Fortinet.NSE5_EDR-5.0.by.Tomy.35q

Number: NSE5_EDR-5.0
Passing Score: 800
Time Limit: 120
File Version: 2.0

Exam Code: NSE5_EDR-5.0

Exam A

QUESTION 1

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

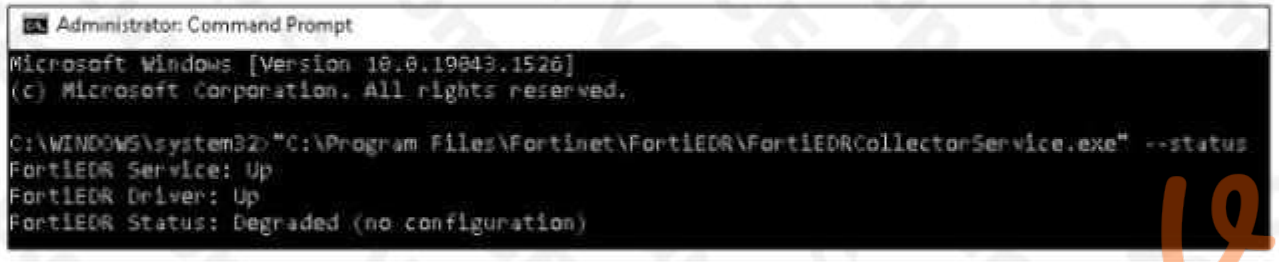
D. FCS is responsible for all classifications

Correct Answer: C

Section:

QUESTION 2

Refer to the exhibit.



```
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

Correct Answer: B, D

Section:

QUESTION 3

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

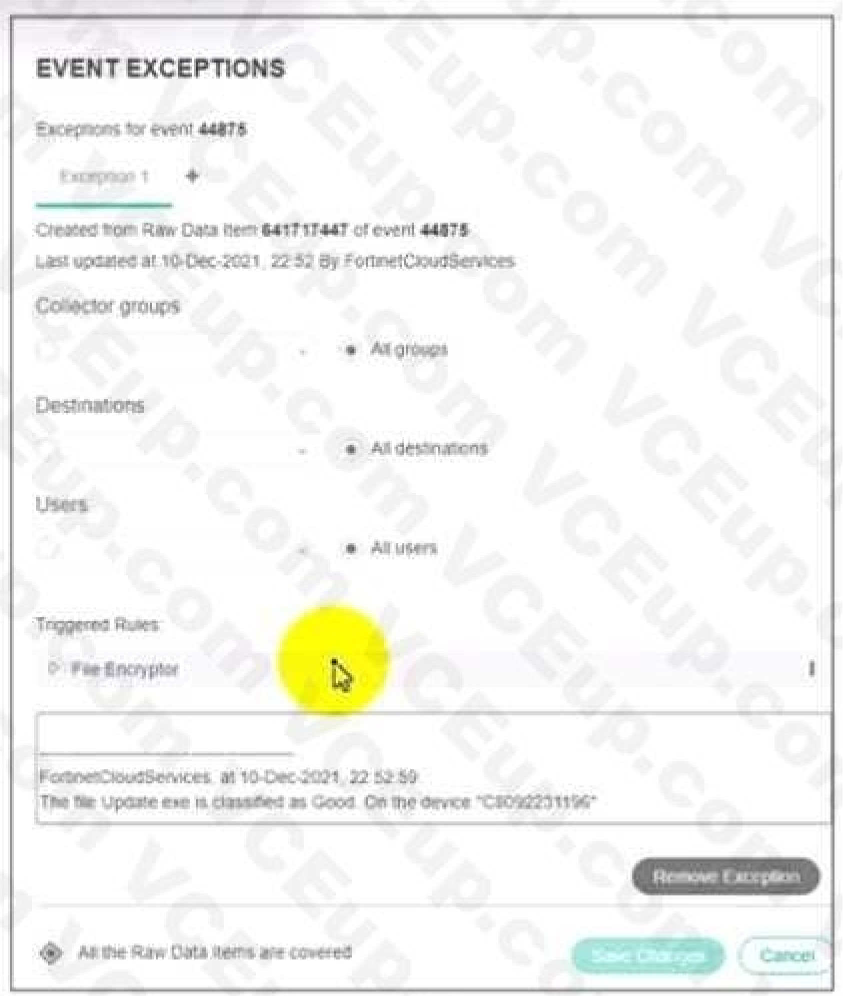
D. An administrator creates a new communication control policy for each organization

Correct Answer: C

Section:

QUESTION 4

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"

Remove Exception

All the Raw Data items are covered

Save Changes Cancel

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

Correct Answer: A, C

Section:

QUESTION 5

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

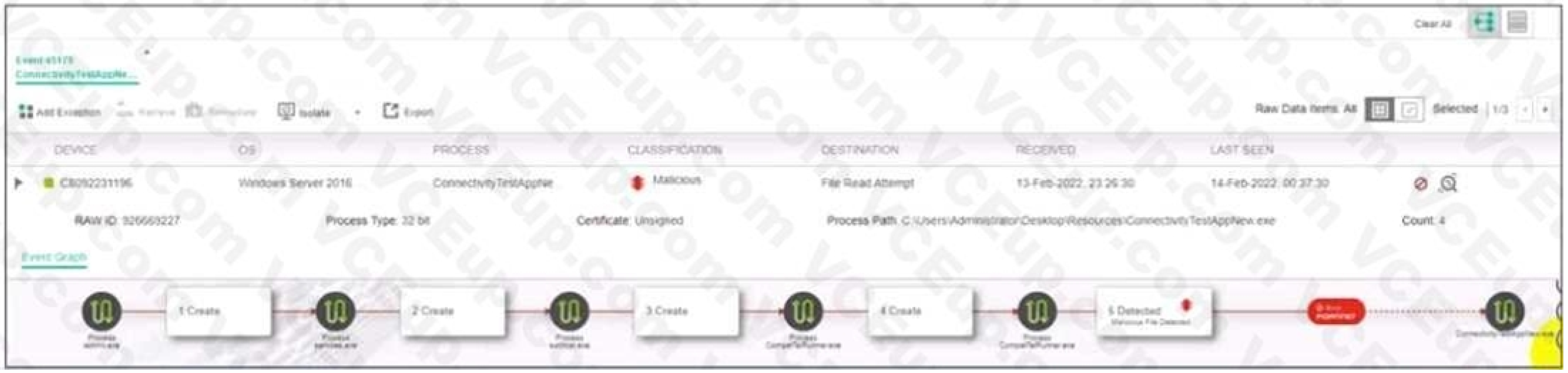
C. The file is quarantined

