



Free Questions for NSE5_EDR-5.0 by certscare

Shared by Jacobson on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibits.

APPLICATIONS						
All	▼	Mark As ... ▼	Delete	Modify Action	Advanced Filter	Export ▼
<input type="checkbox"/>	APPLICATION		VENDOR	REPUTATION	VULNERABILITY	
▼ <input type="checkbox"/>	<input checked="" type="checkbox"/> FileZilla	Signed	Tim Kosse	Unknown	Unknown	
	<input type="checkbox"/> 3.50.0			Unknown	Unknown	
▶ <input type="checkbox"/>	<input checked="" type="checkbox"/> FileZilla	Signed	FileZilla Project	Unknown	Unknown	
<input type="checkbox"/>	COLLECTOR GROUP NAME				DEVICE NAME	
▶ <input type="checkbox"/>	<input checked="" type="checkbox"/> High Security Collector Group (1/1)					
▼ <input type="checkbox"/>	<input checked="" type="checkbox"/> DBA (1/1)					
				<input type="checkbox"/>	C8092231196	
▶ <input type="checkbox"/>	<input checked="" type="checkbox"/> Default Collector Group (0/0)					

APPLICATION DETAILS
FileZilla

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 FileZilla application?

Options:

- 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

Answer:

D

Question 2

Question Type: MultipleChoice

Refer to the exhibits.

DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
<input type="checkbox"/> 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?

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 3

Question Type: MultipleChoice

Refer to the exhibit.

The screenshot shows a Windows Security event log entry for a malicious process. The event details are as follows:

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

CLASSIFICATION DETAILS

- Malicious **runner**
- 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.)

Options:

- 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:

A, B

Question 4

Question Type: MultipleChoice

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?

Options:

- A- Admin
- B- User
- C- Local Admin
- D- REST API

Answer:

C

Question 5

Question Type: MultipleChoice


Exhibit.

CLASSIFICATION DETAILS

 Malicious 

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.)

Options:

- 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

Answer:

B, D

Question 6

Question Type: MultipleChoice

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

Options:

- 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

Answer:

C

Question 7

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

To Get Premium Files for NSE5_EDR-5.0 Visit

https://www.p2pexams.com/products/nse5_edr-5.0

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/nse5-edr-5.0>

