NSE5_EDR-5.0 Q&As

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse5_edr-5-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

A. FortiEDR Aggregator

B. FortiEDR Central Manager

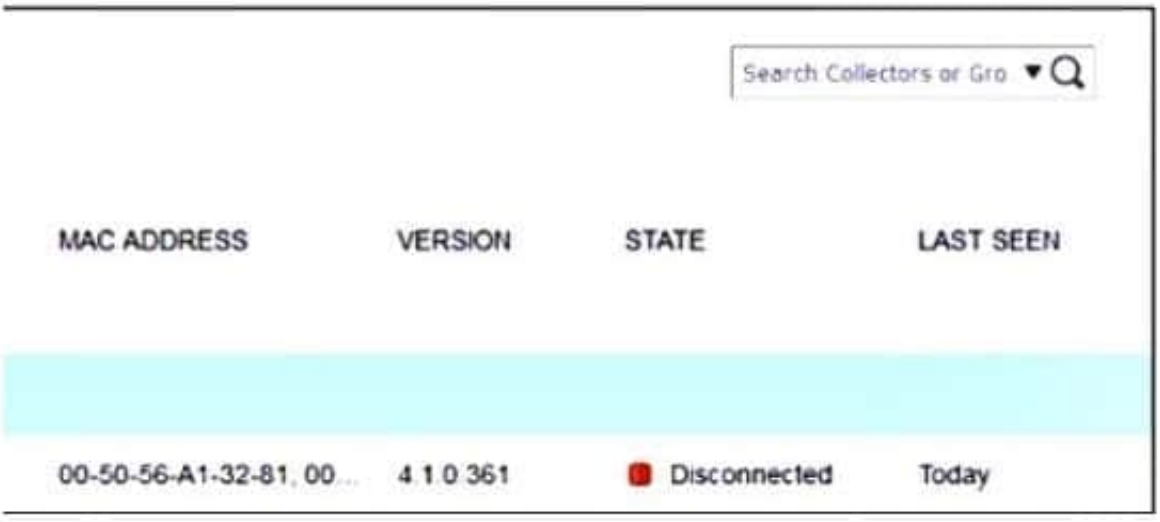
C. FortiEDR Threat Hunting Repository

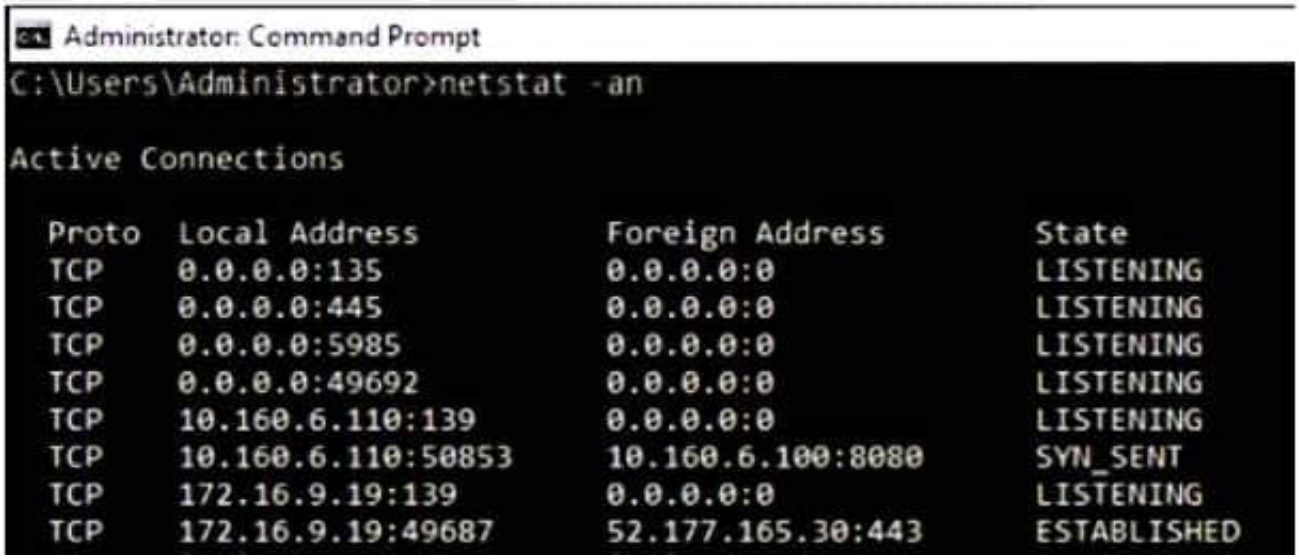
D. FortiEDR Core

Correct Answer: C

QUESTION 2

Refer to the exhibits.