D. The threat hunting module deletes files from collectors that are currently online.

Correct Answer: B, C

Section:

QUESTION 6
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: 926669227 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.

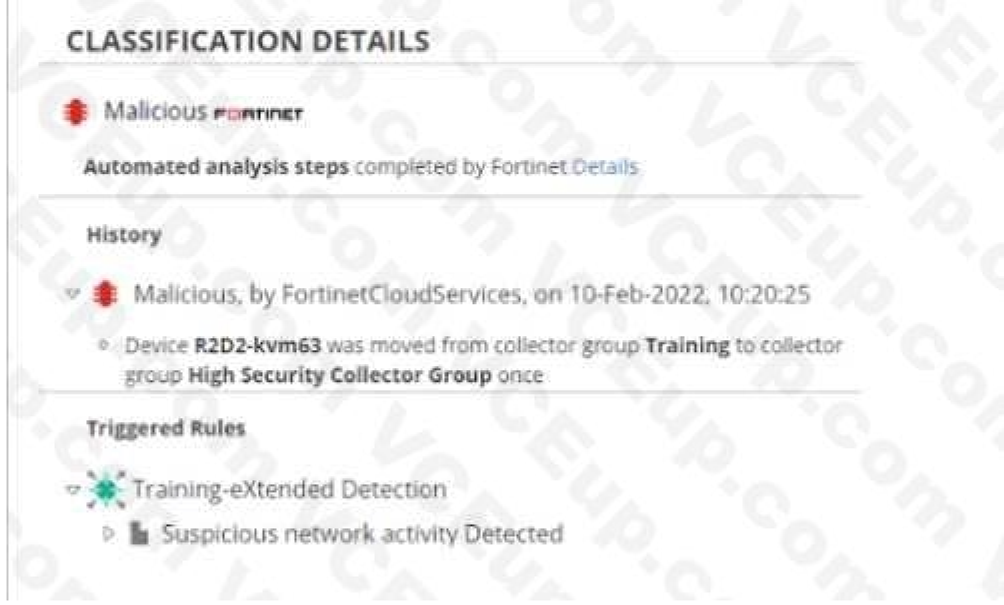
Correct Answer: B, C
Section:

QUESTION 7
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

Correct Answer: C
Section:

QUESTION 8
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

Correct Answer: B, D
Section:

QUESTION 9

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

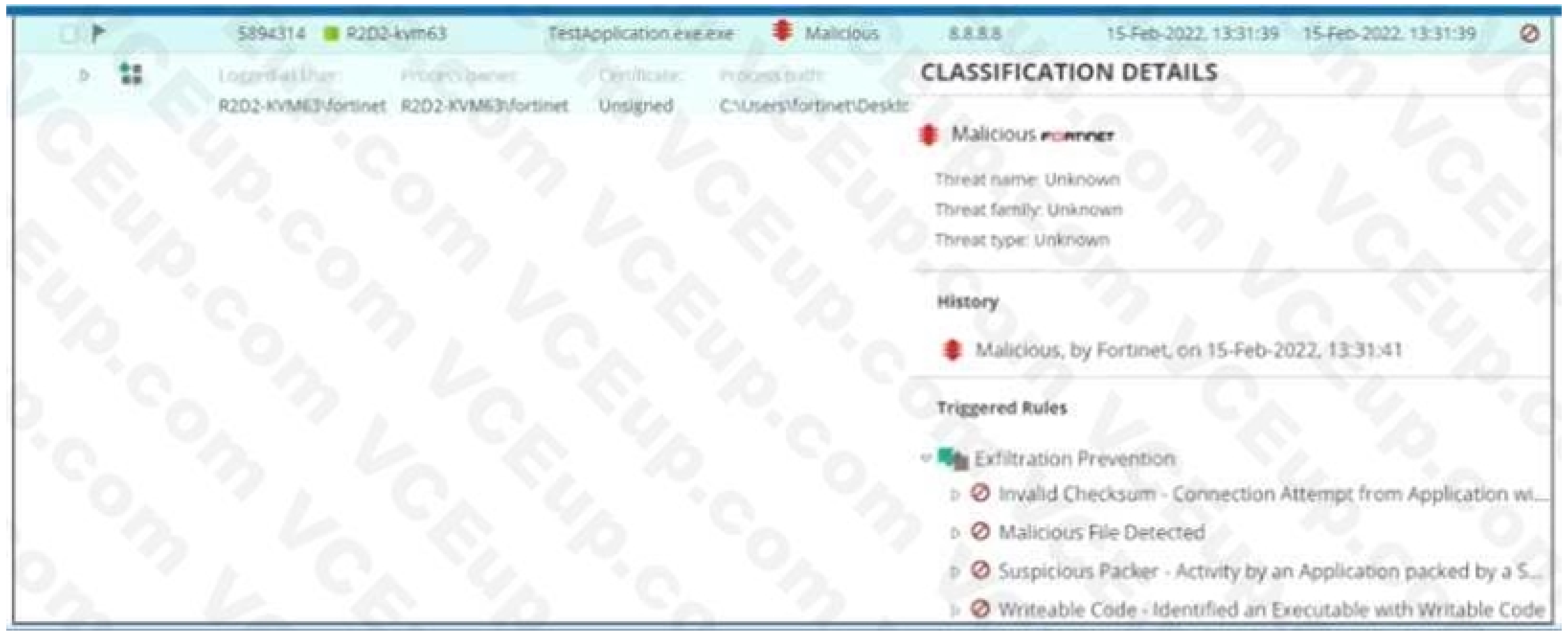
C. Local Admin

D. REST API

Correct Answer: C
Section:

QUESTION 10

