Free Questions for NSE5_EDR-5.0

Shared by Madden on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How does FortiEDR implement post-infection protection?

Options:

A- By preventing data exfiltration or encryption even after a breach occurs

B- By using methods used by traditional EDR

C- By insurance against ransomware

D- By real-time filtering to prevent malware from executing

Answer:

D

Question 2

Question Type: MultipleChoice

What is the purpose of the Threat Hunting feature?

Options:

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

Answer:

C

Question 3

Question Type: **MultipleChoice**

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

How can the administrator achieve this?

Options:

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

Question 4

Question Type: **MultipleChoice**

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

Options:

A- It provides pre-infection and post-infection protection

B- It is Windows OS only

C- It provides central management

D- It provides pant-to-point protection

Answer:

A, D

Question 5

Question Type: MultipleChoice

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

Options:

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

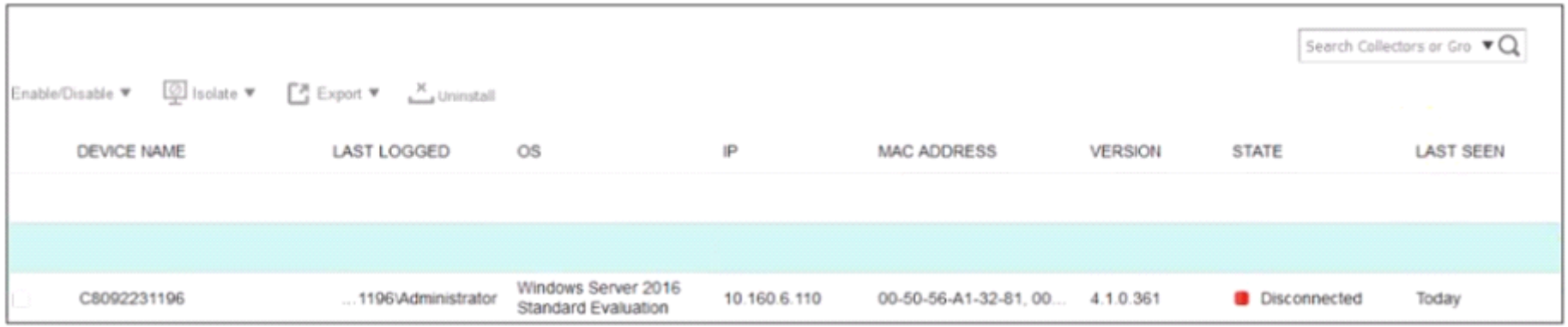
Answer:

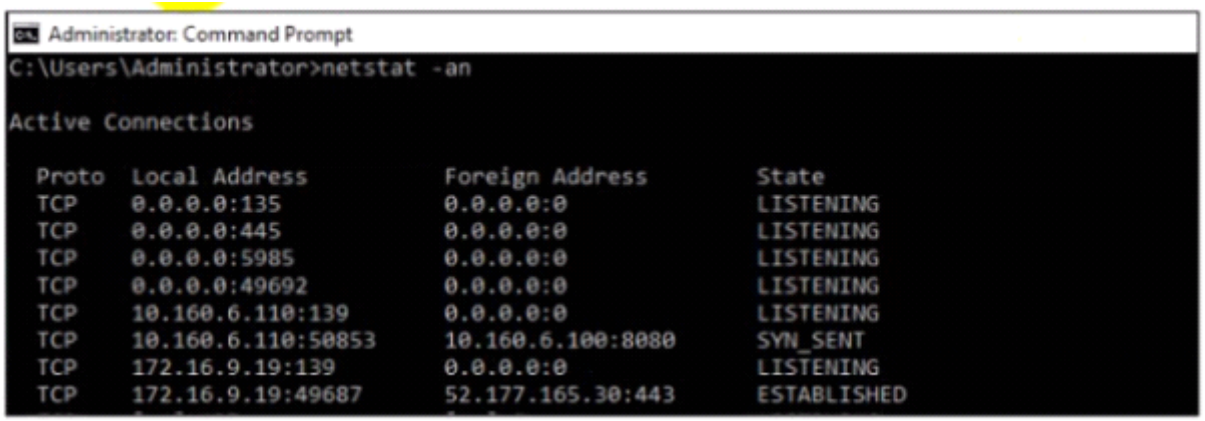
A

Question 6

Question Type: MultipleChoice

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?

Options:

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

Answer:

B

Question 7

Question Type: MultipleChoice

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

Options:

A- Device Control

B- Ransomware Prevention

C- Execution Prevention

D- Exfiltration Prevention

Answer:

B

Question 8

Question Type: MultipleChoice

Exhibit.

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

Options:

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:

B, C

Question 9

Question Type: MultipleChoice

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

Options:

A- FortiEDR Aggregator

B- FortiEDR Central Manager

C- FortiEDR Threat Hunting Repository

D- FortiEDR Core

Answer:

A