



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

Refer to the exhibits.

Search Collectors or Go 							
Enable/Disable  Isolate  Export  Uninstall							
DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
C8092231196	1196\Administrator	Windows Server 2016 Standard Evaluation	10.160.6.110	00-5D-56-A1-32-81.00...	4.1.0.361	 Disconnected	Today

Administrator: Command Prompt			
C:\Users\Administrator>netstat -an			
Active Connections			
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49692	0.0.0.0:0	LISTENING
TCP	10.160.6.110:139	0.0.0.0:0	LISTENING
TCP	10.160.6.110:50853	10.160.6.100:8080	SYN_SENT
TCP	172.16.9.19:139	0.0.0.0:0	LISTENING
TCP	172.16.9.19:49687	52.177.165.30:443	ESTABLISHED

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 2

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 3

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 4

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 5

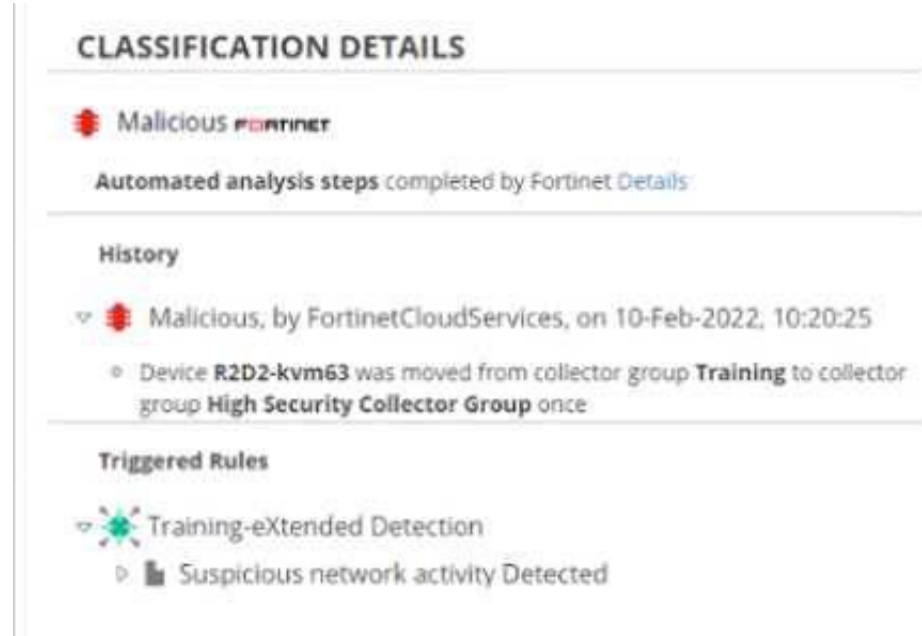
An administrator needs to restrict access to the ADMINISTRATION tab in the central manager for a specific account. What role should the administrator assign to this account?

- A. Admin
- B. User
- C. Local Admin
- D. REST API

Answer: C

NEW QUESTION 6

Exhibit.



CLASSIFICATION DETAILS

Malicious runner

Automated analysis steps completed by Fortinet Details

History

- Malicious, by FortinetCloudServices, on 10-Feb-2022, 10:20:25
 - Device **R2D2-kvm63** was moved from collector group **Training** to collector group **High Security Collector Group** once

