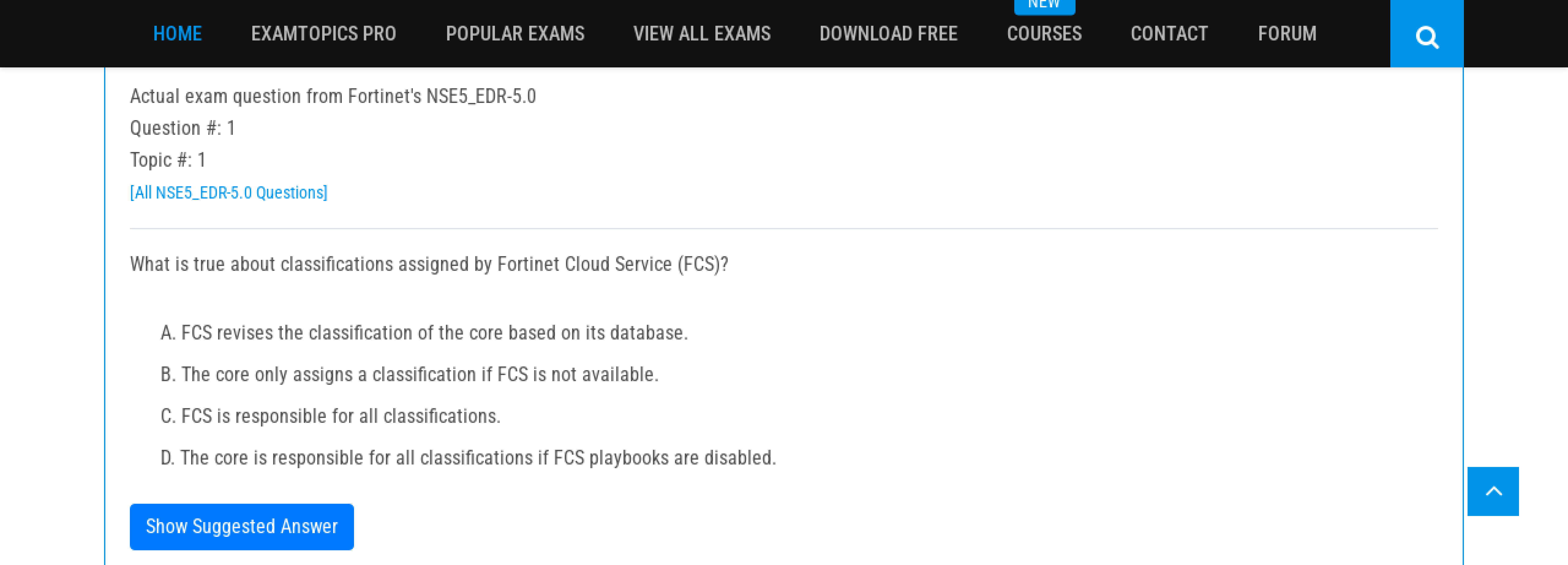


Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 1

Topic #: 1

[All NSE5_EDR-5.0 Questions]

What is true about classifications assigned by Fortinet Cloud Service (FCS)?

A. FCS revises the classification of the core based on its database.

B. The core only assigns a classification if FCS is not available.

C. FCS is responsible for all classifications.

D. The core is responsible for all classifications if FCS playbooks are disabled.

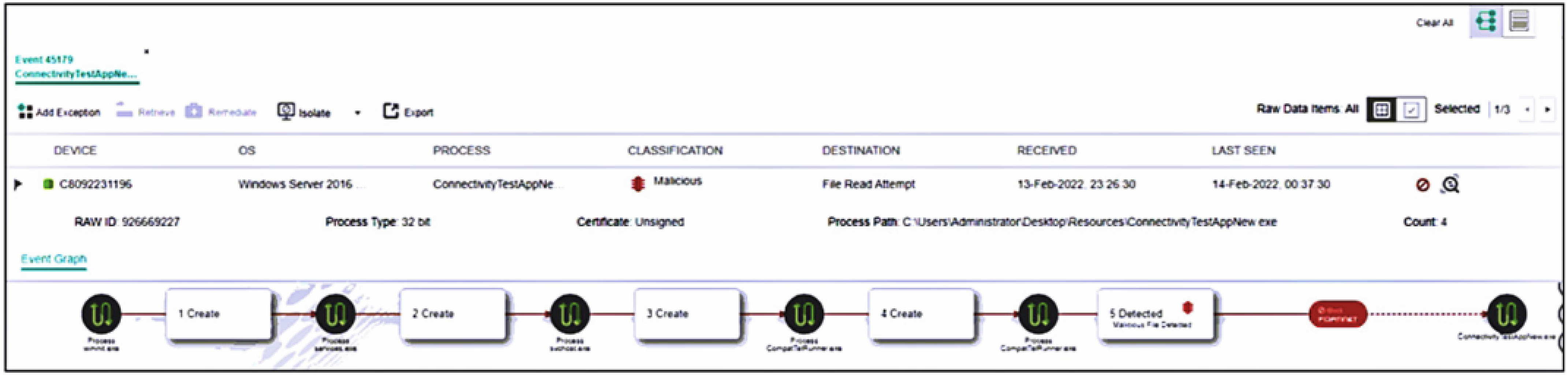
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 2

Topic #: 1

[All NSE5_EDR-5.0 Questions]

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



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

A. The device cannot be remediated.

B. The execution prevention policy has blocked this event.

C. The event was blocked because the certificate is unsigned.

D. Device C8092231196 has been isolated.

Show Suggested Answer

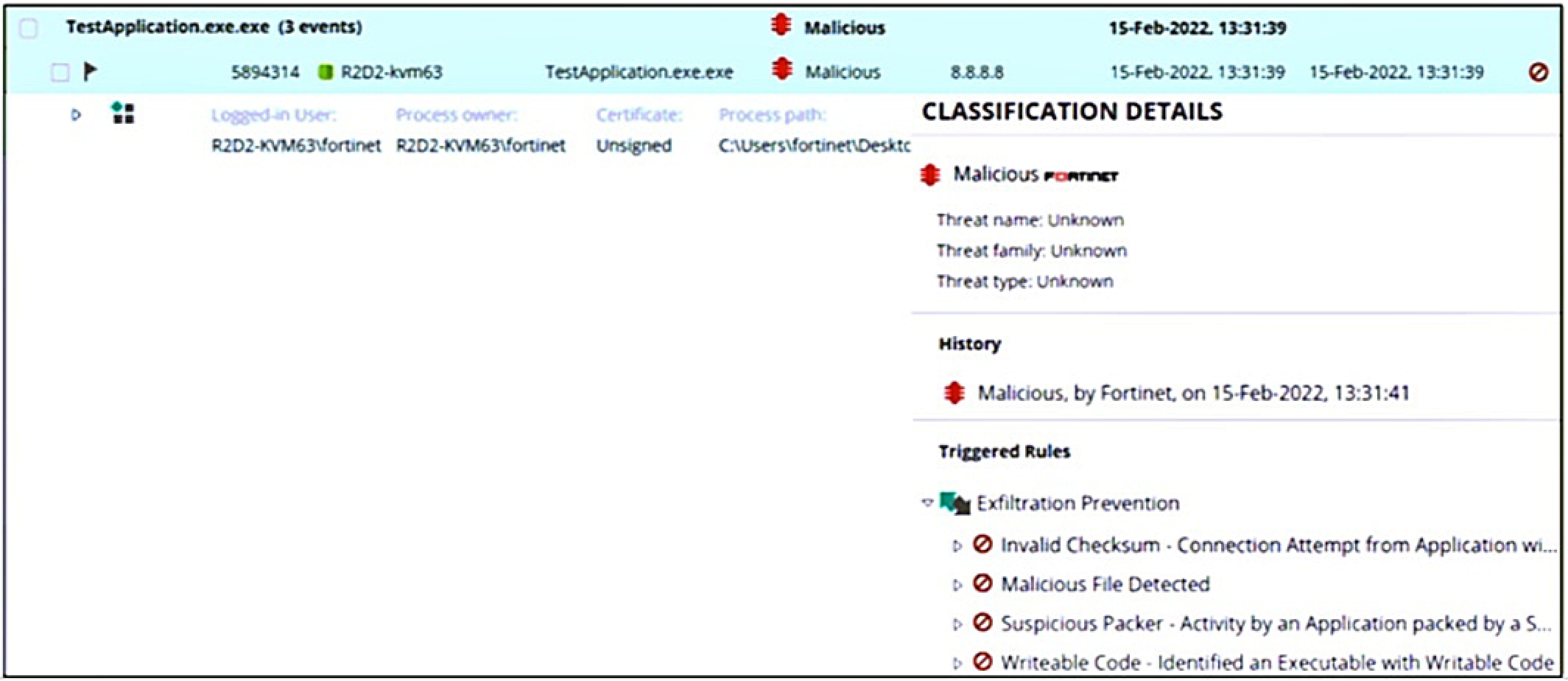
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 3

Topic #: 1

[All NSE5_EDR-5.0 Questions]

Refer to the exhibit.



□ **TestApplication.exe.exe (3 events)** **Malicious** **15-Feb-2022, 13:31:39**

□ 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\Desktc

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.)

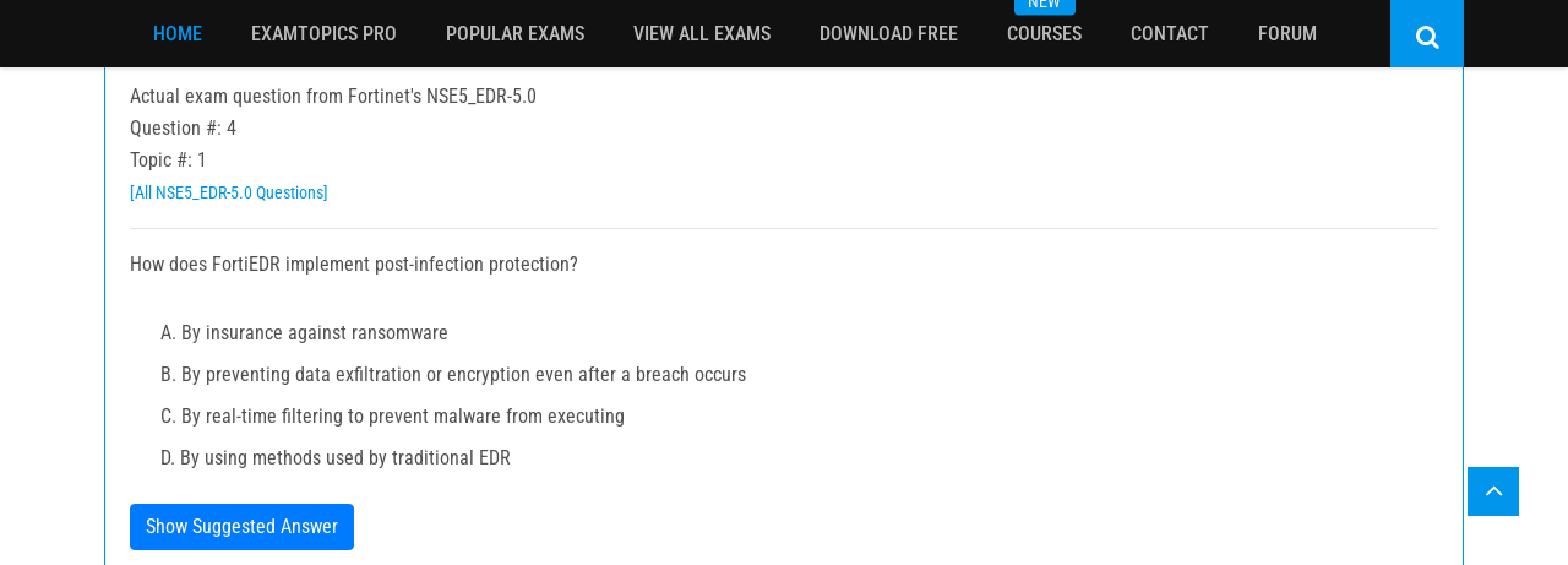
A. The NGAV policy has blocked TestApplication.exe.

