Fortinet

Exam Questions NSE5_EDR-5.0

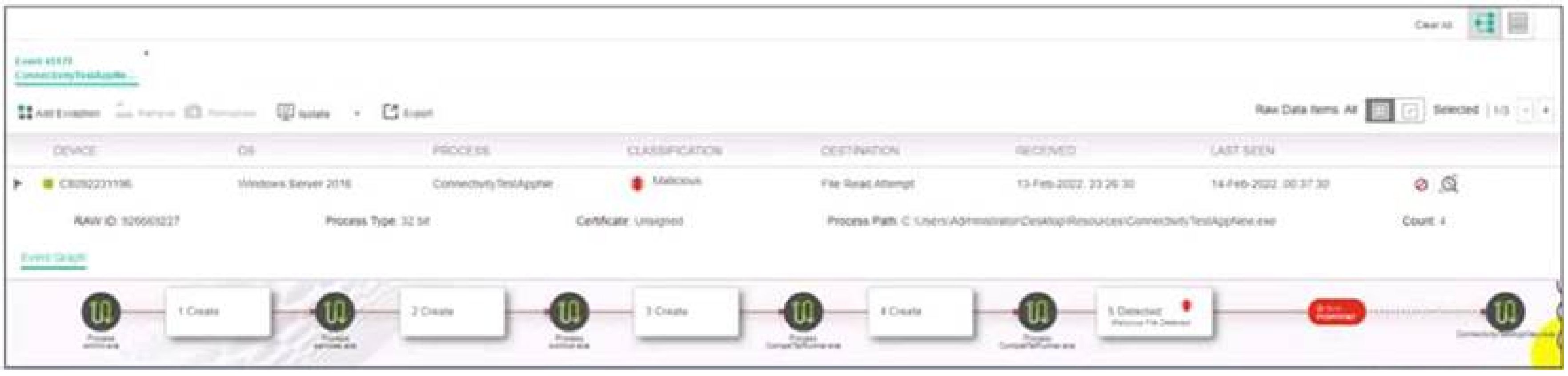
Fortinet NSE 5 - FortiEDR 5.0

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
Exhibit.



DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
C8092231196	Windows Server 2016	ConnectivityTestAppNe	Malicious	File Read Attempt	13-Feb-2022, 23:26:30	14-Feb-2022, 00:37:30

RAW ID: 926603227 Process Type: 32 bit Certificate: Unsigned Process Path: C:\Users\Administrator\Desktop\Resources\ConnectivityTestAppNew.exe Count: 4

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.

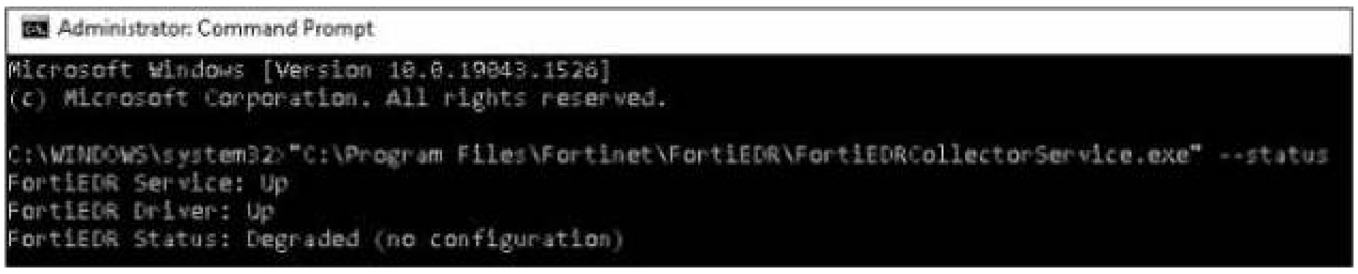
Answer: BC

NEW QUESTION 3
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 4
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

