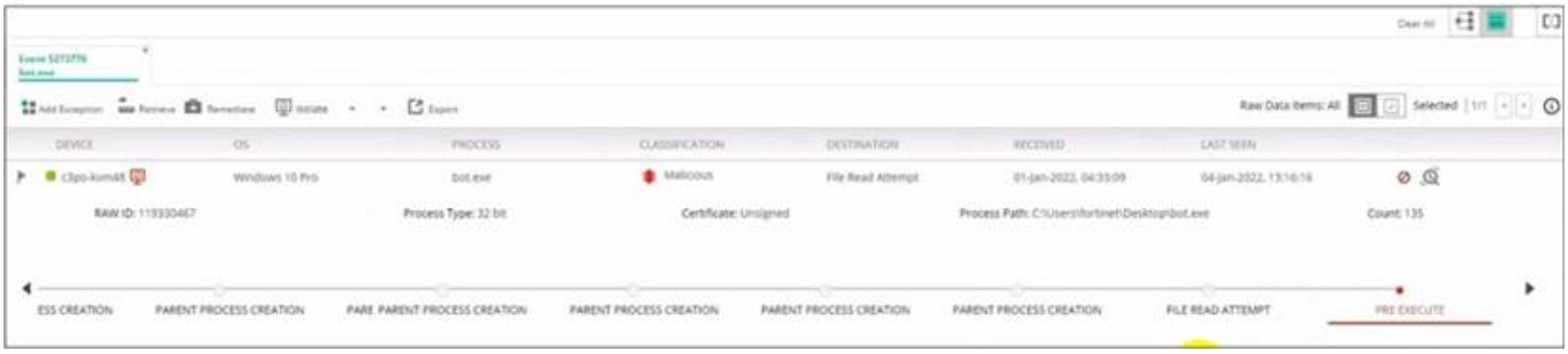
NEW QUESTION 5
Exhibit.

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 6
Exhibit.