B. FCS classified the event as malicious.

C. TestApplication.exe is sophisticated malware.

D. The user was able to launch TestApplication.exe.

Show Suggested Answer



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 4

Topic #: 1

[All NSE5_EDR-5.0 Questions]

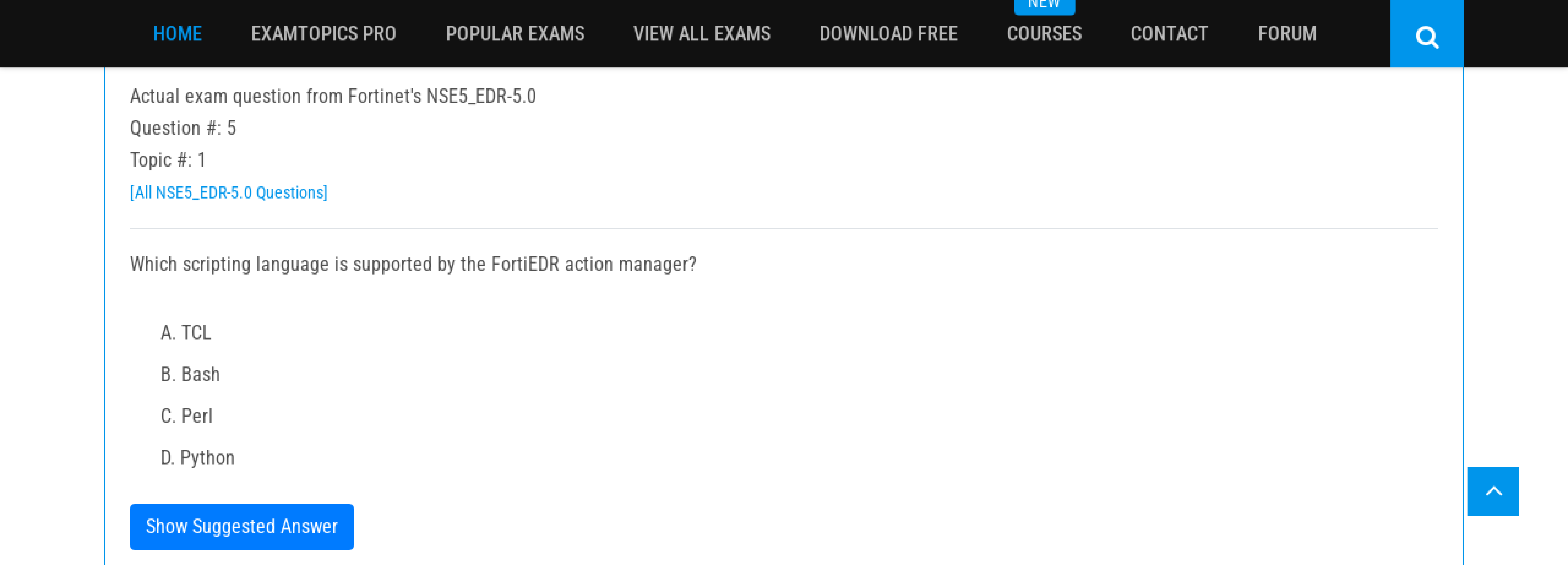
How does FortiEDR implement post-infection protection?

A. By insurance against ransomware

B. By preventing data exfiltration or encryption even after a breach occurs

C. By real-time filtering to prevent malware from executing

D. By using methods used by traditional EDR



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 5

Topic #: 1

[All NSE5_EDR-5.0 Questions]

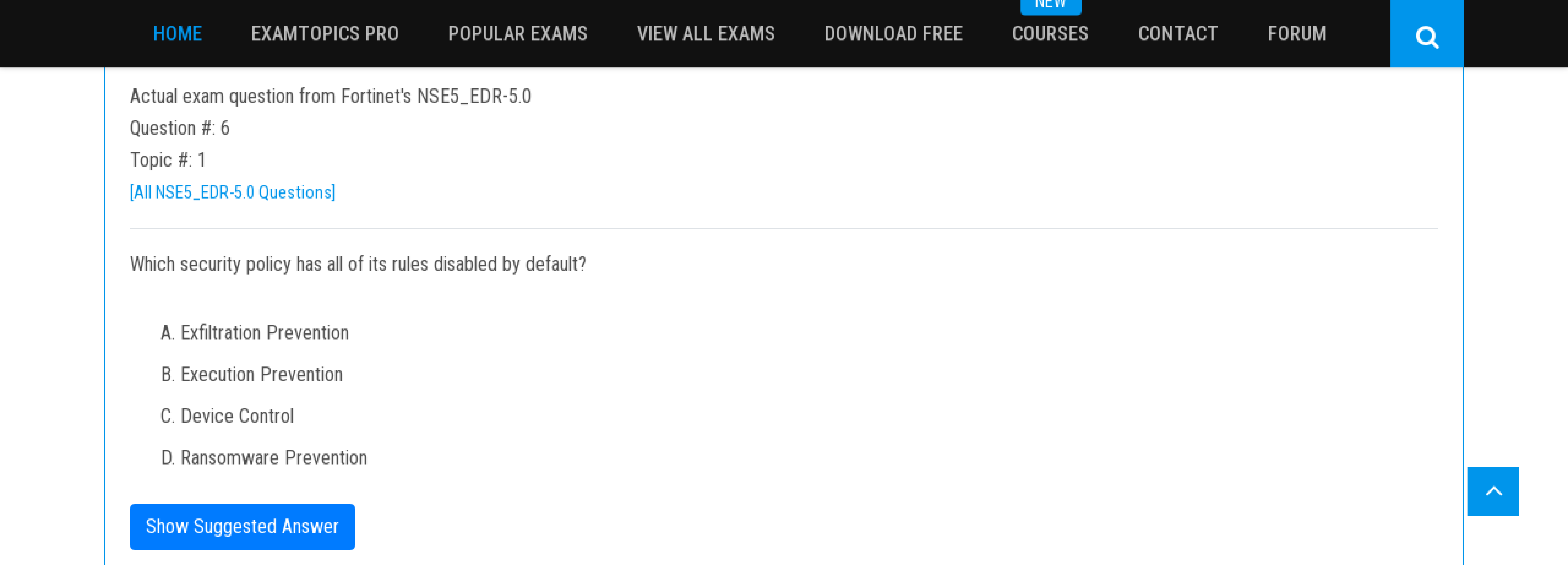
Which scripting language is supported by the FortiEDR action manager?

A. TCL

B. Bash

C. Perl

D. Python



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 6

Topic #: 1

[All NSE5_EDR-5.0 Questions]

Which security policy has all of its rules disabled by default?

A. Exfiltration Prevention

B. Execution Prevention

C. Device Control

D. Ransomware Prevention

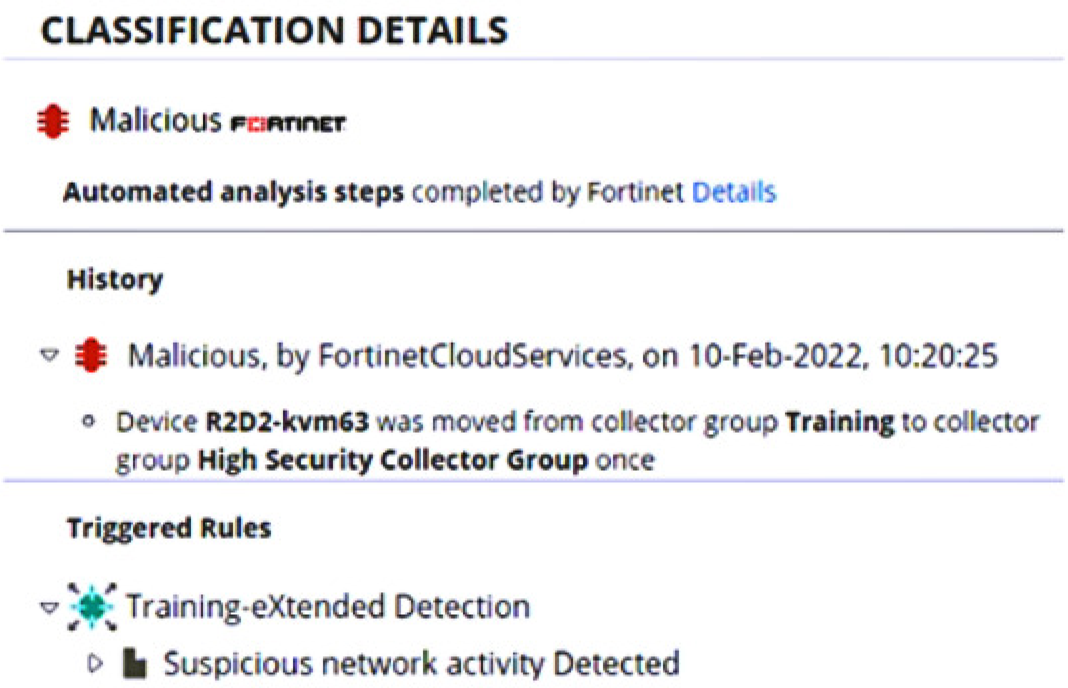
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 7

Topic #: 1

[All NSE5_EDR-5.0 Questions]

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



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

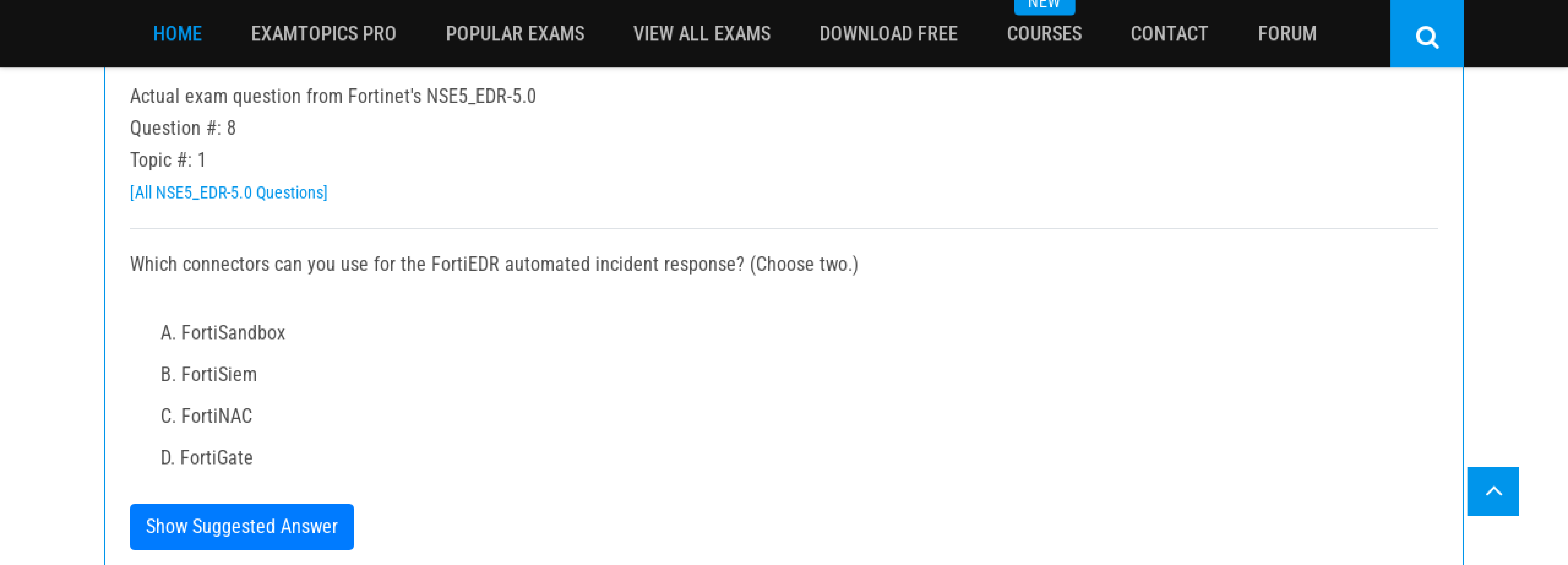
A. The policy is in simulation mode.

