Fortinet

Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

NEW QUESTION 1
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

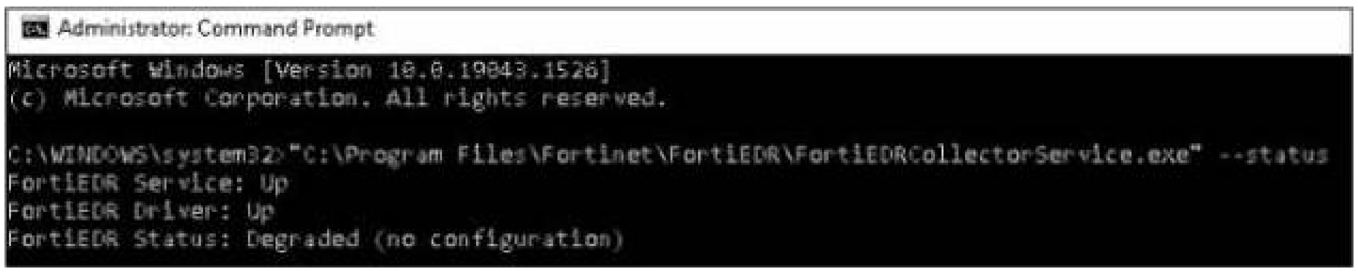
Answer: AD

NEW QUESTION 2
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 3
Refer to the exhibit.



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.19043.1526]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>"C:\Program Files\Fortinet\FortiEDR\FortiEDRCollectorService.exe" --status
FortiEDR Service: Up
FortiEDR Driver: Up
FortiEDR Status: Degraded (no configuration)
```

Based on the FortiEDR status output shown in the exhibit, which two statements about the FortiEDR collector are true? (Choose two.)

A. The collector device has windows firewall enabled
B. The collector has been installed with an incorrect port number
C. The collector has been installed with an incorrect registration password
D. The collector device cannot reach the central manager

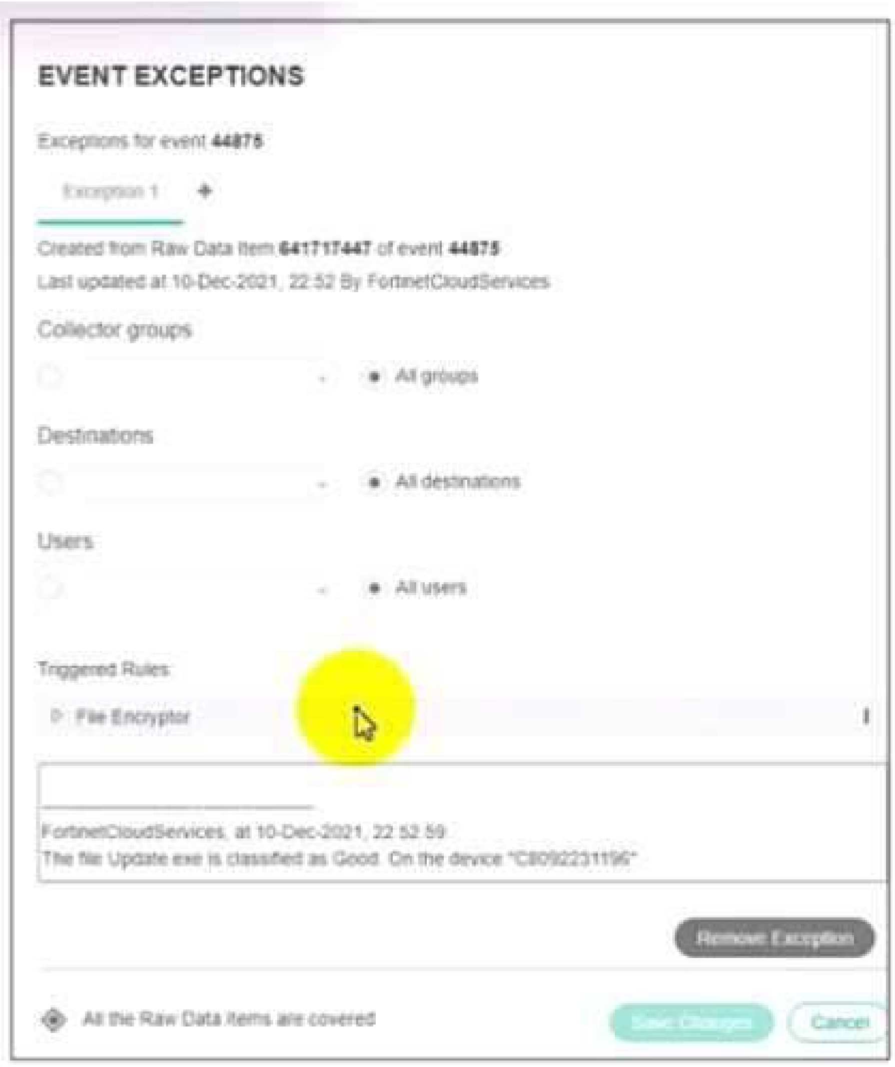
Answer: BD

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
Refer to the exhibit.