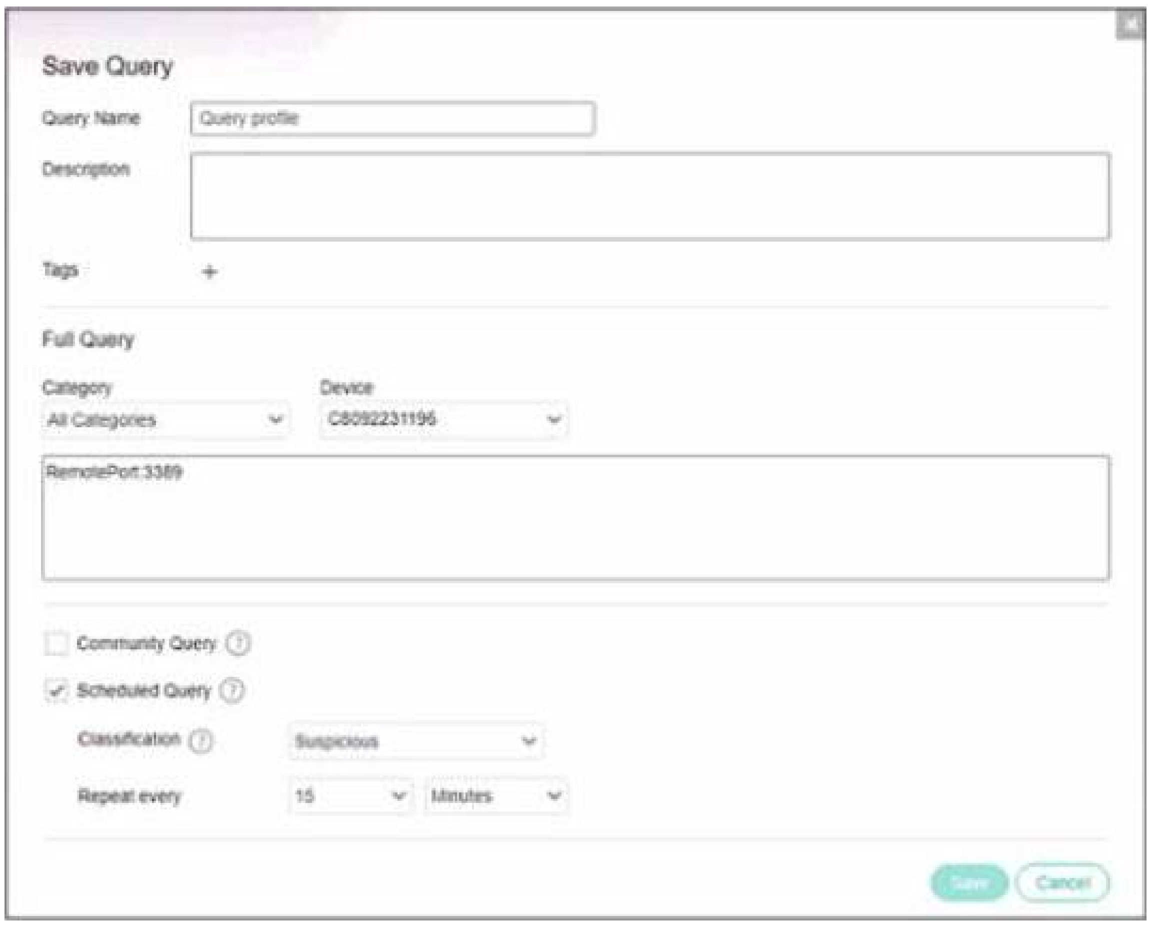
Answer: BD

NEW QUESTION 5
An administrator needs to restrict access to the ADMINISTRATION tab inthe 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
Refer to the exhibit.



Save Query

Query Name: Query profile

Description:

Tags +

Full Query

Category: All Categories

Device: C8092231196

RemotePort:3389

☐ Community Query

☑ Scheduled Query

Classification: Suspicious

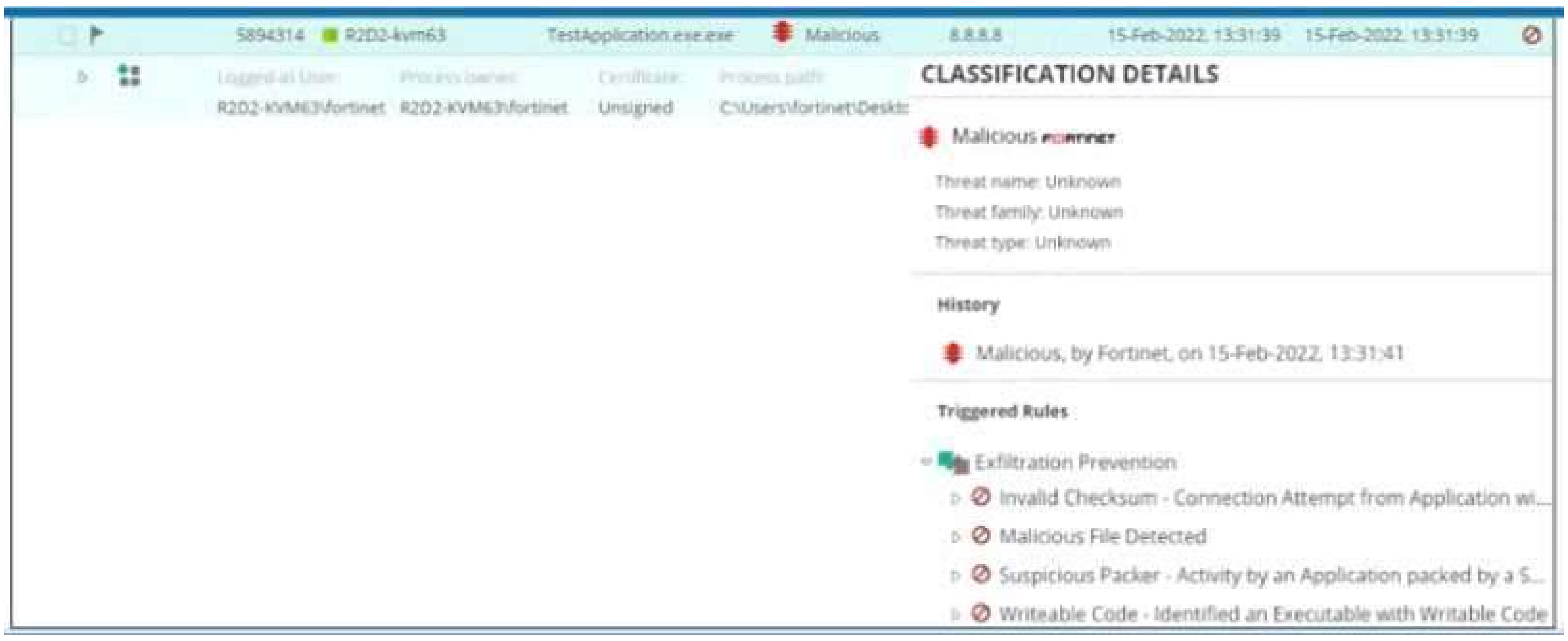
Repeat every: 15 Minutes

Based on the threat hunting query shown in the exhibit which of the following is true?

A. RDP connections will be blocked and classified as suspicious
B. A security event will be triggered when the device attempts a RDP connection
C. This query is included in other organizations
D. The query will only check for network category

Answer: B

NEW QUESTION 7
Refer to the exhibit.



5894314 R2D2-kvm63 TestApplication.exe.exe Malicious 8.8.8.8 15-Feb-2022, 13:31:39 15-Feb-2022, 13:31:39

Logged in User:	Process owner:	Certificate:	Process path:
R2D2-KVM63\fortinet	R2D2-KVM63\fortinet	Unsigned	C:\Users\fortinet\Deskt

CLASSIFICATION DETAILS

Malicious FORTINET

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Malicious, by Fortinet, on 15-Feb-2022, 13:31:41

Triggered Rules

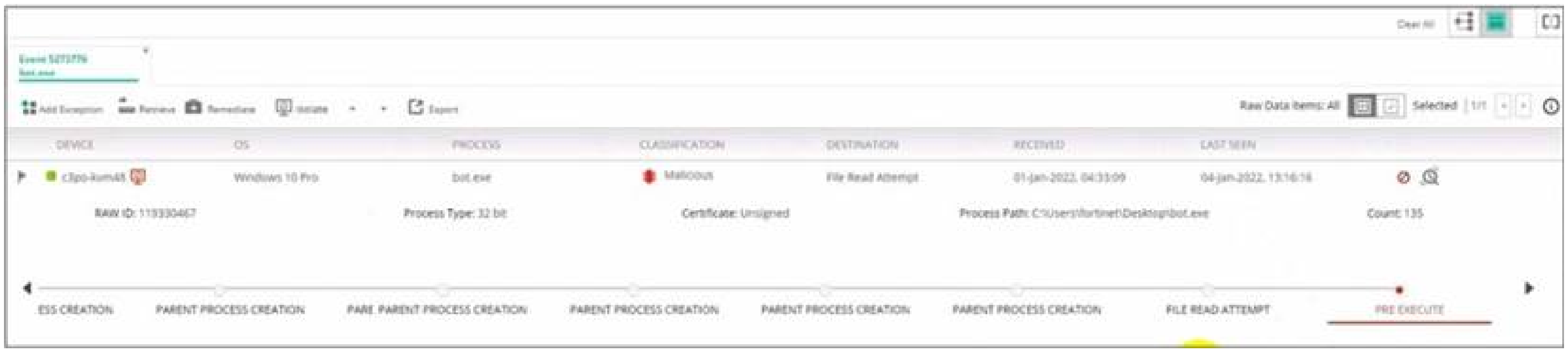
Exfiltration Prevention
- Invalid Checksum - Connection Attempt from Application wi...
- Malicious File Detected
- Suspicious Packer - Activity by an Application packed by a S...
- Writeable Code - Identified an Executable with Writable Code