Triggered Rules

- Training-eXtended Detection
 - Suspicious network activity Detected

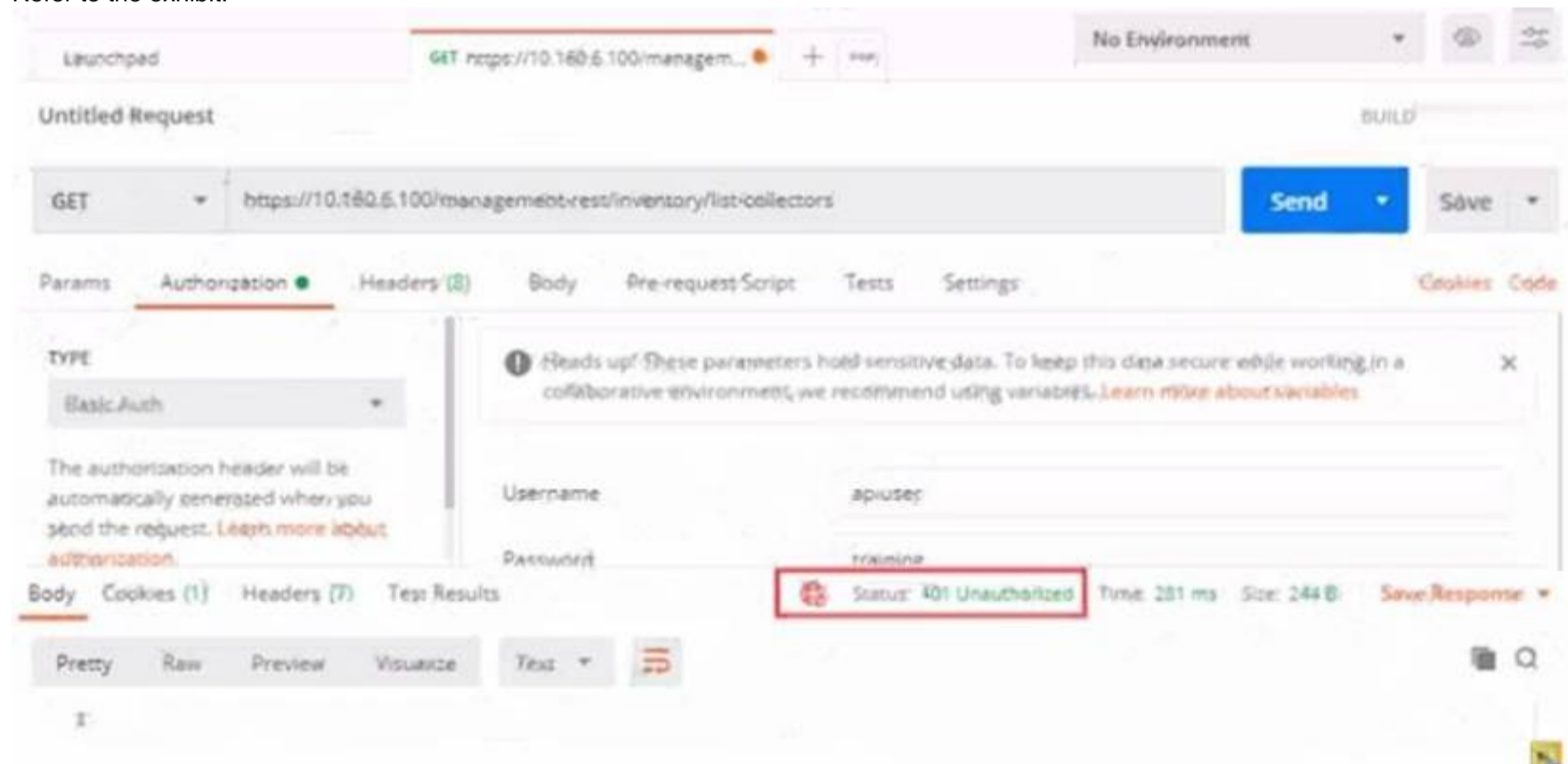
Based on the event shown in the exhibit which two statements about the event are true? (Choose two.)

- 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 7

Refer to the exhibit.



Launched GET https://10.160.5.100/management... No Environment

Untitled Request BUILD

GET https://10.160.5.100/management/rest/inventory/list-collectors Send Save

Params Authorization Headers (8) Body Pre-request Script Tests Settings Cookies Code

Authorization

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. [Learn more about authorization.](#)