EVENT EXCEPTIONS

Exceptions for event **44875**

Exception 1

Created from Raw Data Item **641717447** of event **44875**
Last updated at 10-Dec-2021, 22:52 By FortinetCloudServices

Collector groups
○ ● All groups

Destinations
○ ● All destinations

Users
○ ● All users

Triggered Rules
File Encryptor

FortinetCloudServices, at 10-Dec-2021, 22:52:59
The file Update.exe is classified as Good. On the device "C8092231196"

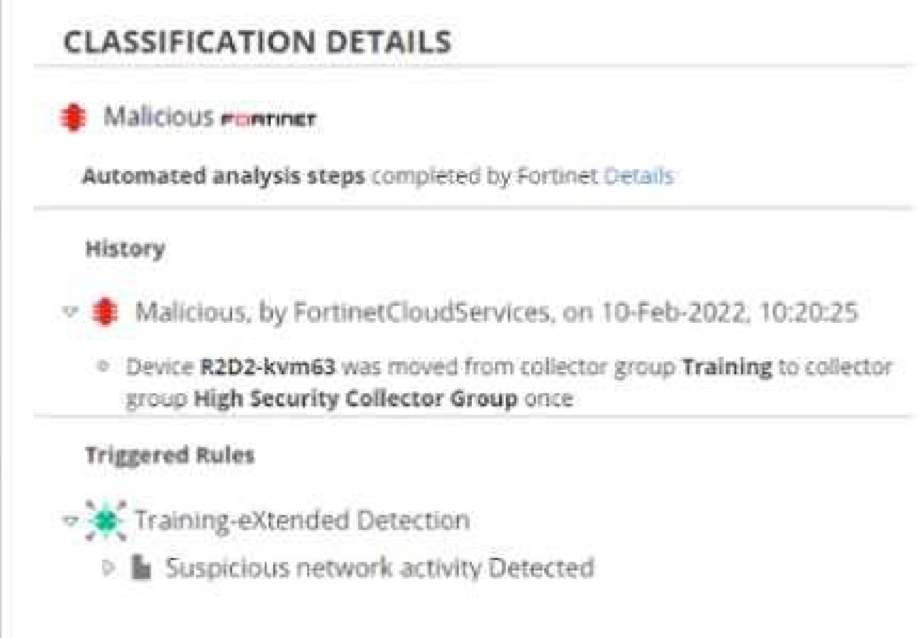
All the Raw Data items are covered

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 6
Exhibit.



CLASSIFICATION DETAILS

Malicious FORTINET

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

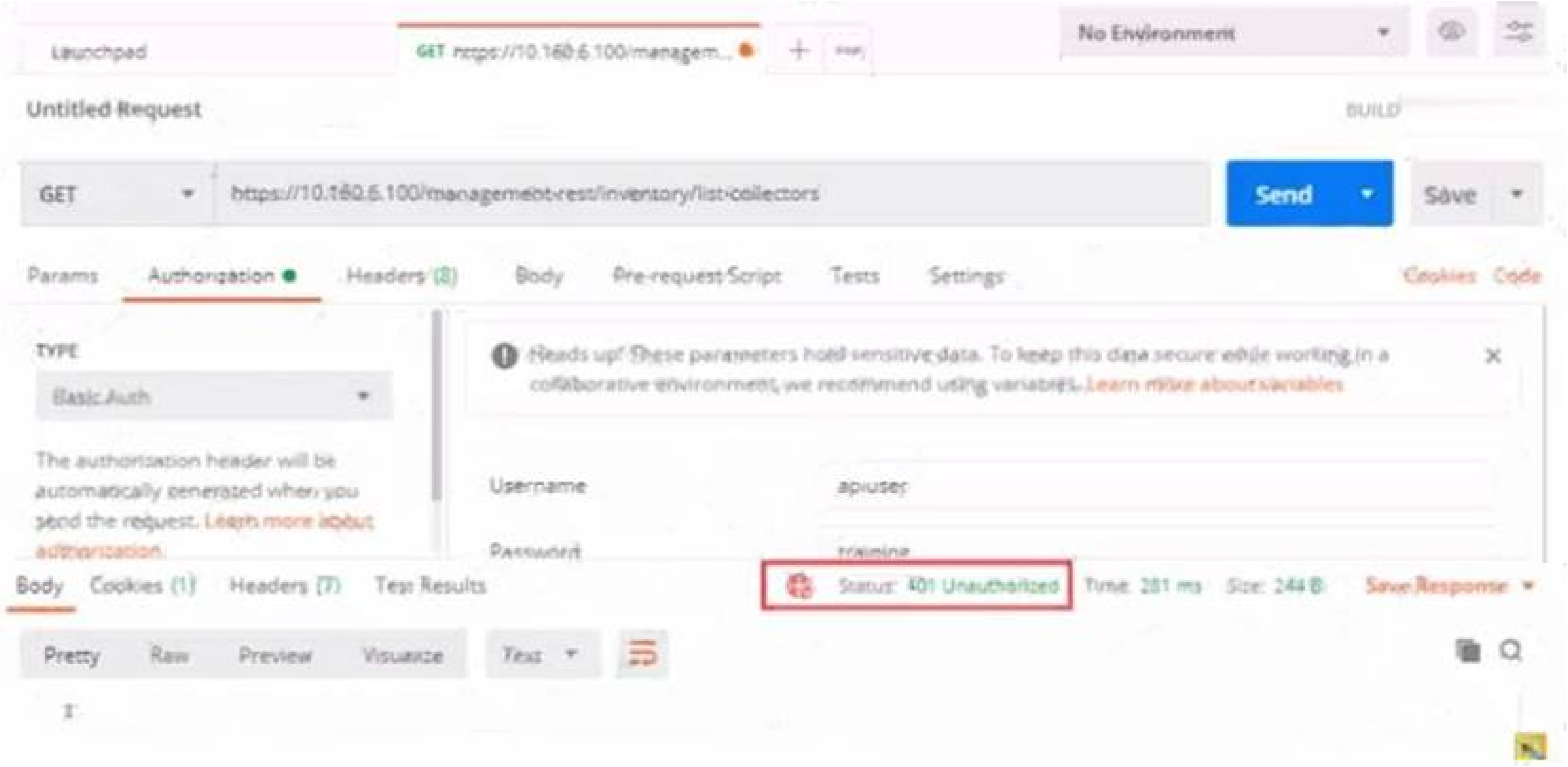
Suspicious network activity Detected

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.



Untitled Request

GET https://10.160.6.100/management-rest/inventory/list-collectors

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables

Username: apiuser

Password: training

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

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
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

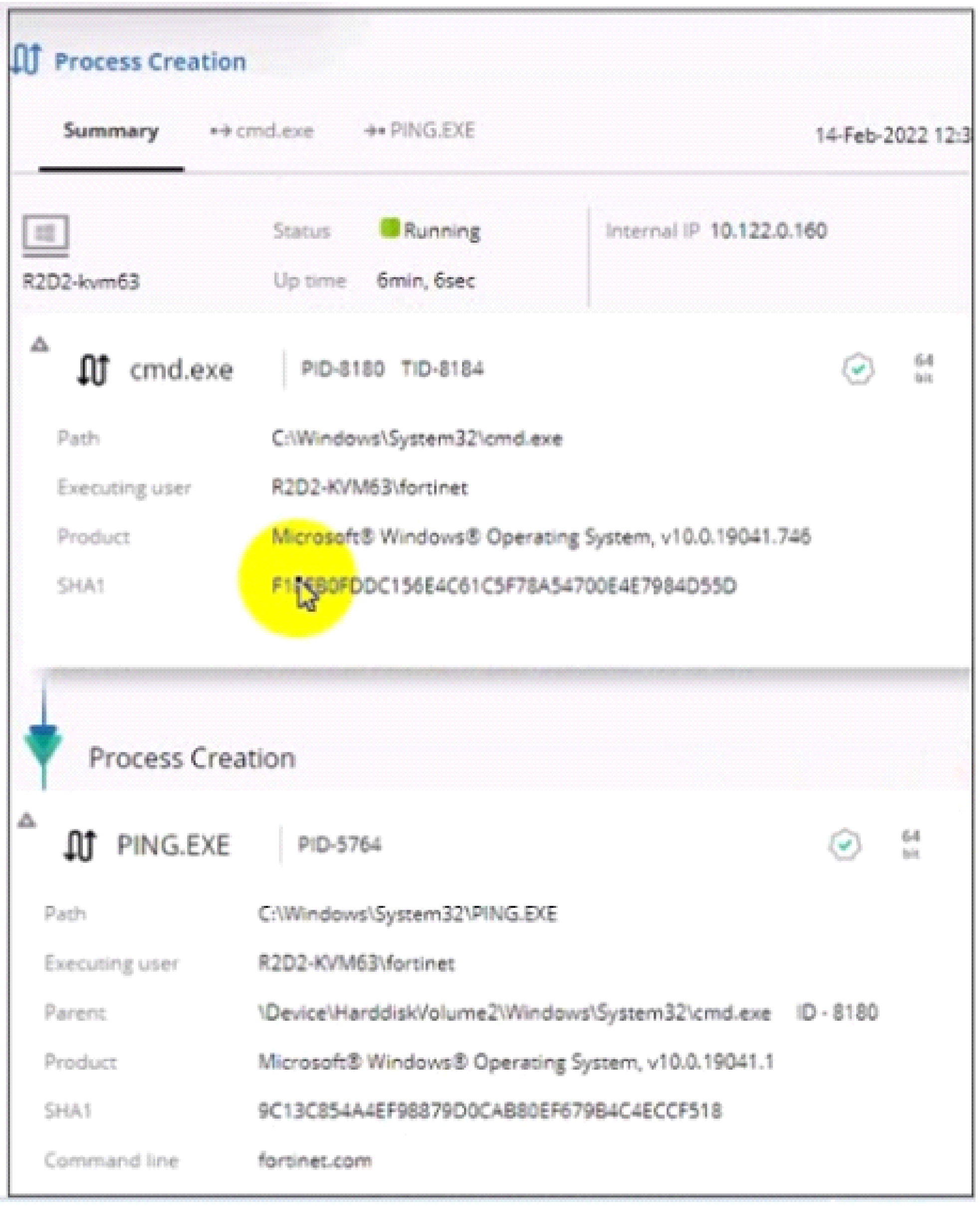
Answer: C

NEW QUESTION 9
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
Refer to the exhibit.



Process Creation

Summary ↔ cmd.exe → PING.EXE 14-Feb-2022 12:3

R2D2-kvm63
Status 🟩 Running
Up time 6min, 6sec
Internal IP 10.122.0.160

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 F1[illegible]B0FDDC156E4C61C5F78A54700E4E7984D55D

Process Creation

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 11
......