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-on 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

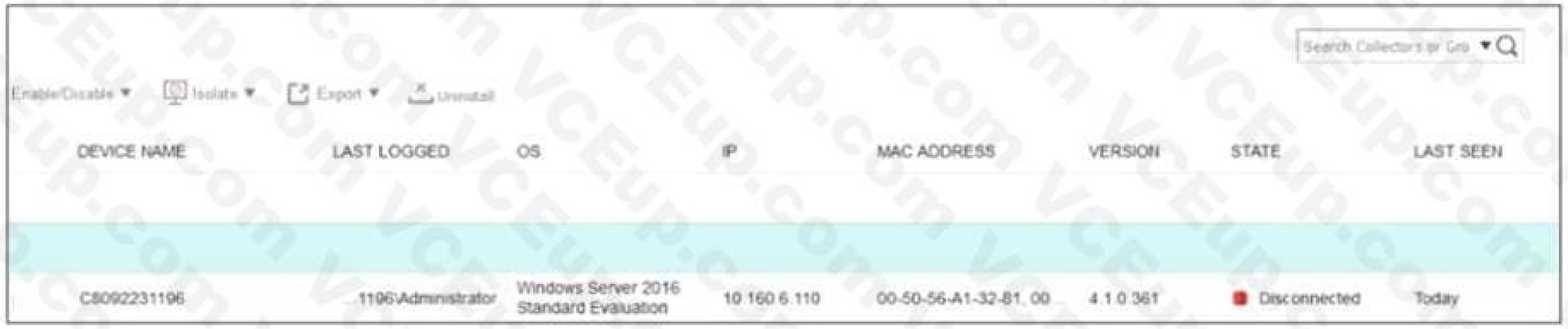
B. TestApplication exe is sophisticated malware

C. The user was able to launch TestApplication exe

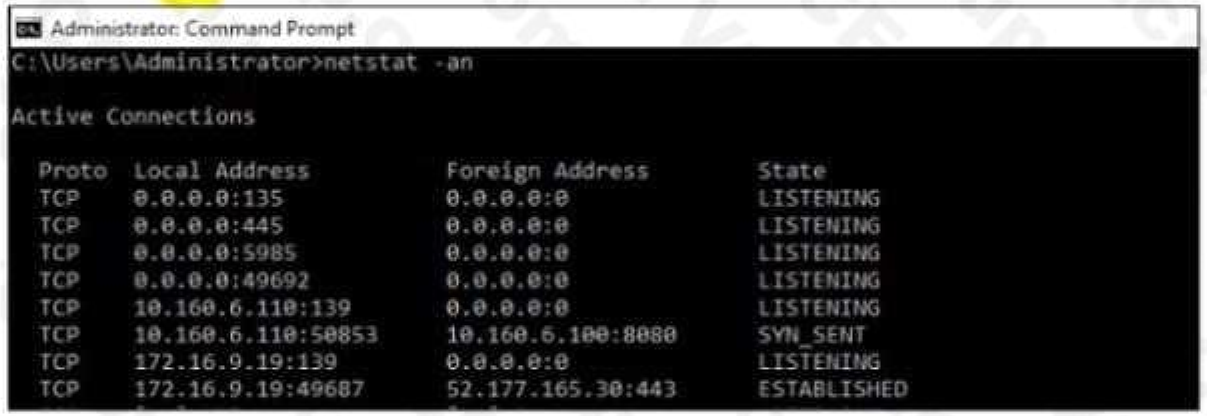
D. FCS classified the event as malicious

Correct Answer: A, B
Section:

QUESTION 11
Refer to the exhibits.



DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
C8092231196	1196\Administrator	Windows Server 2016 Standard Evaluation	10.160.6.110	00-50-56-A1-32-81, 00	4.1.0.361	🟥 Disconnected	Today



Administrator: Command Prompt

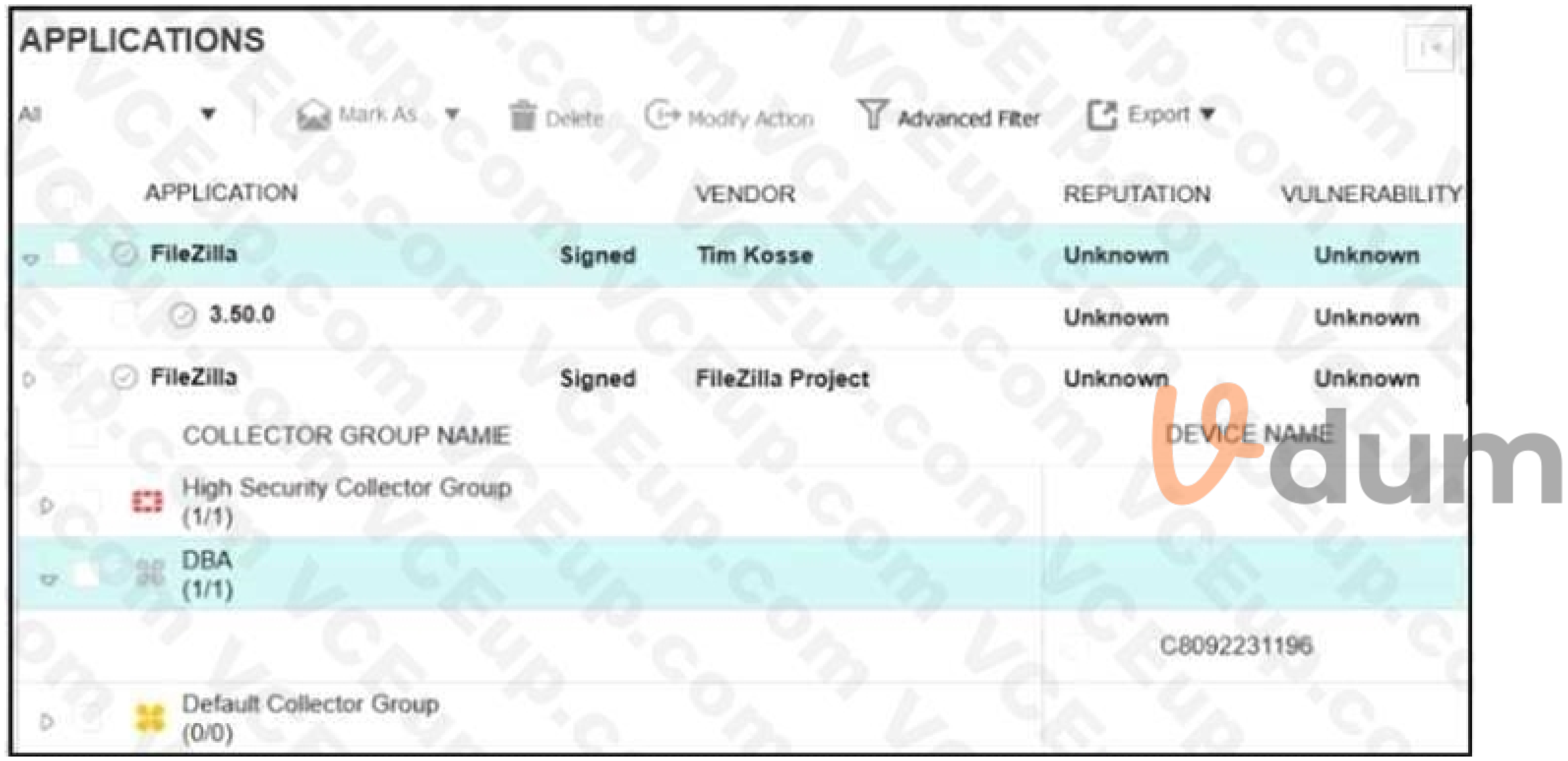
```
C:\Users\Administrator>netstat -an