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

A. The NGAV policy has blocked TestApplication exe
B. TestApplication exe is sophisticated malware
C. The user was able to launch TestApplication exe
D. FCS classified the event as malicious

Answer: AB

NEW QUESTION 8
Exhibit.



DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
c3po-kvm48	Windows 10 Pro	bot.exe	Malicious	File Read Attempt	01-Jan-2022, 04:33:09	04-Jan-2022, 13:16:16

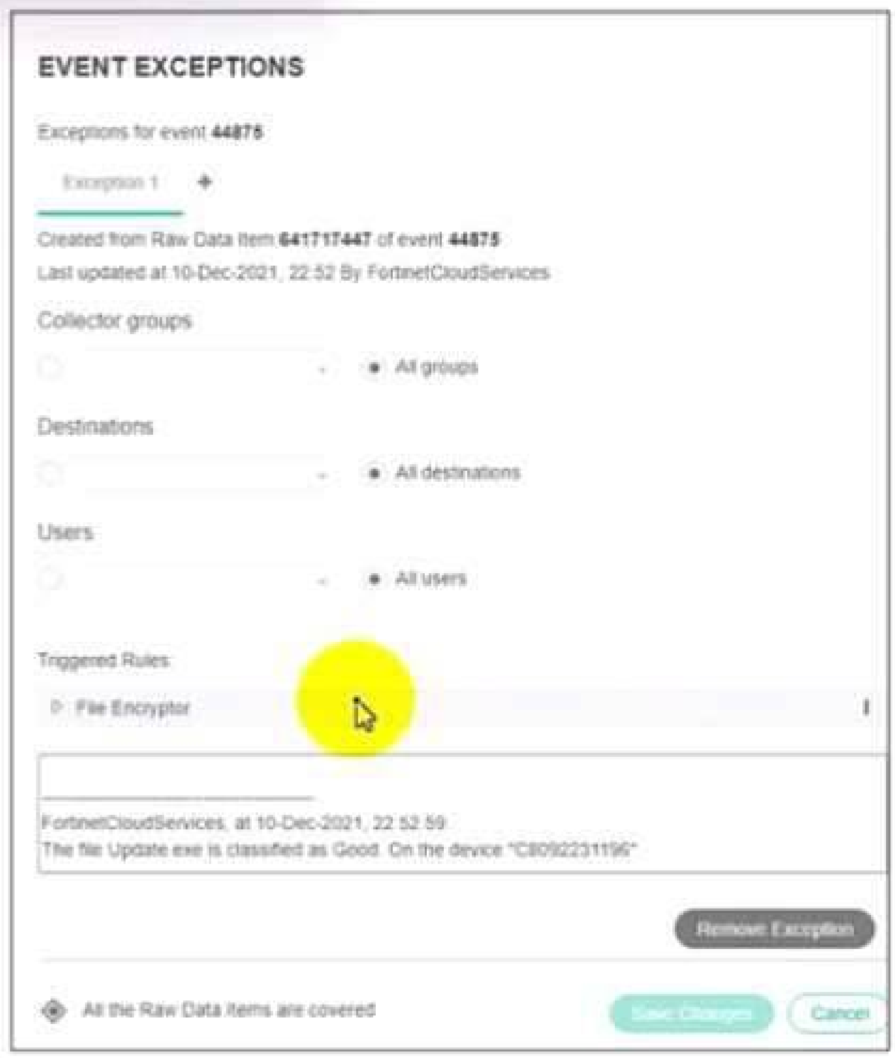
RAW ID: 119330467 Process Type: 32 bit Certificate: Unsigned Process Path: C:\Users\fortinet\Desktop\bot.exe Count: 135