B. The device is moved to isolation.

C. The event has been blocked.

D. Playbooks is configured for this event.

Show Suggested Answer



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 8

Topic #: 1

[All NSE5_EDR-5.0 Questions]

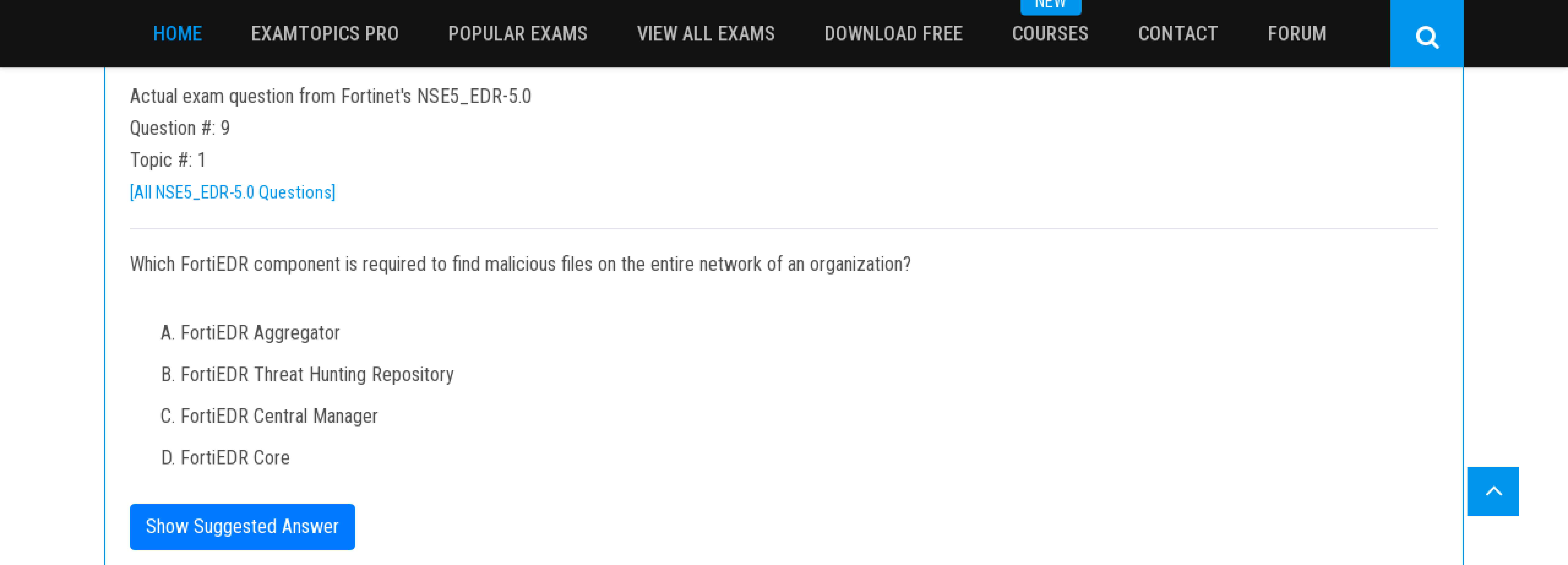
Which connectors can you use for the FortiEDR automated incident response? (Choose two.)

A. FortiSandbox

B. FortiSiem

C. FortiNAC

D. FortiGate



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 9

Topic #: 1

[All NSE5_EDR-5.0 Questions]

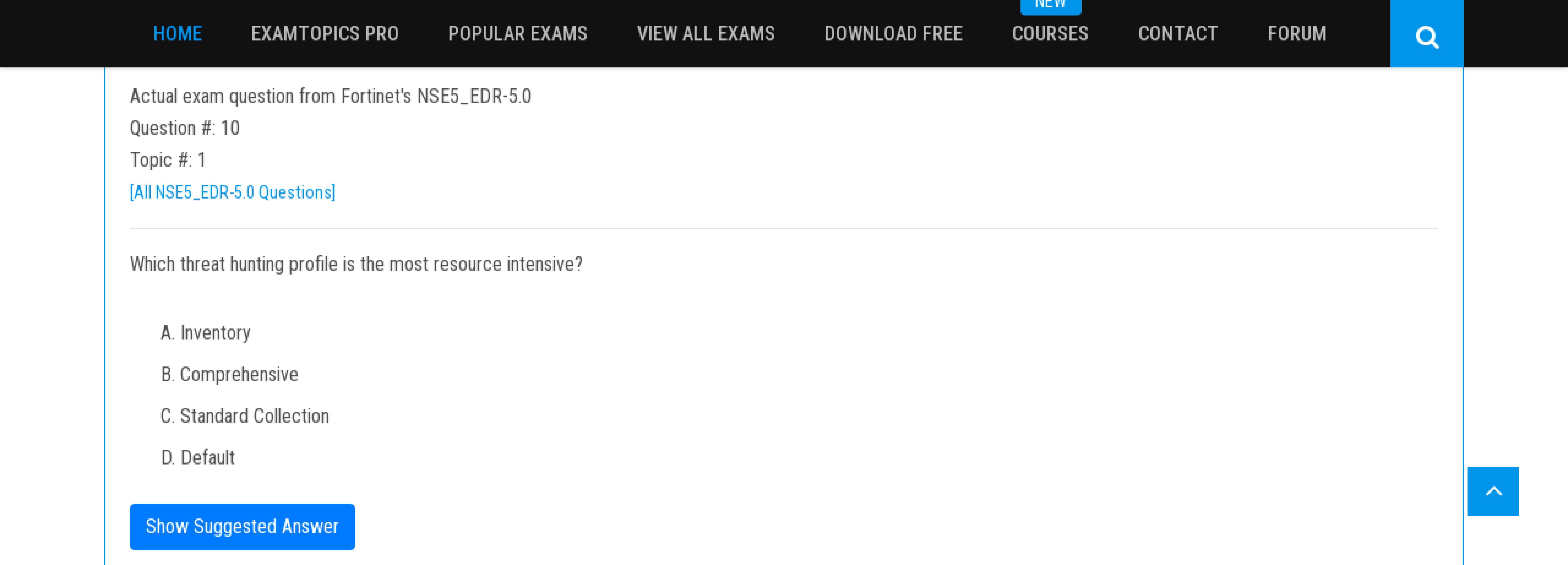
Which FortiEDR component is required to find malicious files on the entire network of an organization?

A. FortiEDR Aggregator

B. FortiEDR Threat Hunting Repository

C. FortiEDR Central Manager

D. FortiEDR Core



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 10

Topic #: 1

[All NSE5_EDR-5.0 Questions]

Which threat hunting profile is the most resource intensive?

A. Inventory

B. Comprehensive

C. Standard Collection

D. Default

Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 11

Topic #: 1

[All NSE5_EDR-5.0 Questions]

What is the role of a collector in the communication control policy?

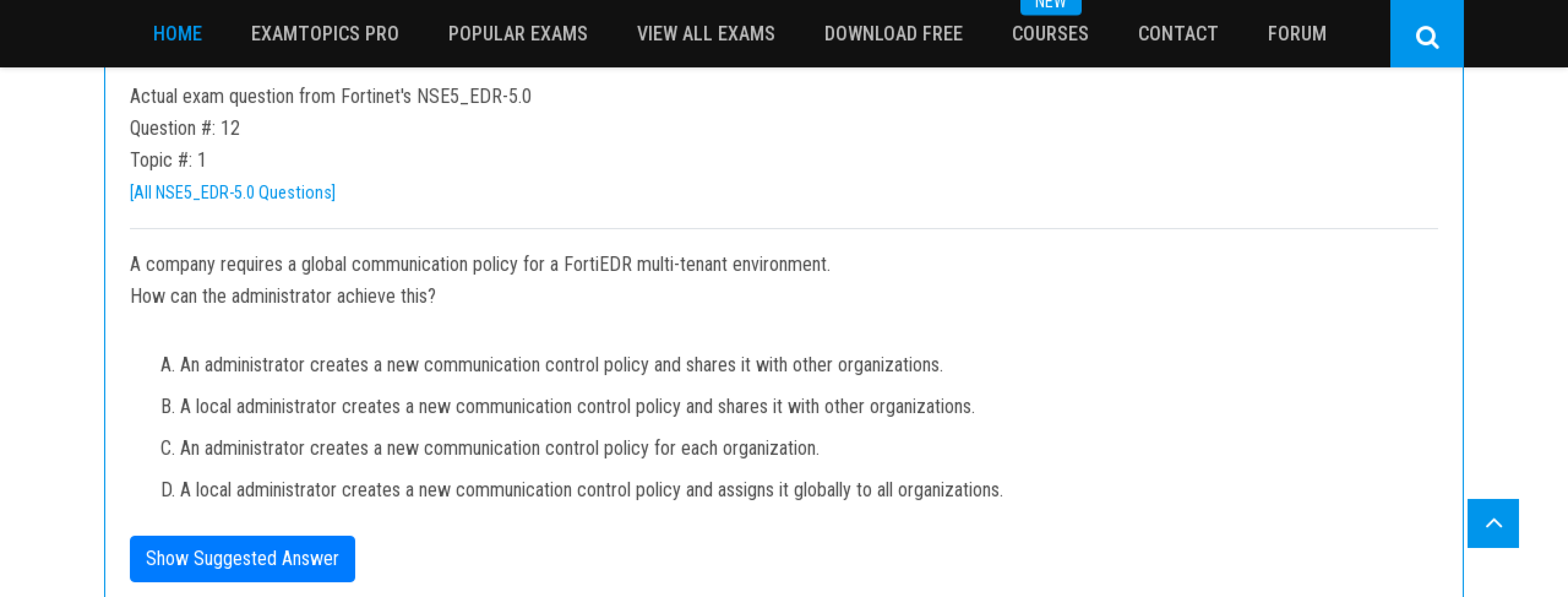
A. A collector is used to change the reputation score of any application that collector runs

B. A collector can quarantine unsafe applications from communicating

C. A collector blocks unsafe applications from running

D. A collector records applications that communicate externally

Show Suggested Answer



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 12

Topic #: 1

[All NSE5_EDR-5.0 Questions]

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 a new communication control policy and shares it with other organizations.