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

Correct Answer: B
Section:

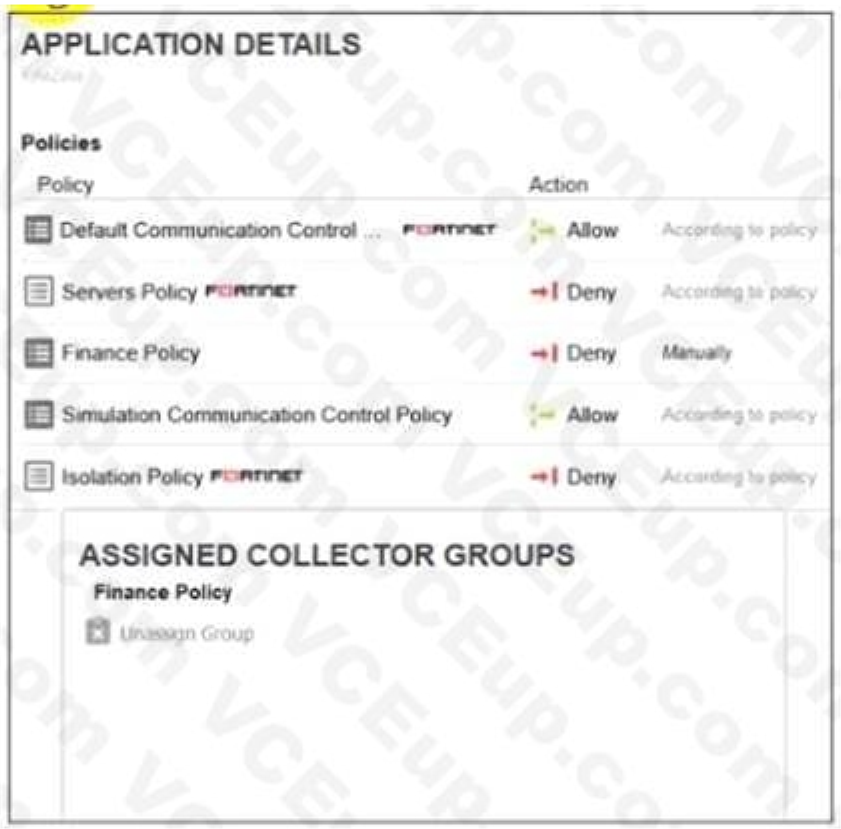
QUESTION 12
Refer to the exhibits.



APPLICATIONS

APPLICATION		VENDOR	REPUTATION	VULNERABILITY
FileZilla	Signed	Tim Kosse	Unknown	Unknown
3.50.0			Unknown	Unknown
FileZilla	Signed	FileZilla Project	Unknown	Unknown

COLLECTOR GROUP NAME	DEVICE NAME
High Security Collector Group (1/1)	
DBA (1/1)	
	C8092231196
Default Collector Group (0/0)	



APPLICATION DETAILS

Policies

Policy	Action	
Default Communication Control ... FORTINET	Allow	According to policy
Servers Policy FORTINET	Deny	According to policy
Finance Policy	Deny	Manually
Simulation Communication Control Policy	Allow	According to policy
Isolation Policy FORTINET	Deny	According to policy