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

QUESTION 3

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: D

QUESTION 4

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

QUESTION 5

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 of a known malicious file or hash in the organization

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

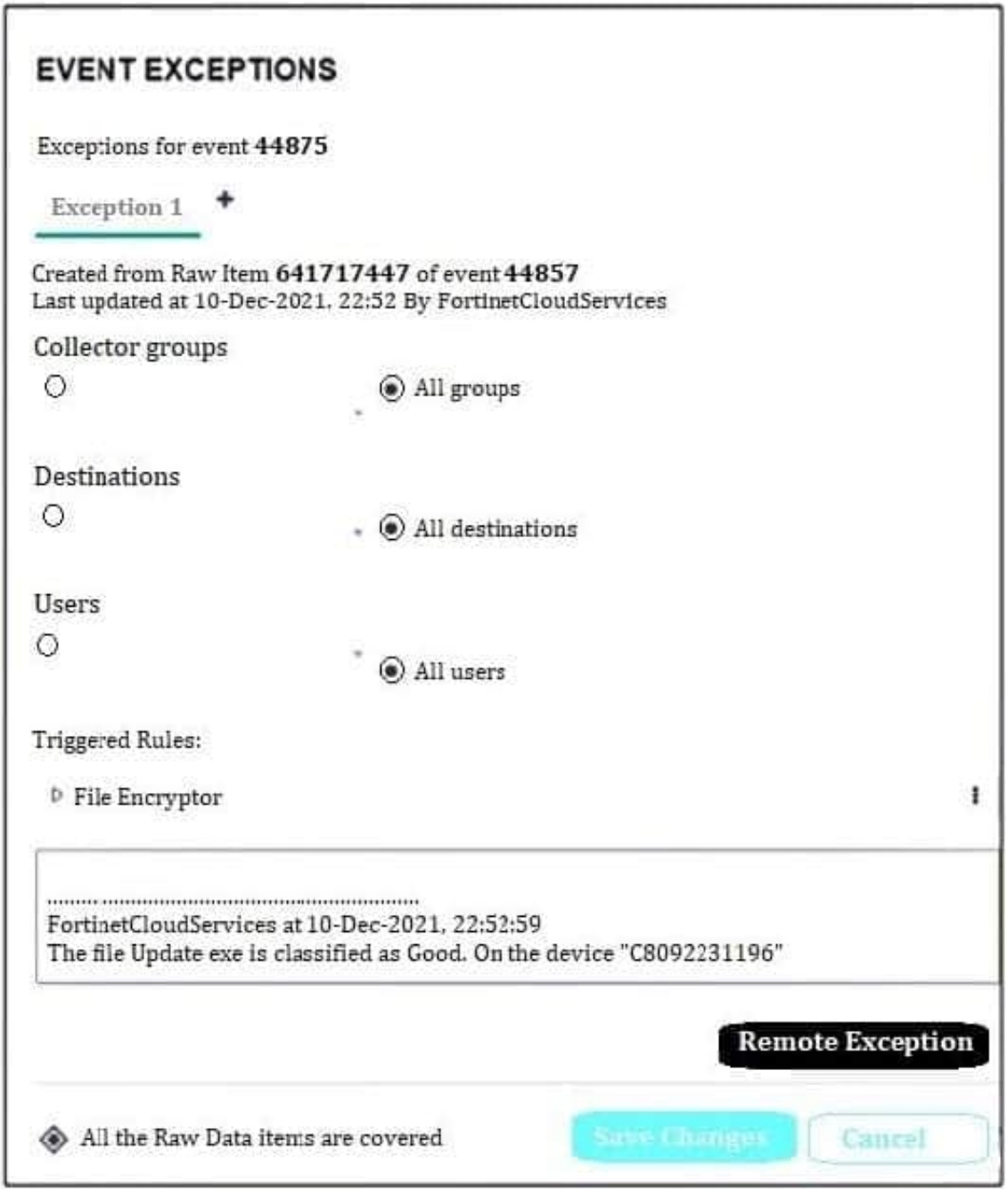
D. Execute playbooks to isolate affected collectors in the organization

Correct Answer: B

"Threat hunting allows management console users to find and remediate dormant threats before they execute. Essentially it\\'s a search and destroy operation."

QUESTION 6

Refer to the exhibit.



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: AC

QUESTION 7

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
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


TestApplication.exe.exe (3 events)
Malicious
5894314
R2D2-kvm63
TestApplication.exe.exe
Malicious
Logged-in User:
Process owner:
Certificate:
Process path:
R2D2-KVM63\fortinet
R2D2-KVM63\fortinet
Unsigned
C:\Users\fortinet\Desktc


15-Feb-2022, 13:31:39
8.8.8.8
15-Feb-2022, 13:31:39
15-Feb-2022, 13:31:39
CLASSIFICATION DETAILS
Malicious
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: BC

QUESTION 8

A company requires a global exception for a FortiEDR multi-tenant environment.

How can the administrator achieve this?

A. The local administrator can create a new exception and share it with other organizations.

B. A user account can create a new exception and share it with other organizations.

C. The administrator can create a new exception and assign it globally to all organizations.

D. The administrator can create a new exception policy for each organization hosted on FortiEDR.

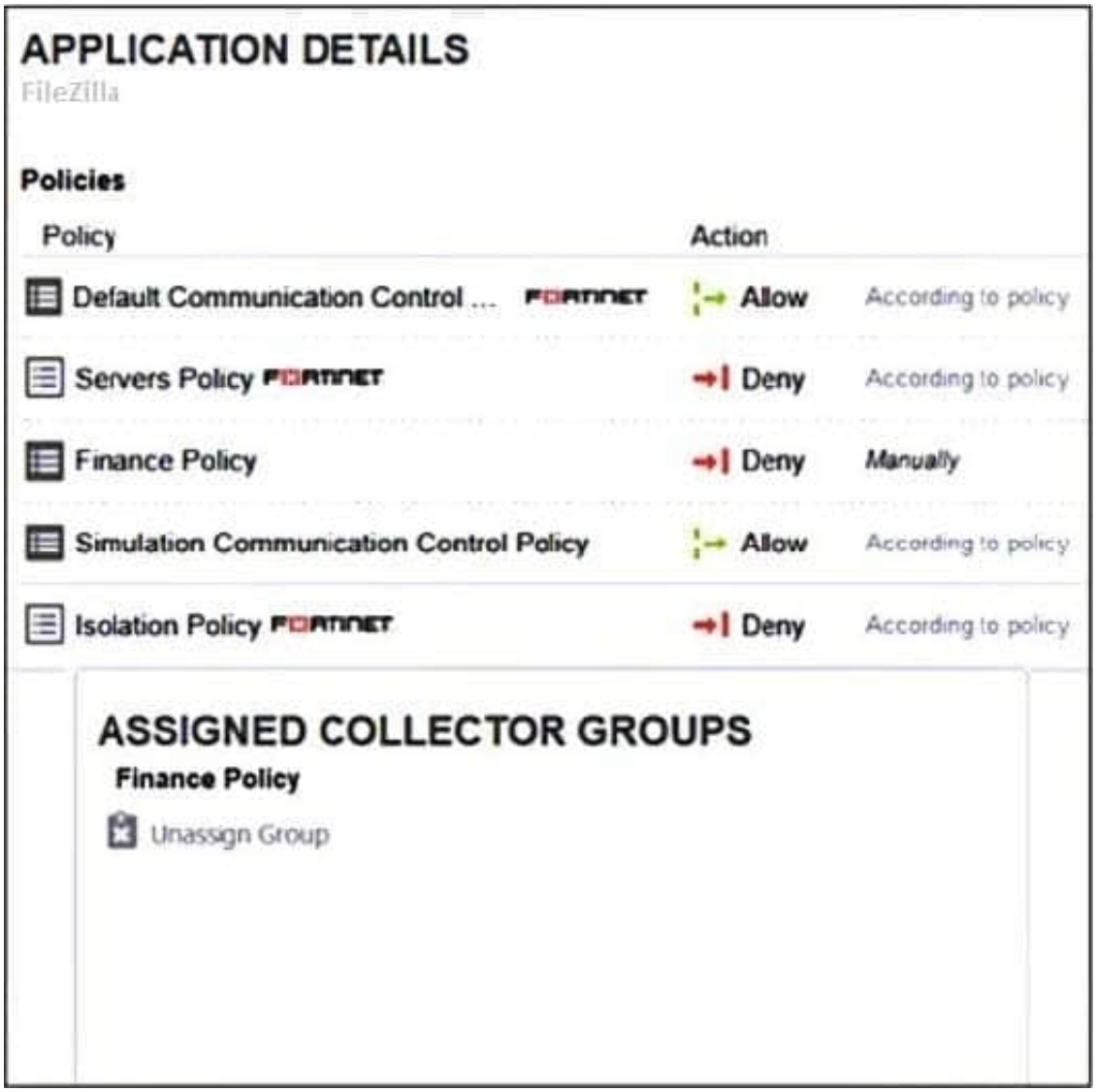
Correct Answer: C

Fortiedr AdminGuide "For a multi-organization FortiEDR system, an Administrator who is assigned to All organizations (see Users) can also specify whether the exception applies to all organizations. The All organizations option applies the exception to all organizations, regardless of whether or not the security event already occurred."

QUESTION 9

Refer to the exhibits.


APPLICATIONS
All
Mark As
Delete
Modify Action
Advanced Filter
Export
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)



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: B

QUESTION 10

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

A. Playbooks

B. Security Policies

C. Forensic

D. Communication Control

Correct Answer: A