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

D. A local administrator creates a new communication control policy and assigns it globally to all organizations.

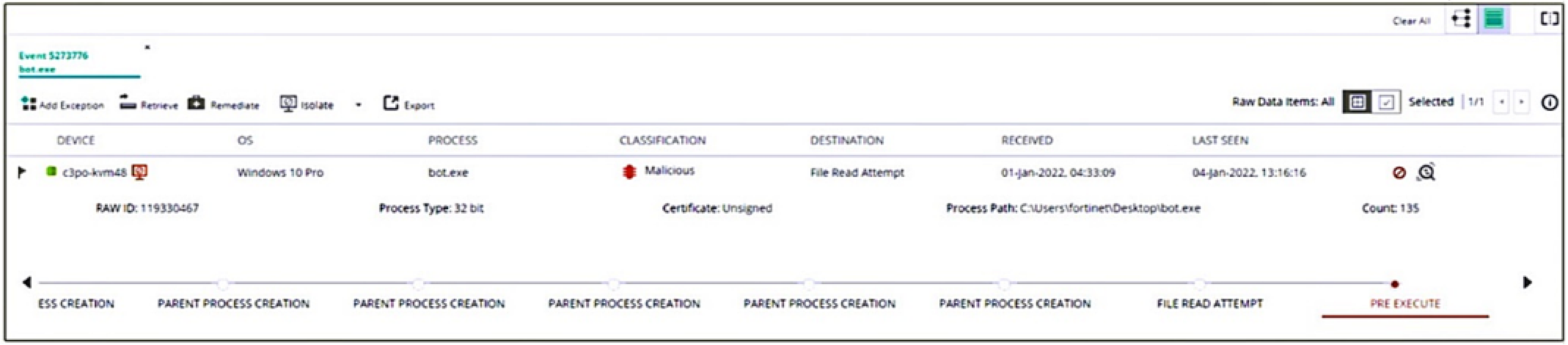
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 13

Topic #: 1

[All NSE5_EDR-5.0 Questions]

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



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

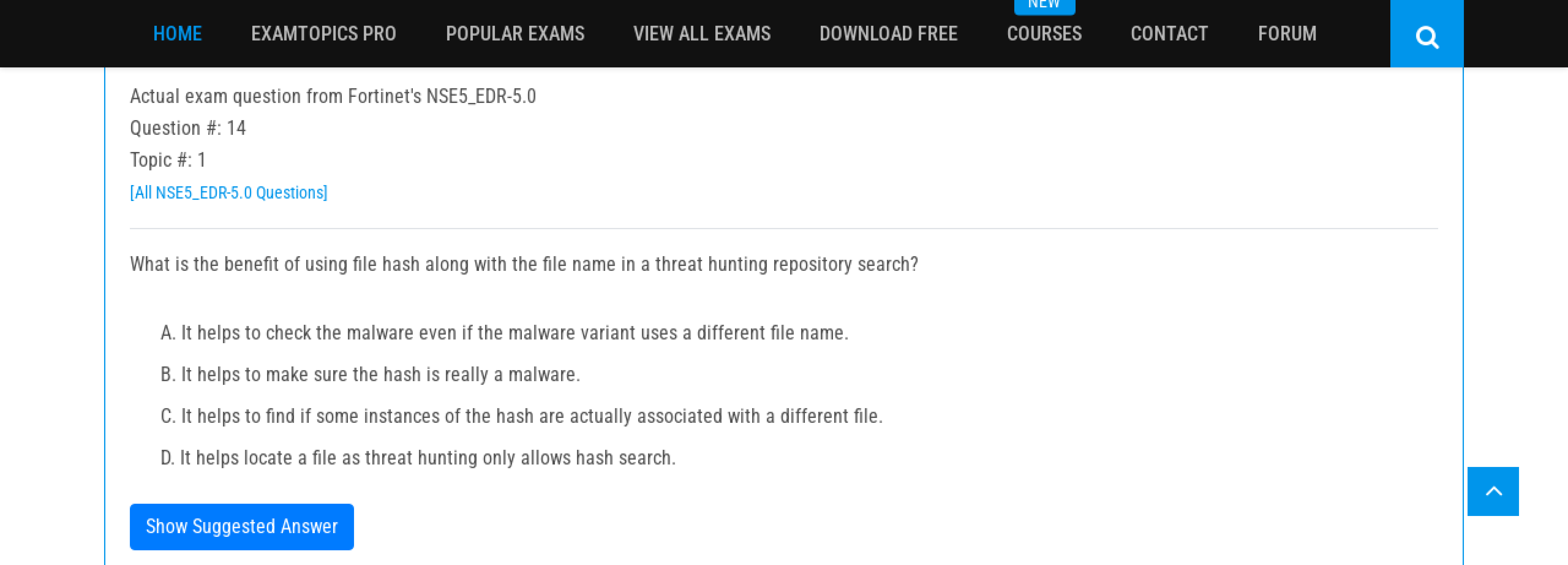
A. An exception has been created for this event.

B. The device has been isolated.

C. The exfiltration prevention policy has blocked this event.

D. The forensics data is displayed in the stacks view.

Show Suggested Answer



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 14

Topic #: 1

[All NSE5_EDR-5.0 Questions]

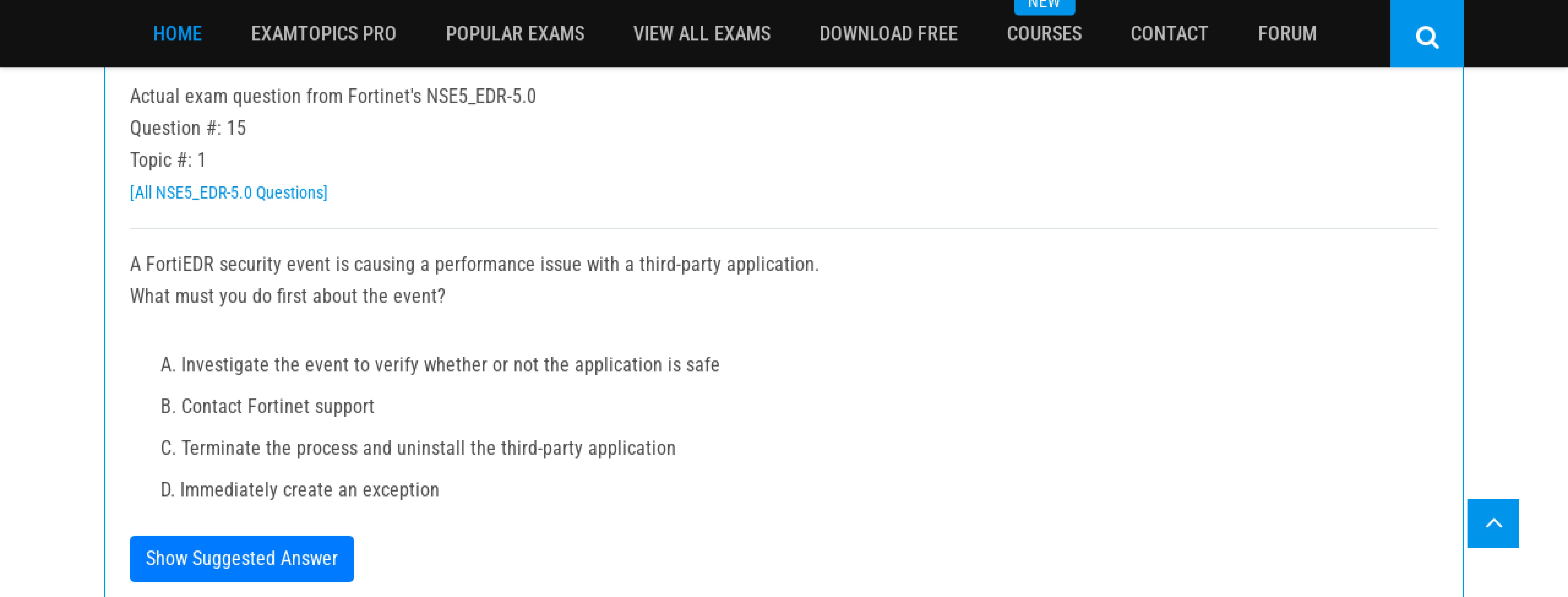
What is the benefit of using file hash along with the file name in a threat hunting repository search?

A. It helps to check the malware even if the malware variant uses a different file name.

B. It helps to make sure the hash is really a malware.

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.



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 15

Topic #: 1

[All NSE5_EDR-5.0 Questions]

A FortiEDR security event is causing a performance issue with a third-party application.

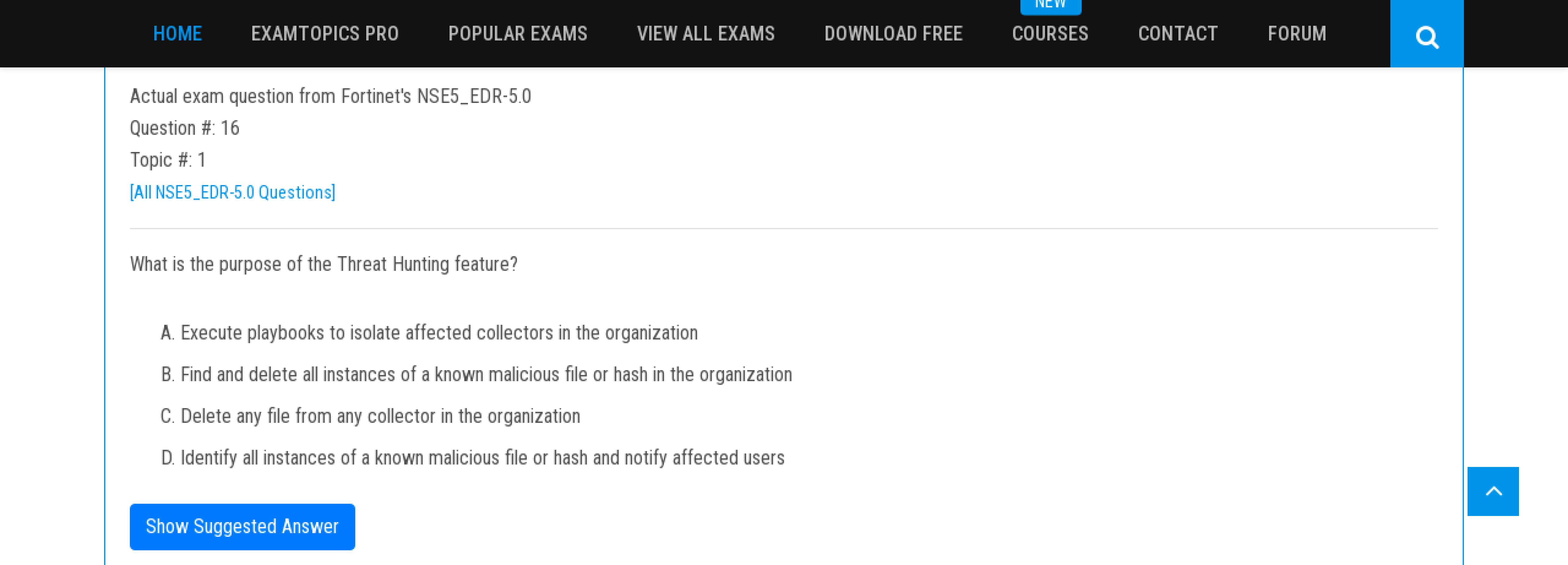
What must you do first about the event?

A. Investigate the event to verify whether or not the application is safe

B. Contact Fortinet support

C. Terminate the process and uninstall the third-party application

D. Immediately create an exception



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 16

Topic #: 1

[All NSE5_EDR-5.0 Questions]

What is the purpose of the Threat Hunting feature?

A. Execute playbooks to isolate affected collectors in the organization

B. Find and delete all instances of a known malicious file or hash in the organization

C. Delete any file from any collector in the organization

D. Identify all instances of a known malicious file or hash and notify affected users

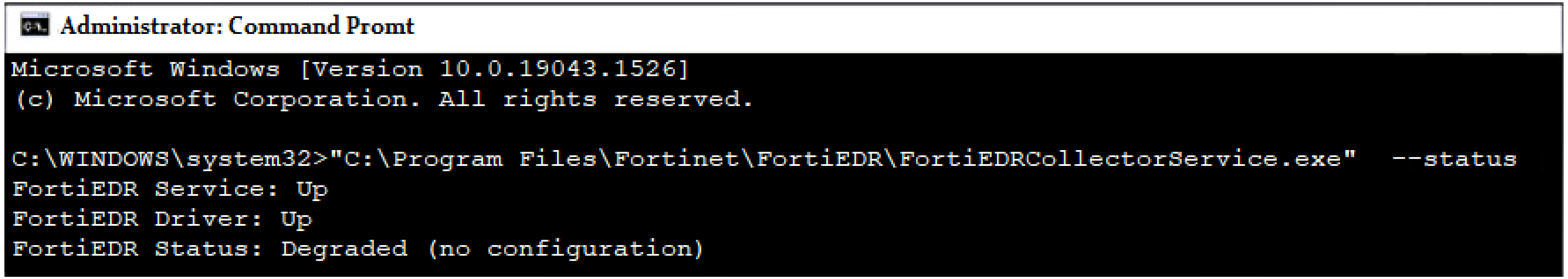
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 17

Topic #: 1

[All NSE5_EDR-5.0 Questions]

Refer to the exhibit.



Administrator: Command Promt

```
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.)

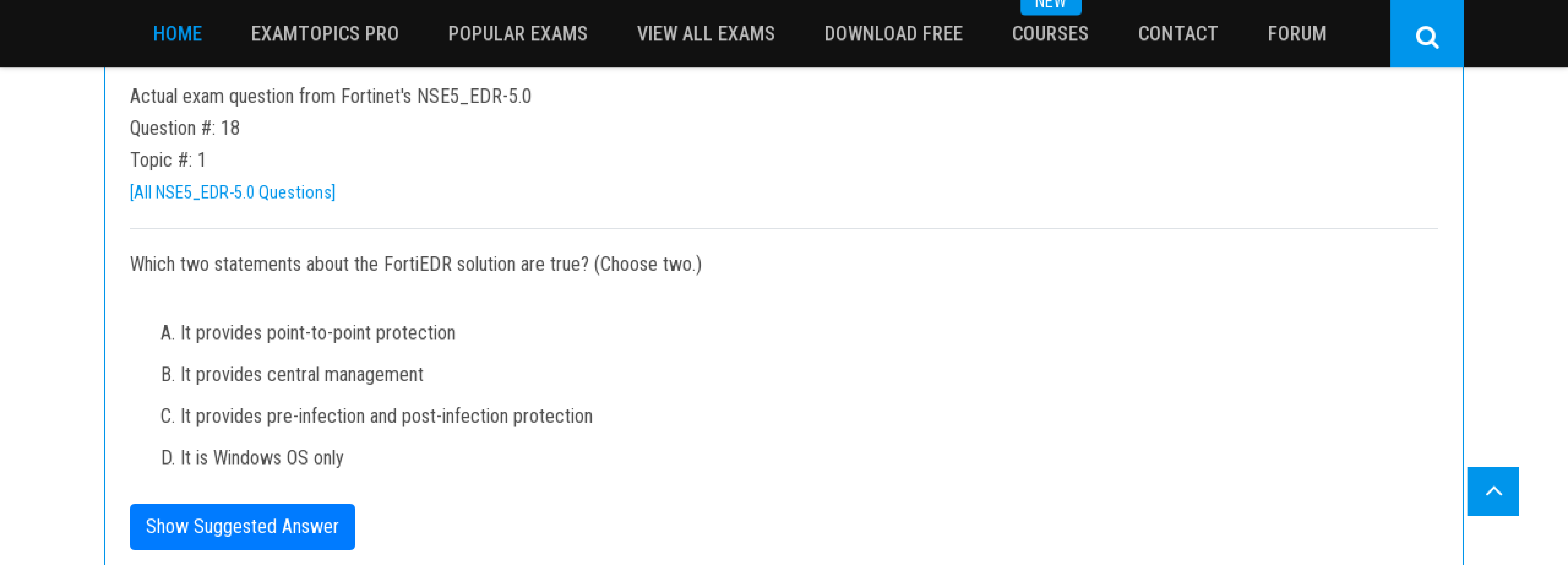
A. The collector device has windows firewall enabled.

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 18

Topic #: 1

[All NSE5_EDR-5.0 Questions]

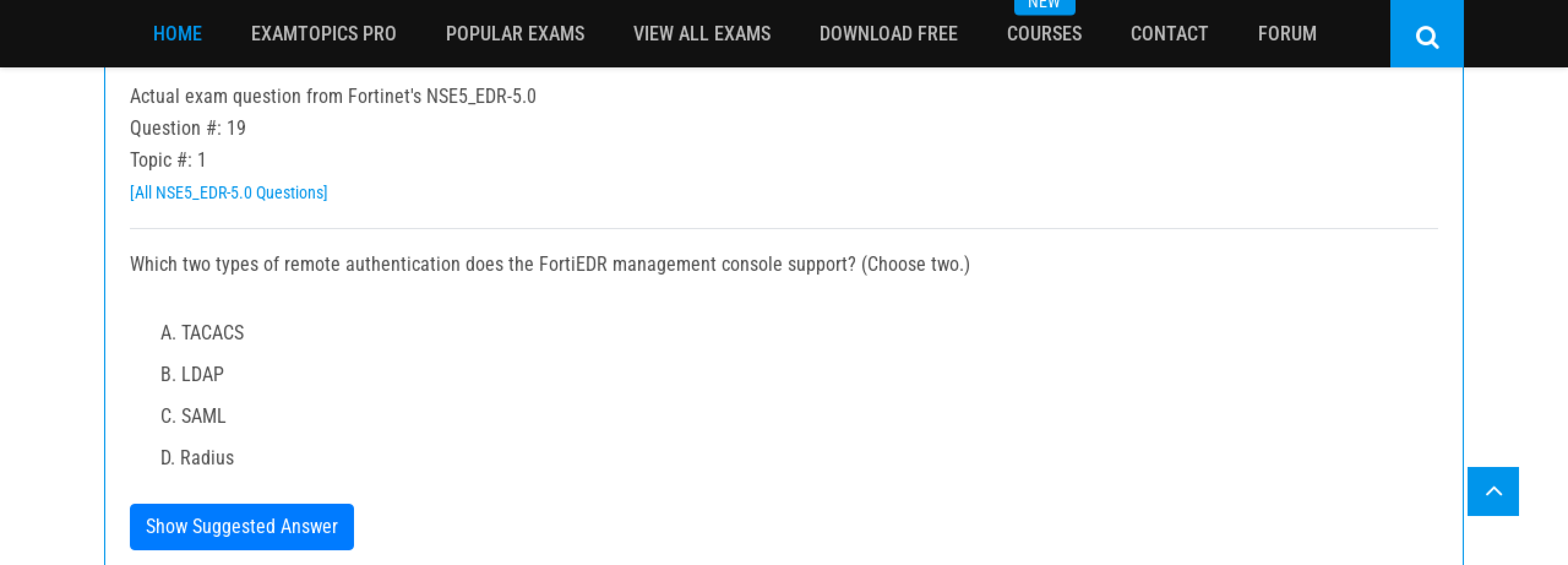
Which two statements about the FortiEDR solution are true? (Choose two.)

A. It provides point-to-point protection

B. It provides central management

C. It provides pre-infection and post-infection protection

D. It is Windows OS only



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 19

Topic #: 1

[All NSE5_EDR-5.0 Questions]

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

A. TACACS

B. LDAP

C. SAML

D. Radius

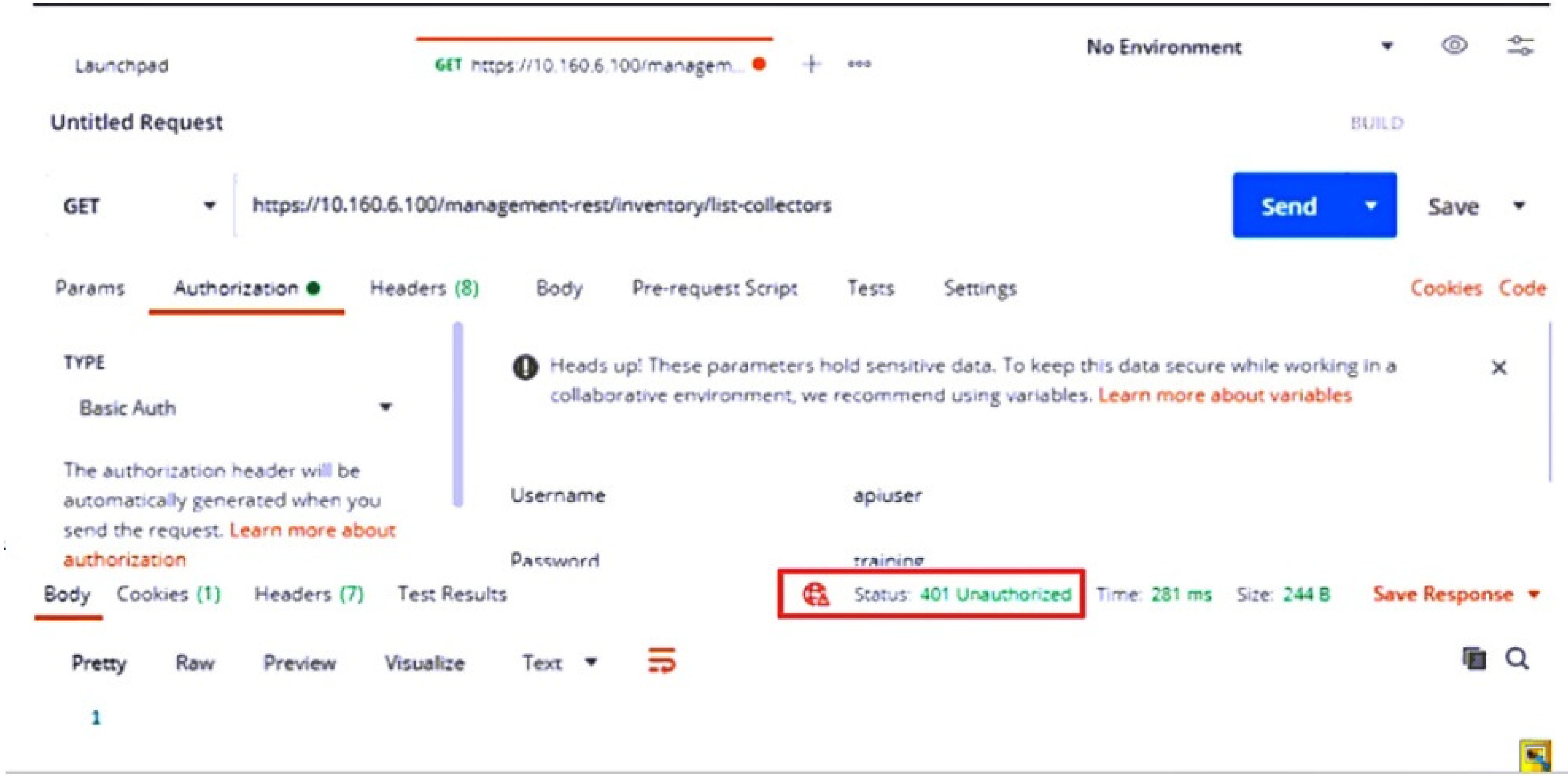
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 20

Topic #: 1

[All NSE5_EDR-5.0 Questions]

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

1

Based on the postman output shown in the exhibit, why is the user getting an unauthorized error?

A. Postman cannot reach the central manager.

B. API access is disabled on the central manager.

C. The user has been assigned Admin and Rest API roles.

D. FortiEDR requires a password reset the first time a user logs in.

Show Suggested Answer

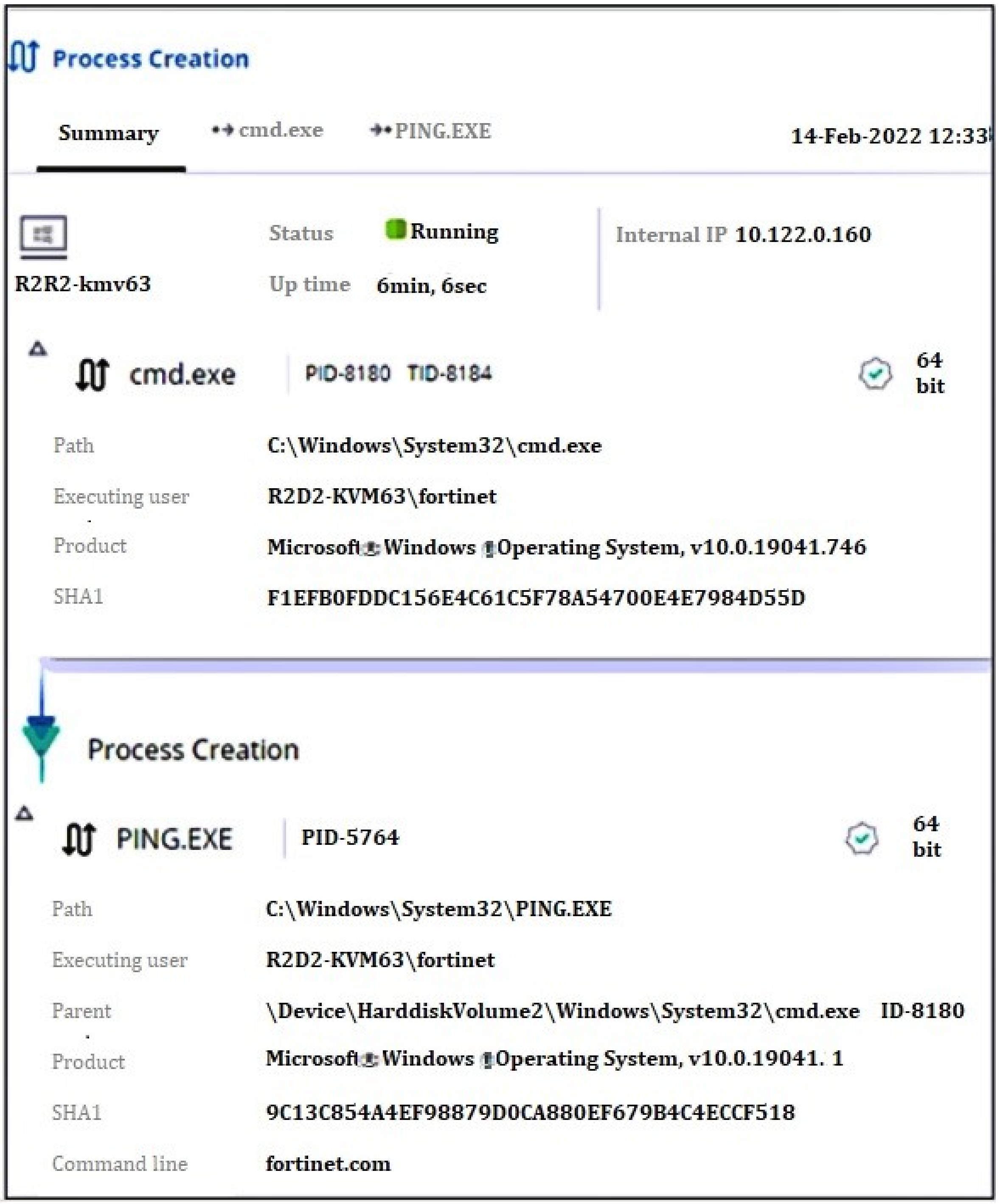
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 21

Topic #: 1

[All NSE5_EDR-5.0 Questions]

Refer to the exhibit.



Process Creation

Summary ↔ cmd.exe ↔ PING.EXE 14-Feb-2022 12:33

R2R2-kmv63

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	F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D

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	9C13C854A4EF98879D0CA880EF679B4C4ECCF518
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 activity event is associated with the file action.

B. The user fortinet has executed a ping command.

C. The PING.EXE process was blocked.

D. There are no MITRE details available for this event.

Show Suggested Answer

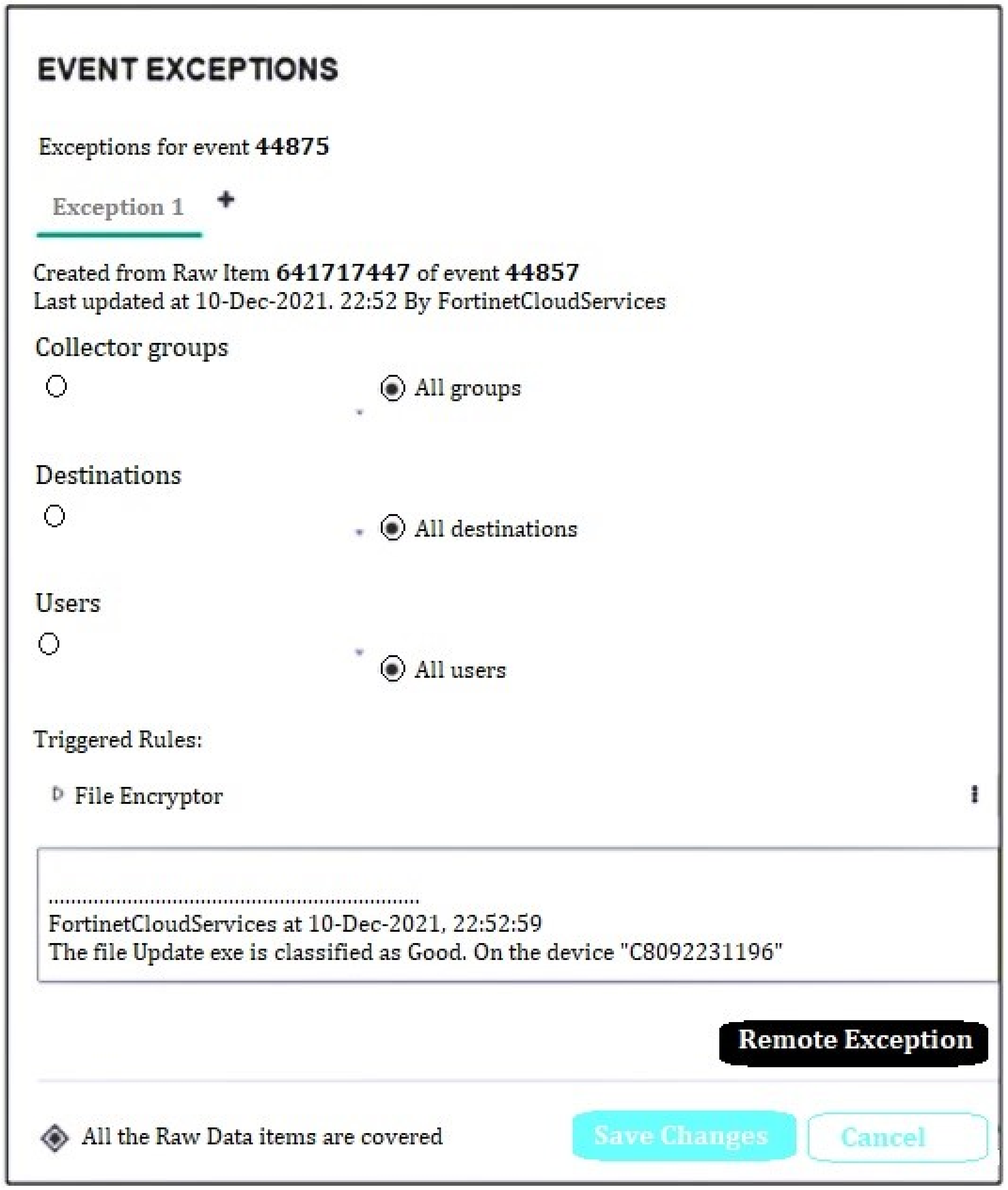
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 22

Topic #: 1

[All NSE5_EDR-5.0 Questions]

Refer to the exhibit.



EVENT EXCEPTIONS

Exceptions for event **44875**

Exception 1 +

Created from Raw Item **641717447** of event **44857**
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"

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

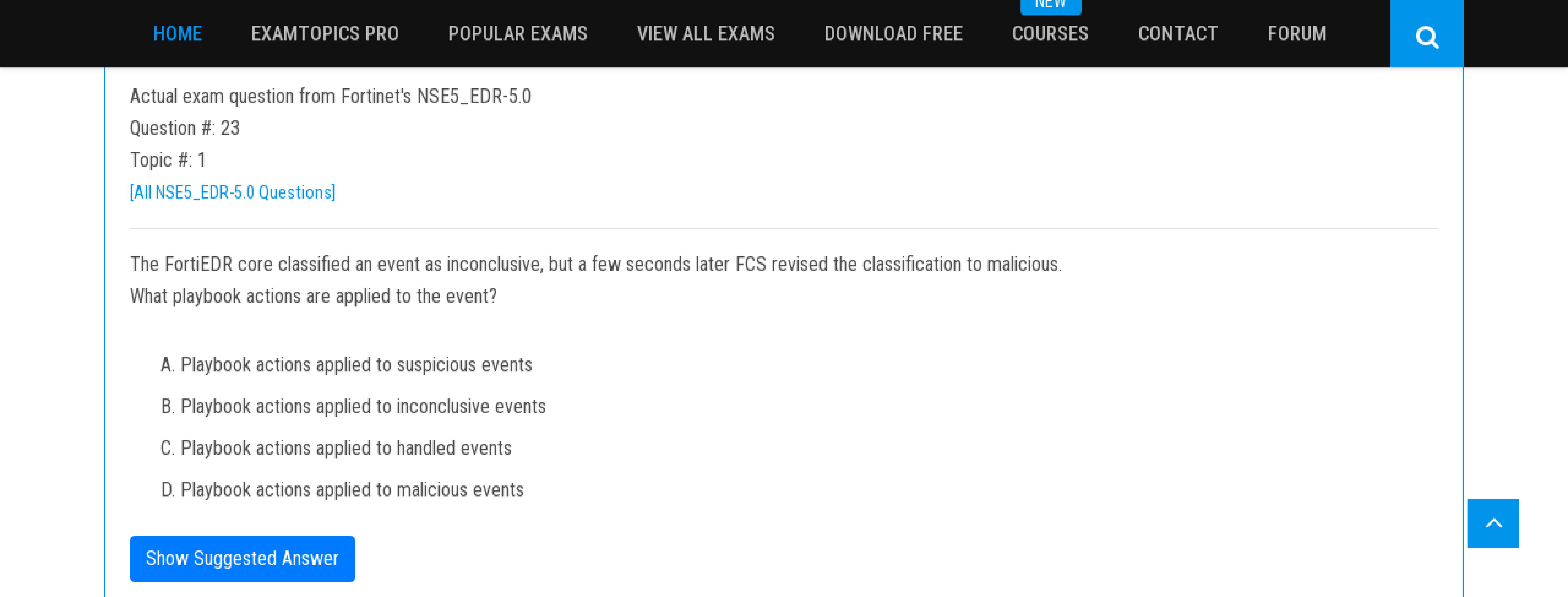
A. FCS playbooks is enabled by Fortinet support.

B. The system owner can modify the trigger rules parameters.

C. The exception is applied only on device C8092231196.

D. A partial exception is applied to this event.

Show Suggested Answer



Actual exam question from Fortinet's NSE5_EDR-5.0
Question #: 23
Topic #: 1
[All NSE5_EDR-5.0 Questions]

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

A. Playbook actions applied to suspicious events

B. Playbook actions applied to inconclusive events

C. Playbook actions applied to handled events

D. Playbook actions applied to malicious events

Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 24

Topic #: 1

[All NSE5_EDR-5.0 Questions]

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

A. Security Policies

B. Forensic

C. Playbooks

D. Communication Control

Show Suggested Answer

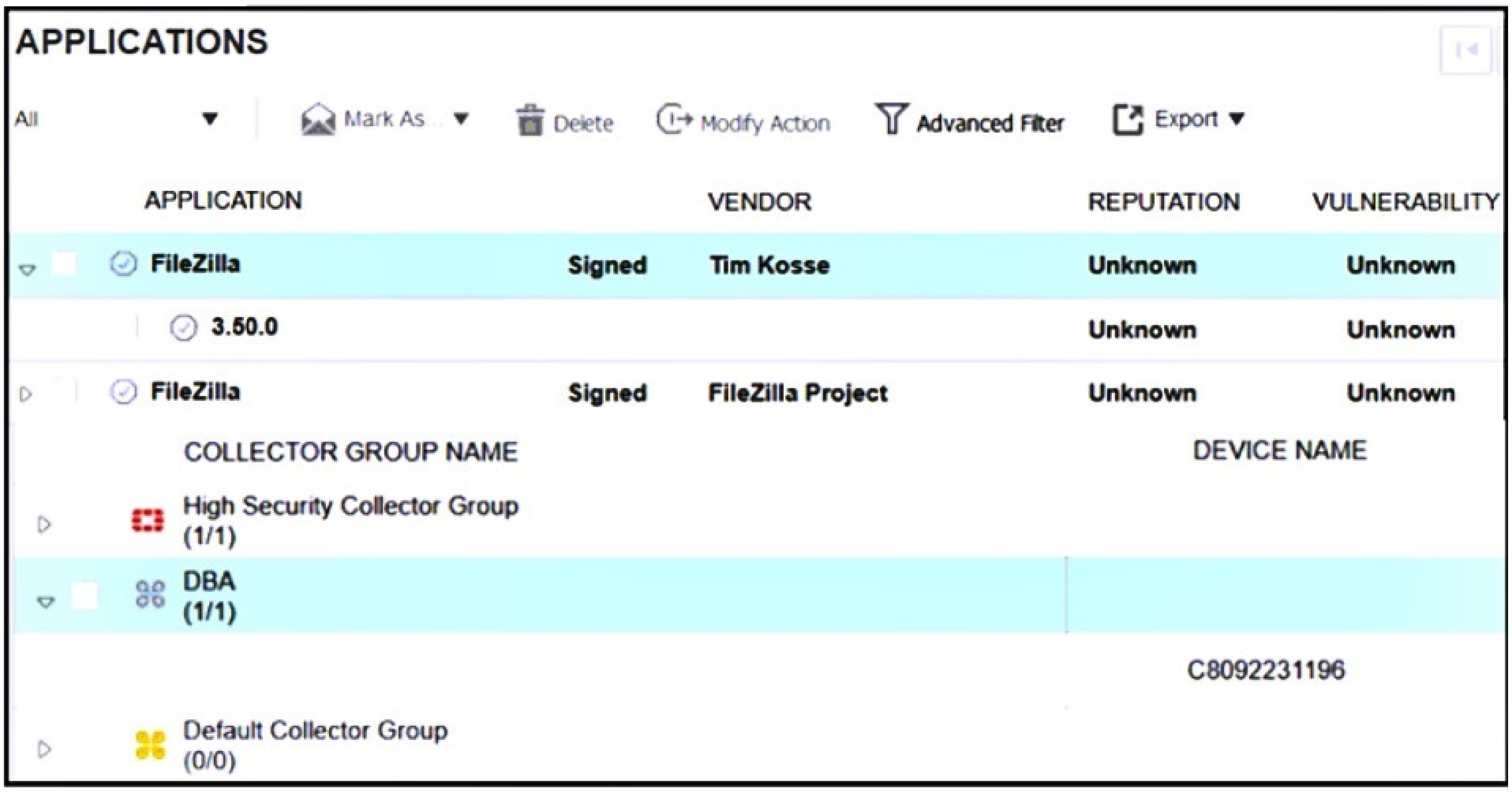
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 25

Topic #: 1

[All NSE5_EDR-5.0 Questions]

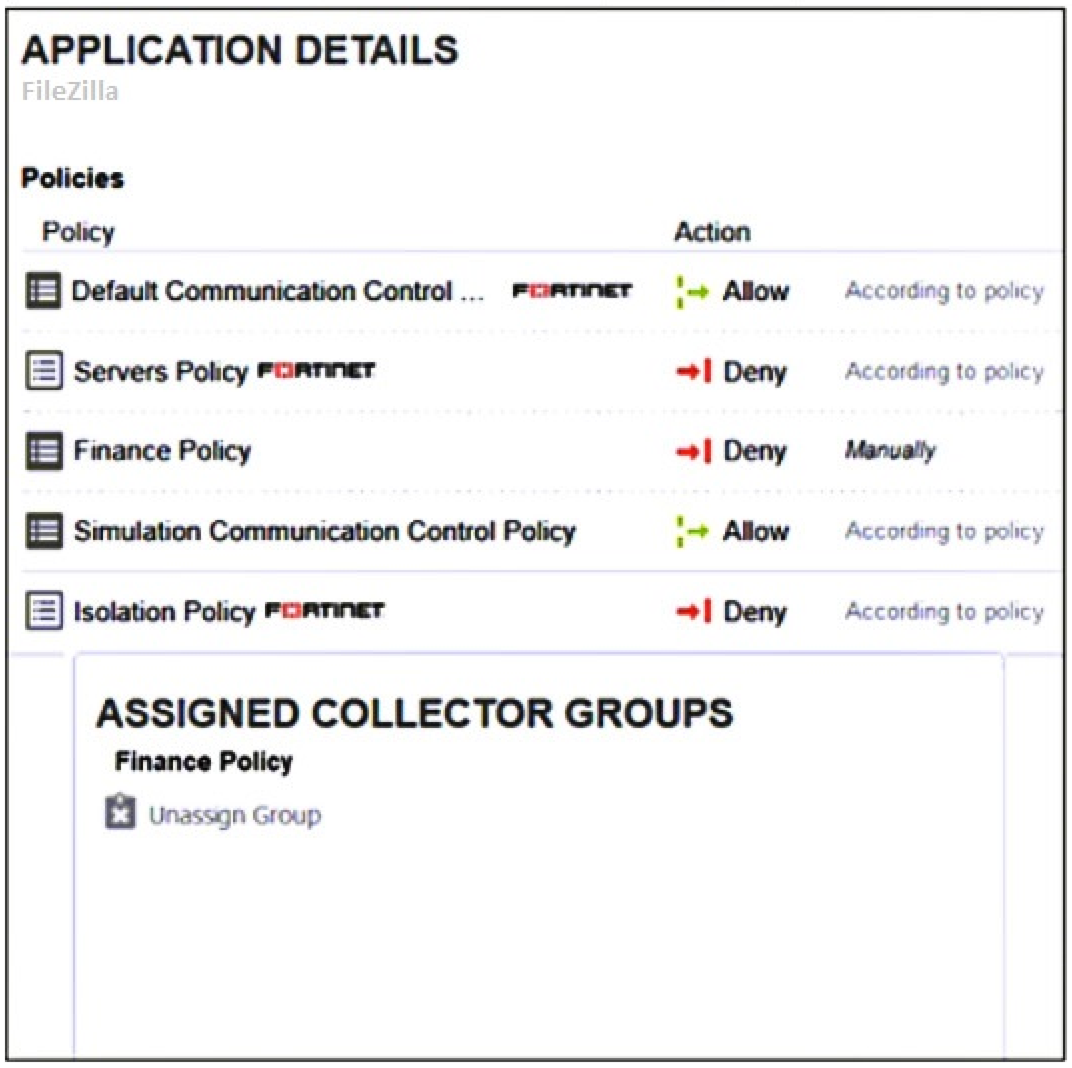
Refer to the exhibits.



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

FileZilla

Policies

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