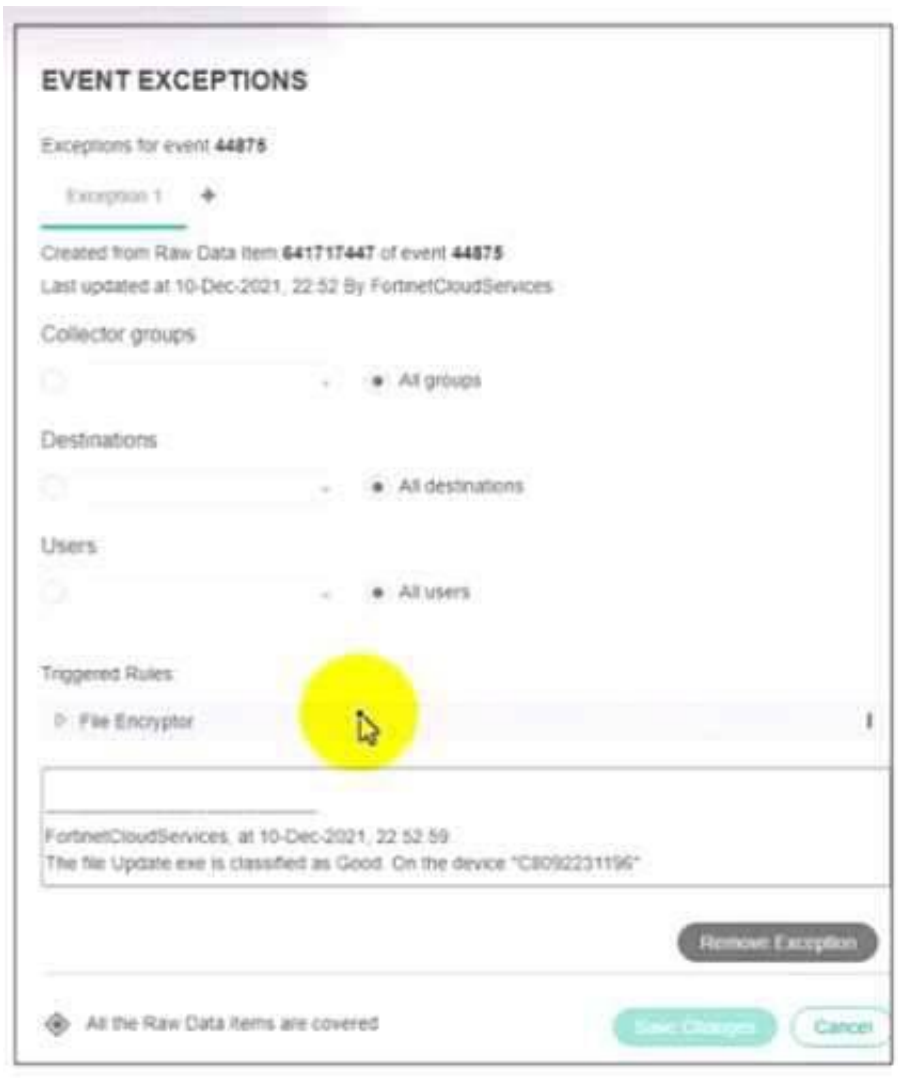


Based on the forensics data shown in the exhibit, which two statements are true? (Choose two.)

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 7
Refer to the exhibit.



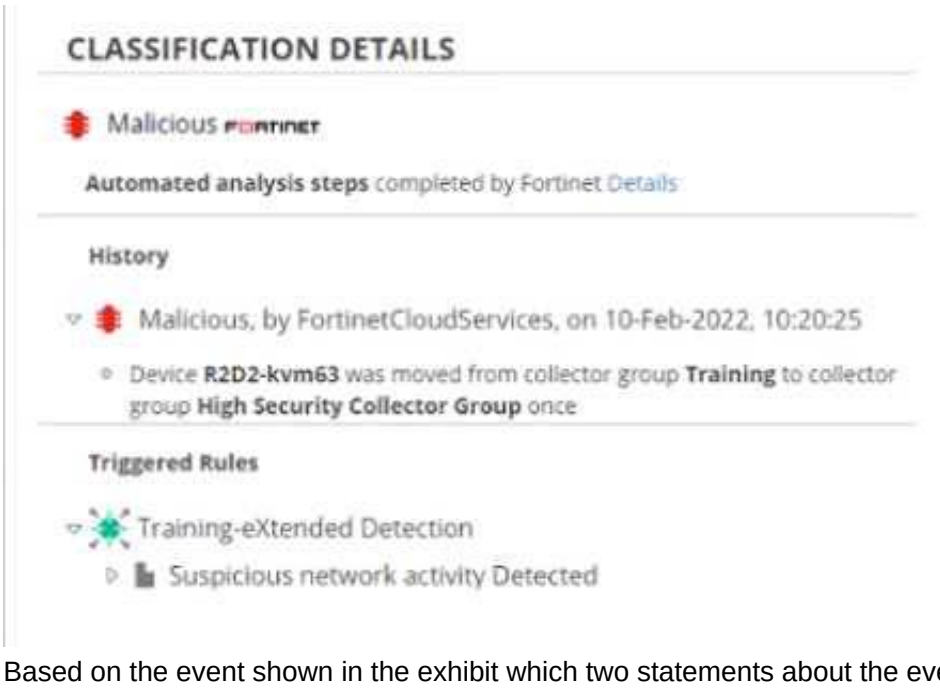
Based on the event exception shown in the exhibit which two statements about the exception are true? (Choose two)

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 8
Exhibit.

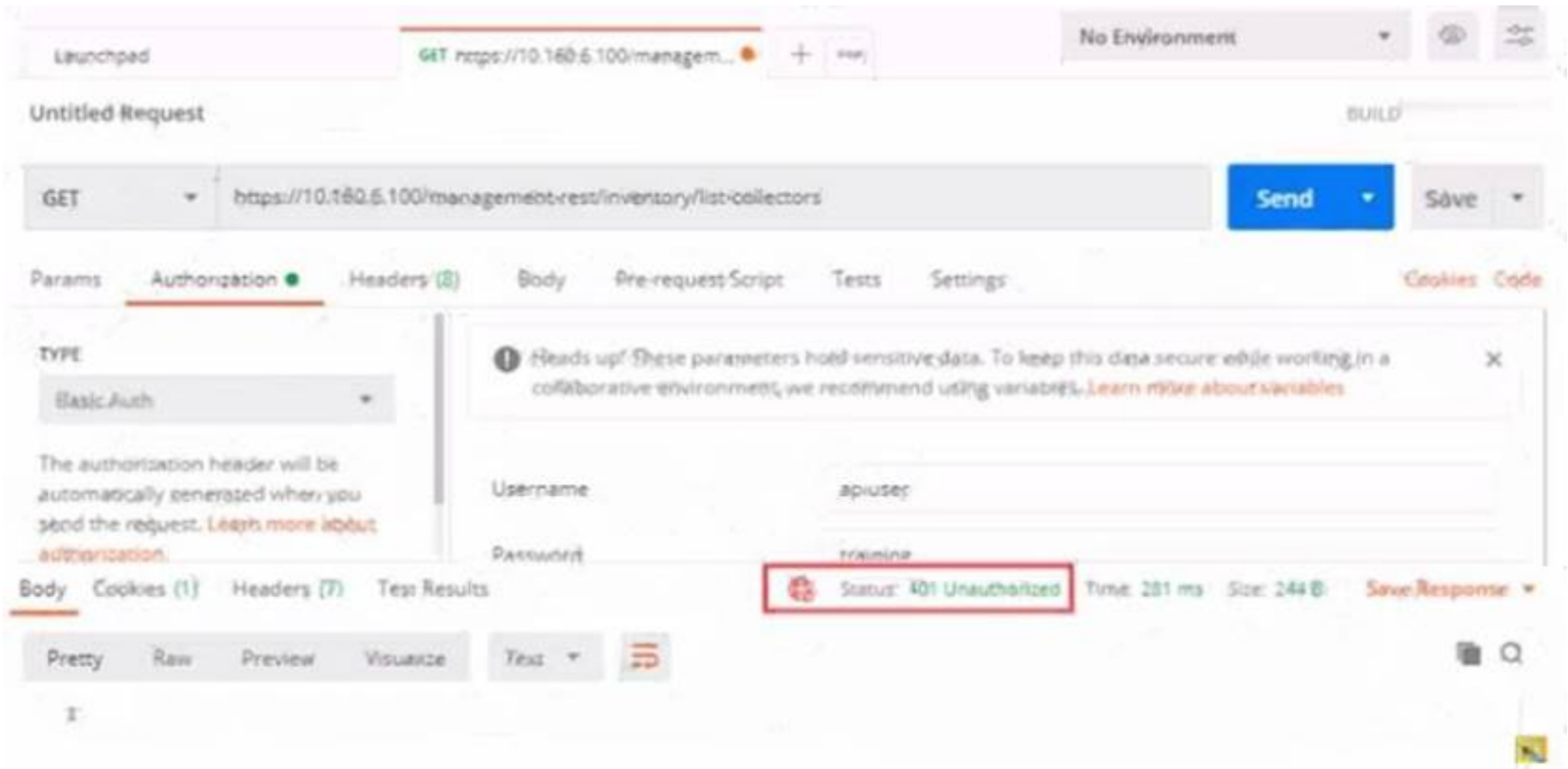


Based on the event shown in the exhibit which two statements about the event are true? (Choose two.)

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 9
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 10
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 10
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 14
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 18
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 22
Which scripting language is supported by the FortiEDR action managed?

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

Answer: A

NEW QUESTION 25
.....

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/