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 9
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 10
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

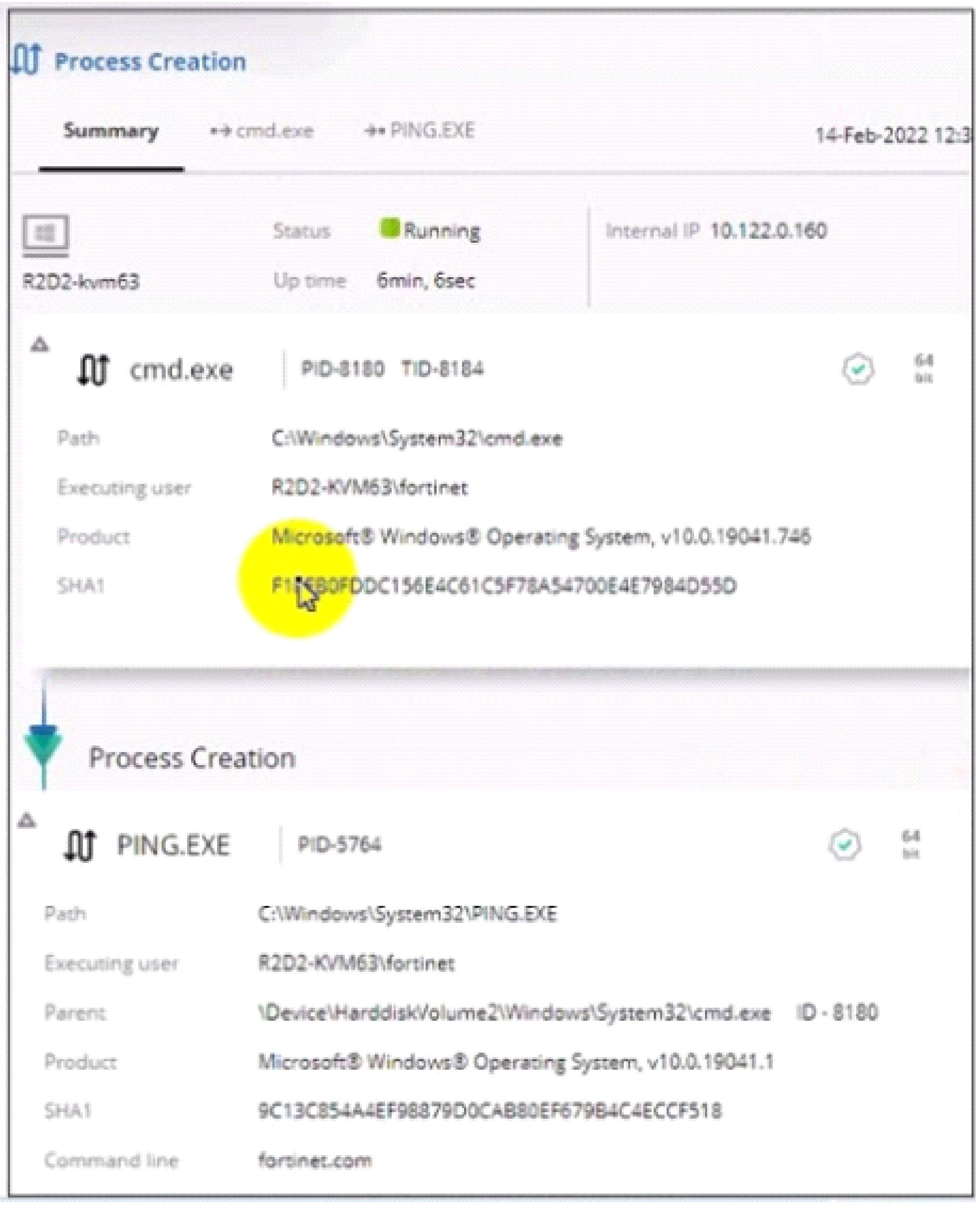
Answer: D

NEW QUESTION 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 12
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

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

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 15
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 19
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE5_EDR-5.0 Practice Exam Features:

* NSE5_EDR-5.0 Questions and Answers Updated Frequently

* NSE5_EDR-5.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_EDR-5.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_EDR-5.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The NSE5_EDR-5.0 Practice Test Here