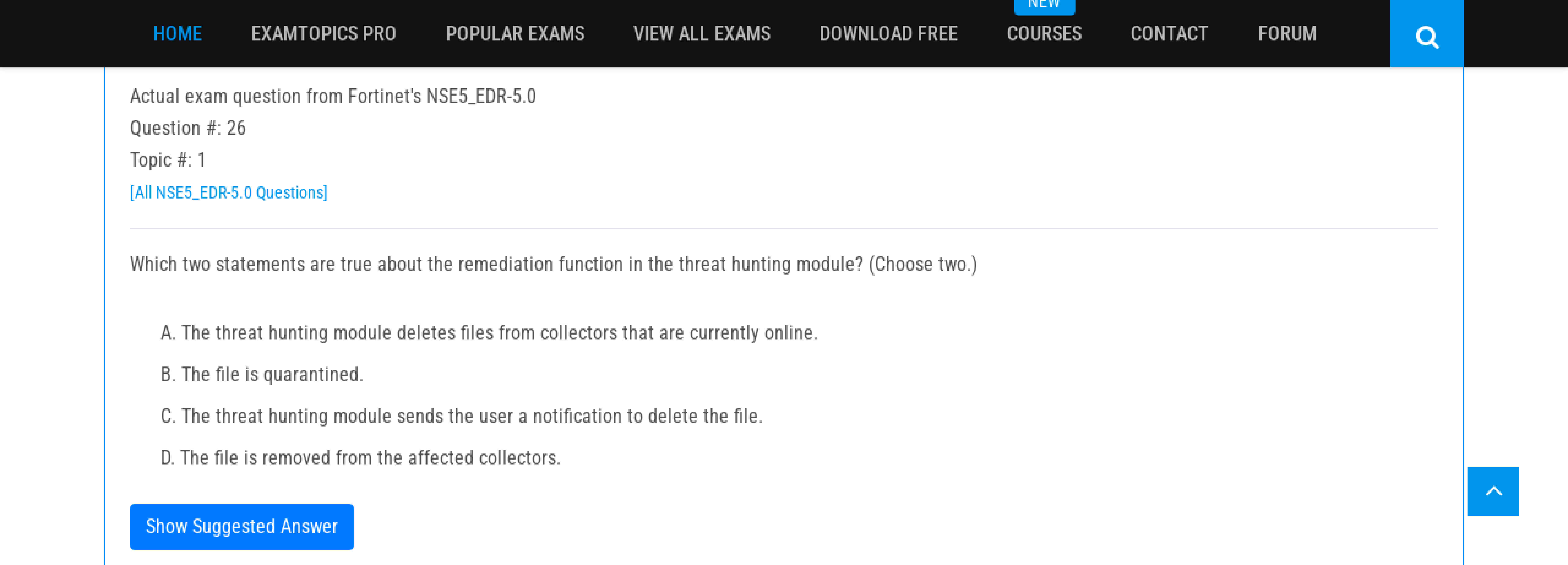
A. Deny application in Finance policy

B. Assign Finance policy to DBA group

C. Assign Finance policy to Default Collector Group

D. Assign Simulation Communication Control Policy to DBA group

Show Suggested Answer



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 26

Topic #: 1

[All NSE5_EDR-5.0 Questions]

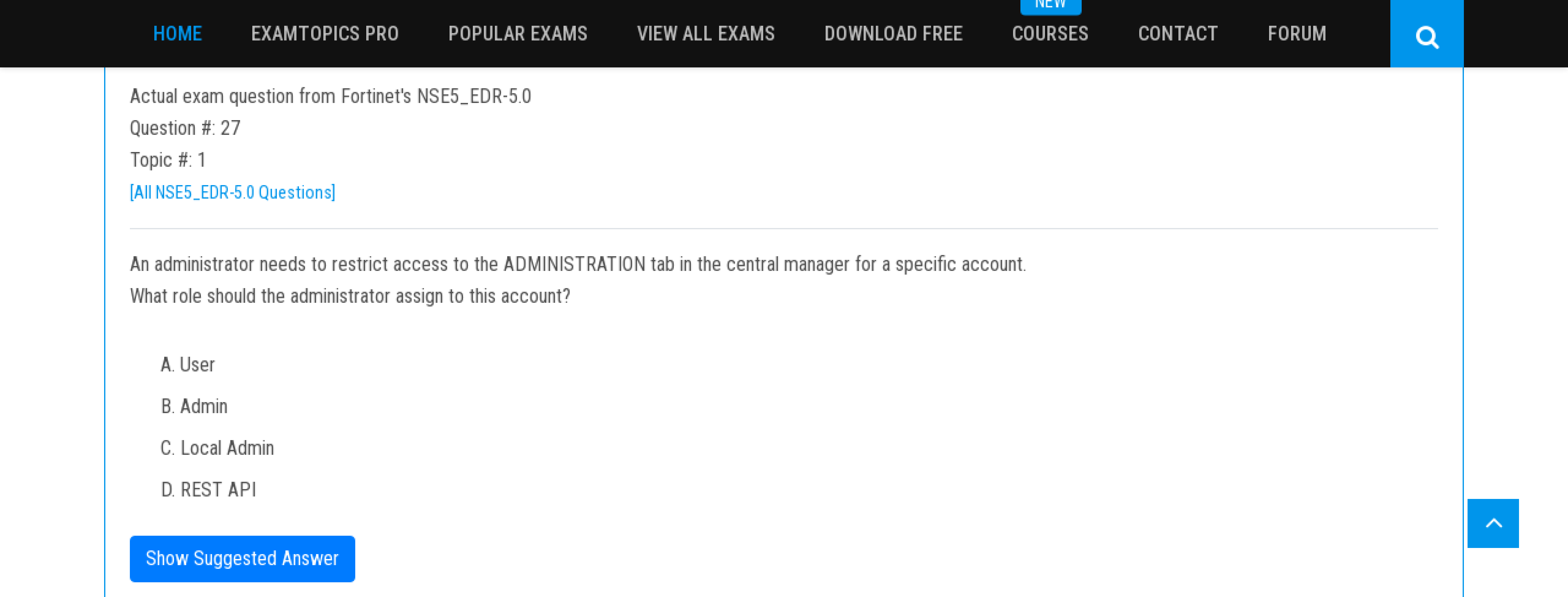
Which two statements are true about the remediation function in the threat hunting module? (Choose two.)

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

B. The file is quarantined.

C. The threat hunting module sends the user a notification to delete the file.

D. The file is removed from the affected collectors.



Actual exam question from Fortinet's NSE5_EDR-5.0
Question #: 27
Topic #: 1
[All NSE5_EDR-5.0 Questions]

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?

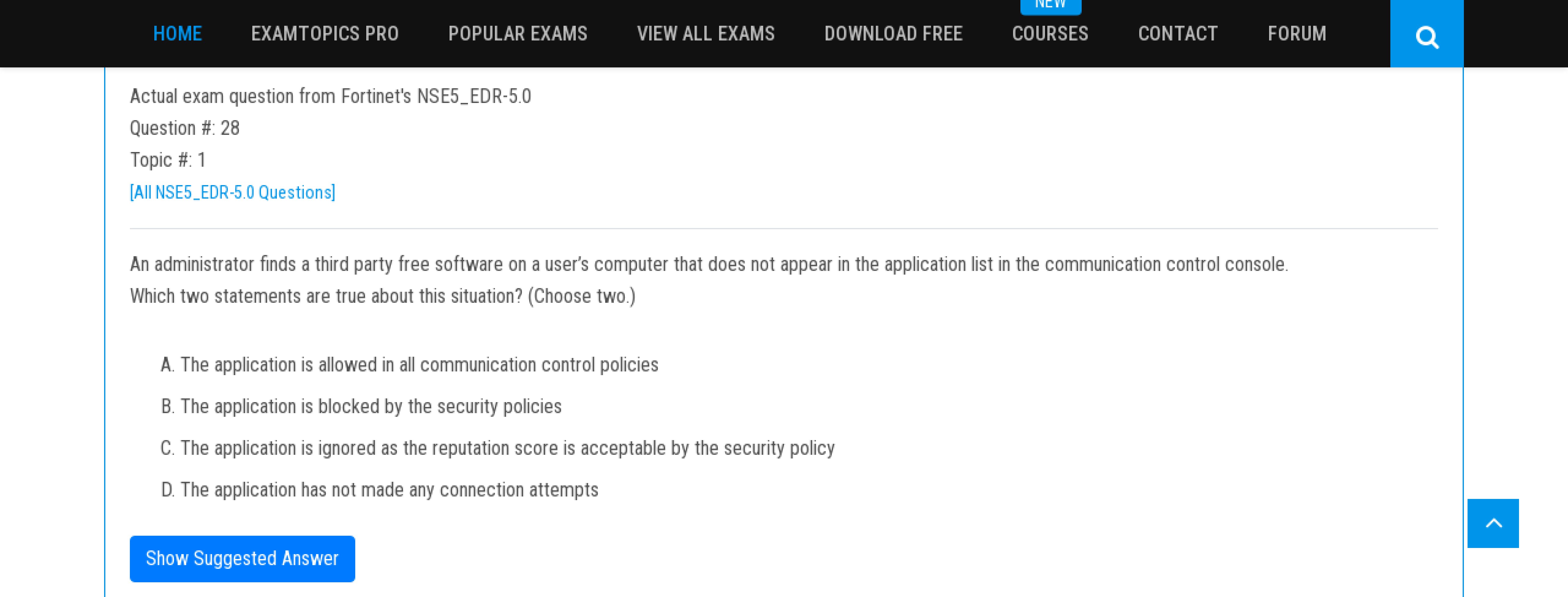
A. User

B. Admin

C. Local Admin

D. REST API

Show Suggested Answer



Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 28

Topic #: 1

[All NSE5_EDR-5.0 Questions]

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 blocked by the security policies

C. The application is ignored as the reputation score is acceptable by the security policy

D. The application has not made any connection attempts

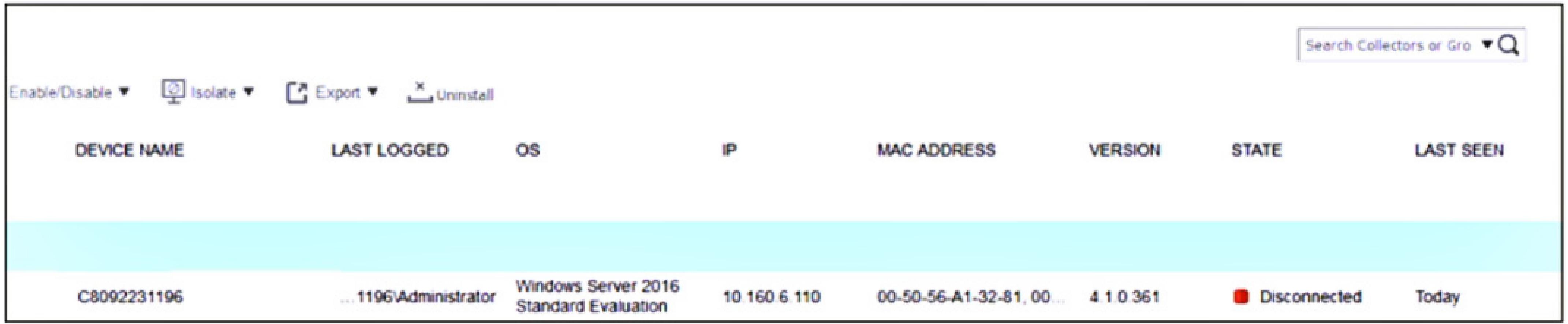
Actual exam question from Fortinet's NSE5_EDR-5.0

Question #: 29

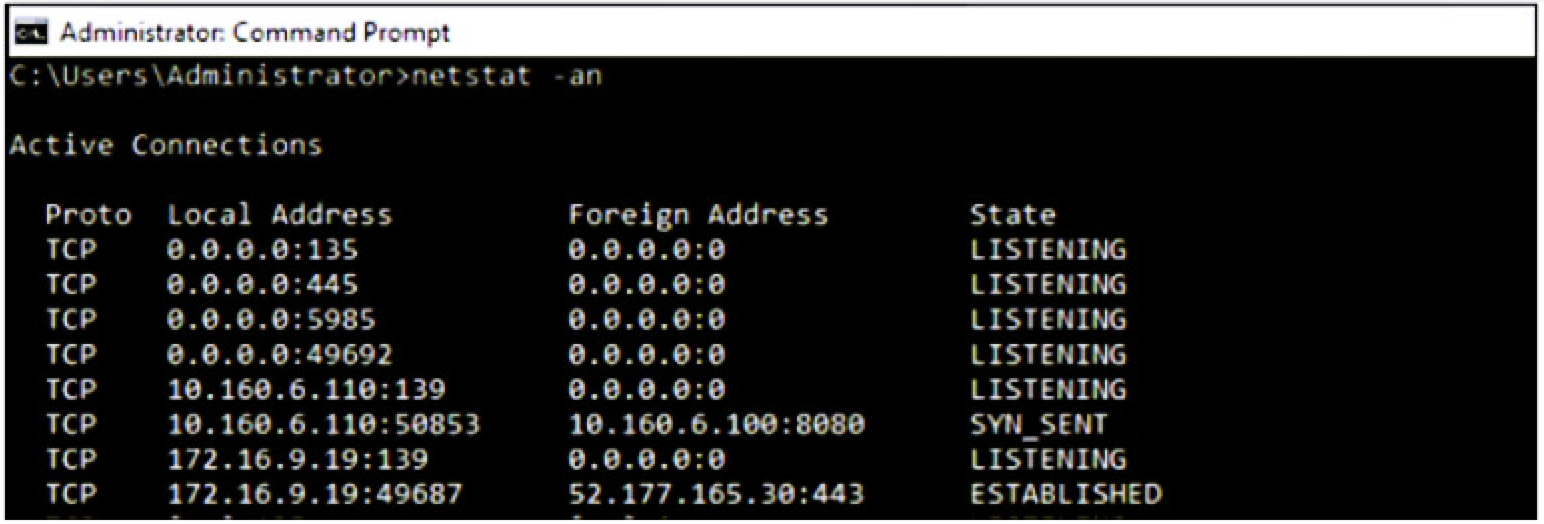
Topic #: 1

[All NSE5_EDR-5.0 Questions]

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



```
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 555

B. Reinstall collector agent and use port 443

C. Reinstall collector agent and use port 6514

D. Reinstall collector agent and use port 8081

Show Suggested Answer