ASSIGNED COLLECTOR GROUPS

Finance Policy

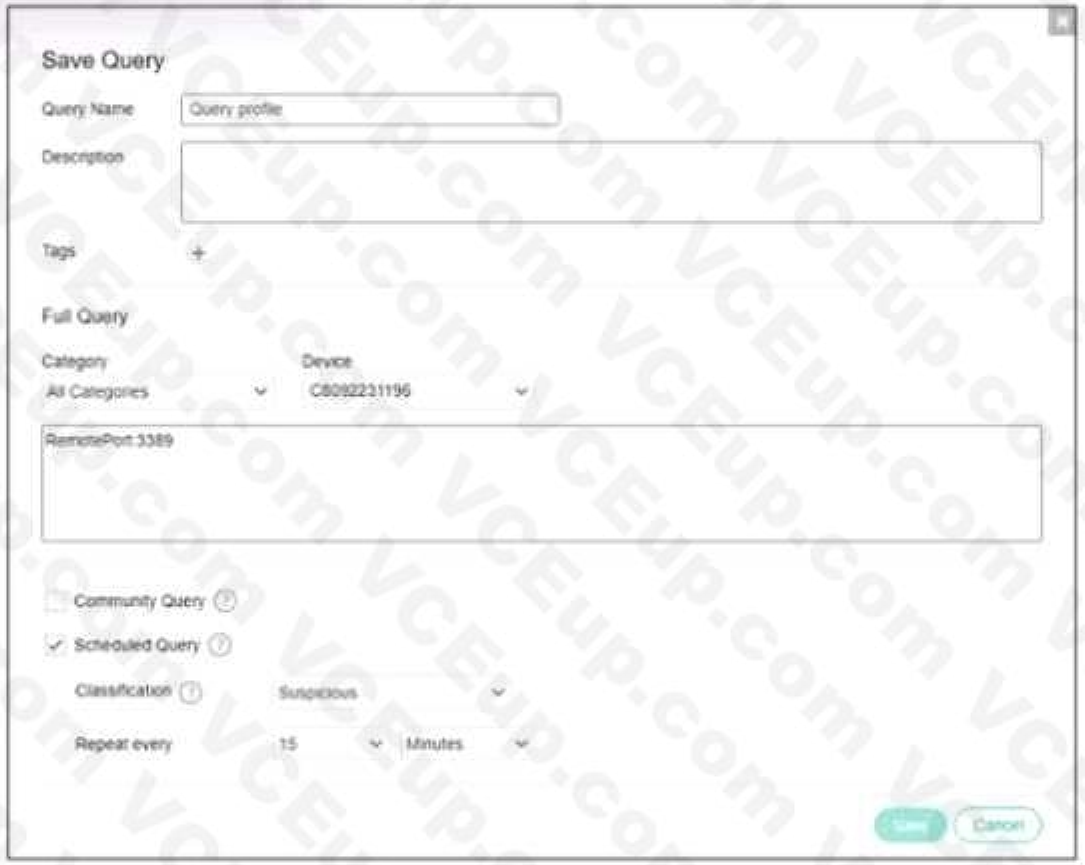
Unassign Group

The exhibits show application policy logs and application details Collector C8092231196 is a member of the Finance group What must an administrator do to block the FileZilia application?

A. Deny application in Finance policy
B. Assign Finance policy to DBA group
C. Assign Finance policy to Default Collector Group
D. Assign Simulation Communication Control Policy to DBA group

Correct Answer: D
Section:

QUESTION 13
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

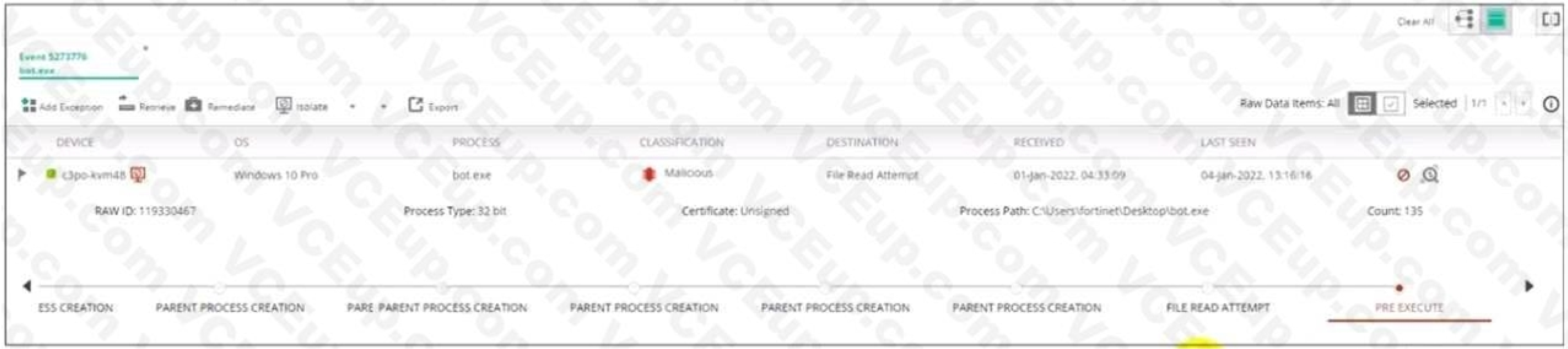
Correct Answer: B
Section:

QUESTION 14
Which connectors can you use for the FortiEDR automated incident response? (Choose two.)

A. FortiNAC
B. FortiGate
C. FortiSiem
D. FortiSandbox

Correct Answer: B, C
Section:

QUESTION 15
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

ESS CREATION — PARENT PROCESS CREATION — PARE PARENT PROCESS CREATION — PARENT PROCESS CREATION — PARENT PROCESS CREATION — PARENT PROCESS CREATION — FILE READ ATTEMPT — PRE EXECUTE

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

Correct Answer: C, D
Section:

QUESTION 16
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

Correct Answer: D
Section:

QUESTION 17
Which threat hunting profile is the most resource intensive?

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

Correct Answer: A
Section:

QUESTION 18

Which two types of remote authentication does the FortiEDR management console support? (Choose two.)

A. Radius
B. SAML
C. TACACS
D. LDAP

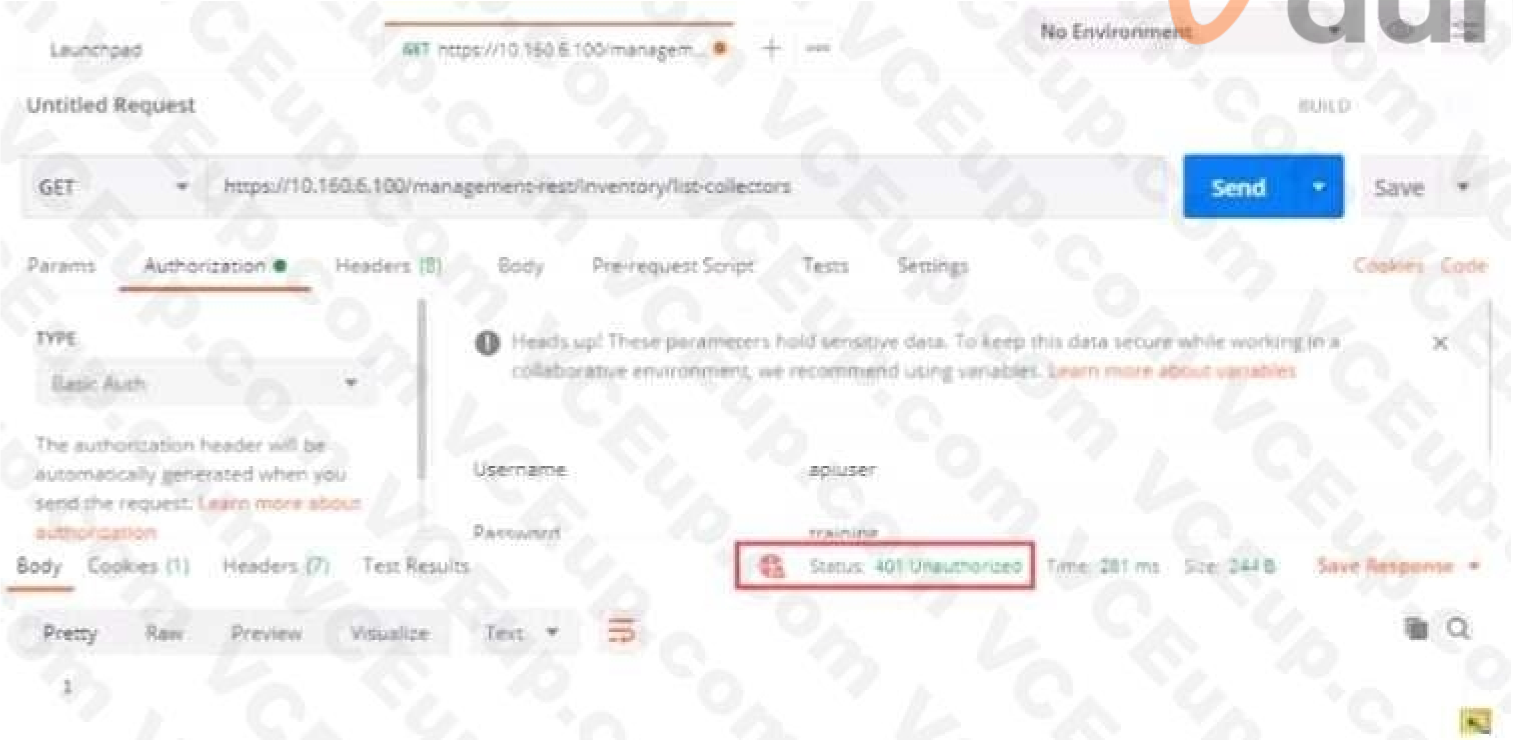
Correct Answer: A, D
Section:

QUESTION 19
FortiXDR relies on which feature as part of its automated extended response?