Username: apiuser Password: training

Status: 401 Unauthorized Time: 281 ms Size: 244 B Save Response

Pretty Raw Preview Visualize Text

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 8

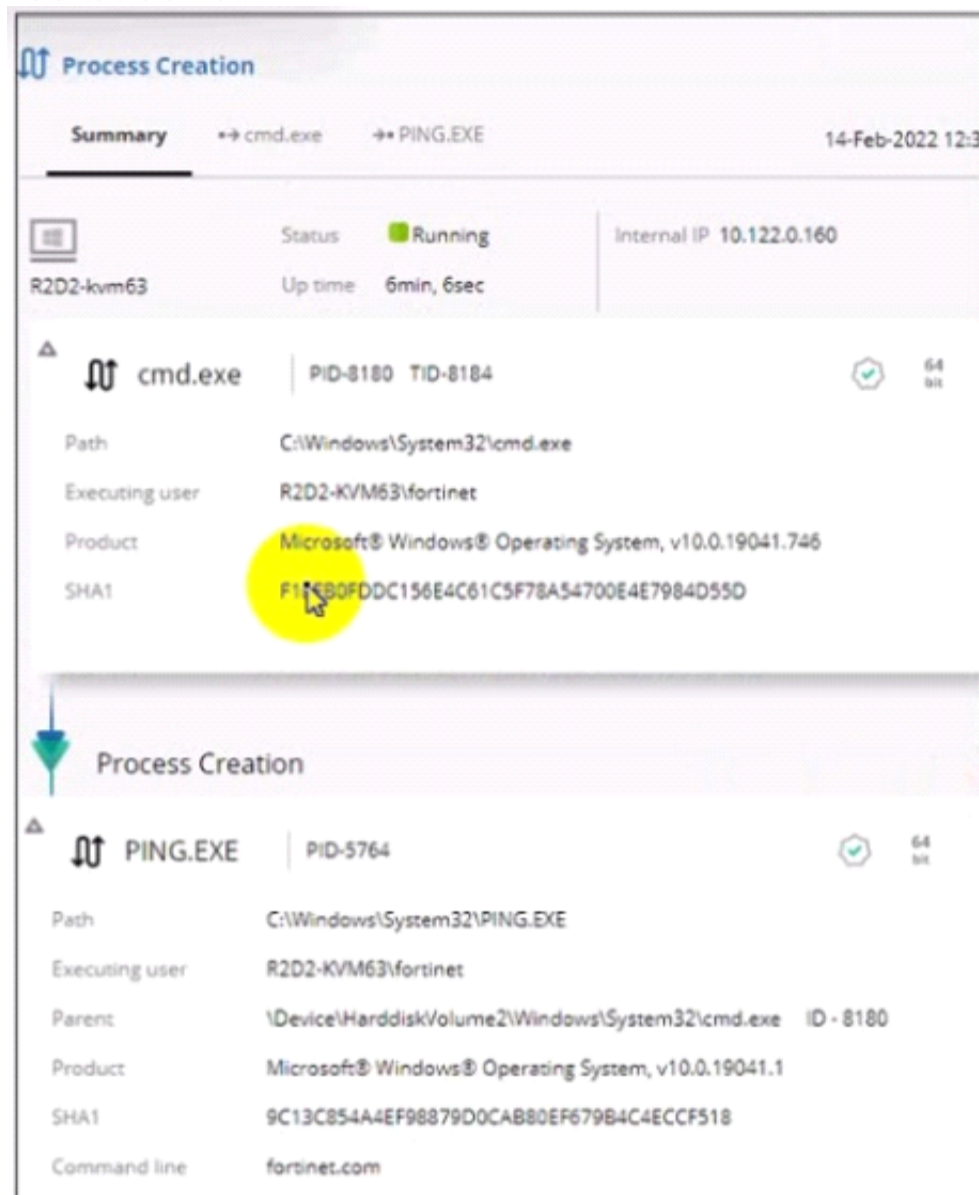
The FortiEDR axe classified an event as inconclusive, out a few seconds later FCS revised the classification to malicious. What playbook actions ate applied to the event?

- 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 9

Refer to the exhibit.



Process Creation Summary
 Summary → cmd.exe → PING.EXE 14-Feb-2022 12:30
 R2D2-kvm63 Status: Running Internal IP: 10.122.0.160
 Up time: 6min, 6sec

cmd.exe | PID-8180 TID-8184 64 bit
 Path: C:\Windows\System32\cmd.exe
 Executing user: R2D2-KVM63\fortinet
 Product: Microsoft® Windows® Operating System, v10.0.19041.746
 SHA1: F11C80FDDC156E4C61C5F78A54700E4E7984D55D

PING.EXE | PID-5764 64 bit
 Path: C:\Windows\System32\PING.EXE
 Executing user: R2D2-KVM63\fortinet
 Parent: \Device\HarddiskVolume2\Windows\System32\cmd.exe ID - 8180
 Product: Microsoft® Windows® Operating System, v10.0.19041.1
 SHA1: 9C13C854A4EF98879D0CAB80EF679B4C4ECCF518
 Command line: fortinet.com

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

Which threat hunting profile is the most resource intensive?

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

Answer: A

NEW QUESTION 10

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 15

What is the benefit of using file hash along with the file name in a threat hunting repository search?

- A. It helps to make sure the hash is really a malware
- B. It helps to check the malware even if the malware variant uses a different file name
- C. It helps to find if some instances of the hash are actually associated with a different file
- D. It helps locate a file as threat hunting only allows hash search

Answer: C

NEW QUESTION 17

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 20

.....

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/>