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

Correct Answer: B
Section:

QUESTION 20
Refer to the exhibit.



Untitled Request

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

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

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

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

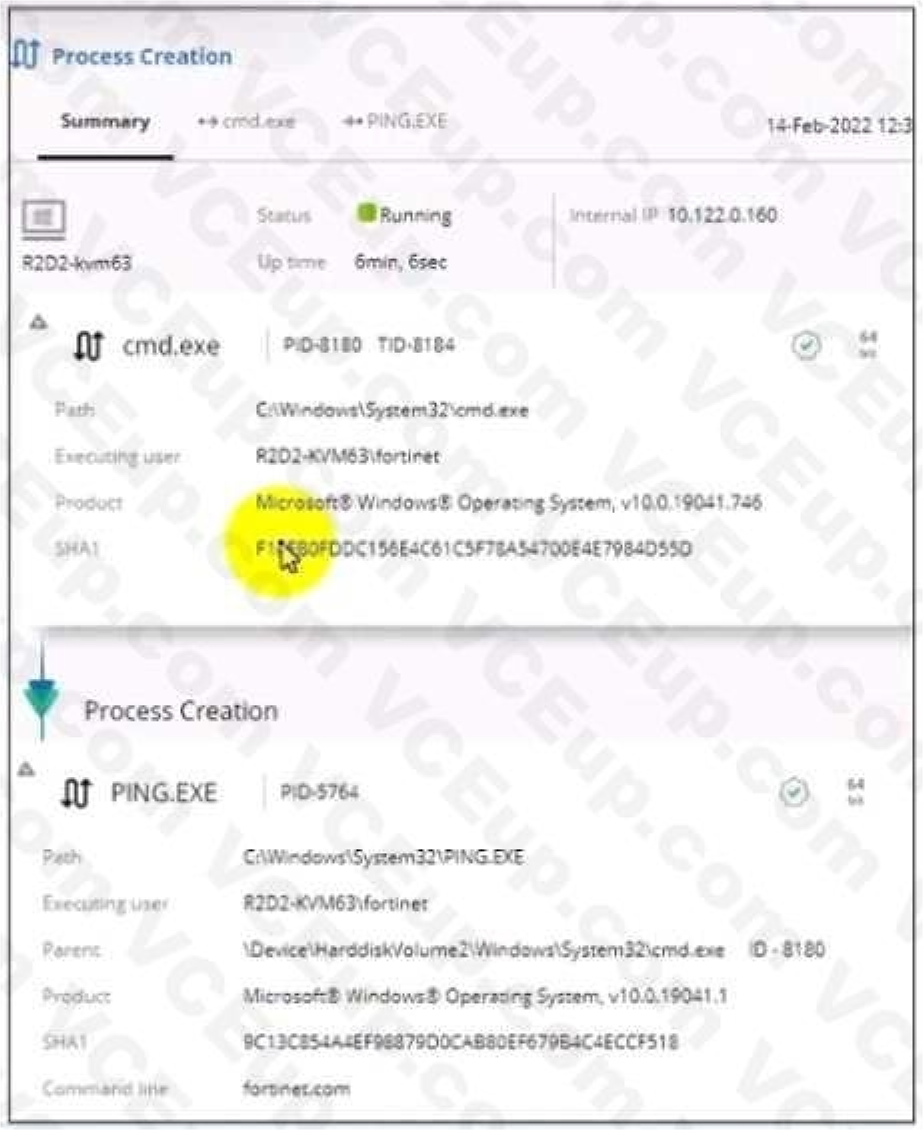
Correct Answer: A
Section:

QUESTION 21
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

Correct Answer: A
Section:

QUESTION 22
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 F1C680FDDC156E4C61C5F78A54700E4E7984D55D

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

Correct Answer: A, D
Section:

QUESTION 23
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

Correct Answer: C
Section:

QUESTION 24
Which scripting language is supported by the FortiEDR action managed?

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

Correct Answer: A
Section:

QUESTION 25
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

Correct Answer: A
Section: