

VCEup

Exam Code: NSE5_EDR-5.0

Exam Name: Fortinet NSE 5 - FortiEDR 5.0

Website: <https://VCEup.com/>

Team-Support: <https://VCEplus.io/>



Question No: 1

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

Answer: C

Explanation:

Question No: 2

How does FortiEDR implement post-infection protection?

- 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

Explanation:

Question No: 3

Exhibit.



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.

Answer: B, C

Explanation:

Question No: 4

www.VCEplus.io

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

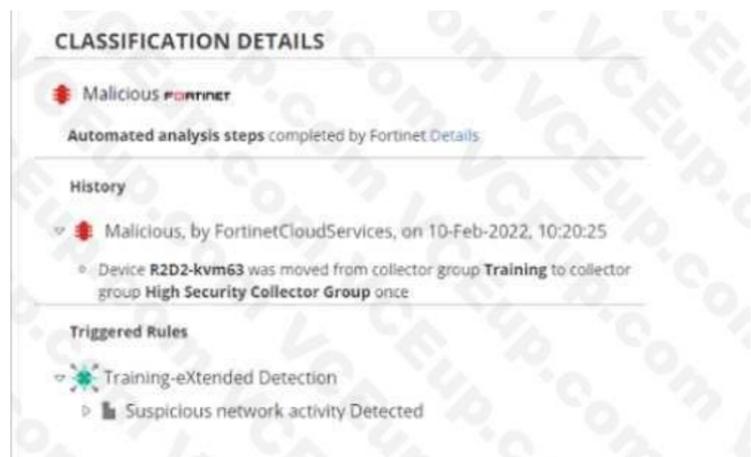
- A. It helps to make sure the hash is really a malware
- B. It helps to check the malware even if the malware variant uses a different file name
- C. It helps to find if some instances of the hash are actually associated with a different file
- D. It helps locate a file as threat hunting only allows hash search

Answer: C

Explanation:

Question No: 5

Exhibit.



www.VCEplus.io

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

Answer: B, D

Explanation:

Question No: 6

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

Answer: C

Explanation:

Question No: 7

Refer to the exhibit.



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

Answer: A, B

Explanation:

Question No: 8

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

www.VCEplus.io

```

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:*               LISTENING
TCP   0.0.0.0:445             0.0.0.0:*               LISTENING
TCP   0.0.0.0:5985            0.0.0.0:*               LISTENING
TCP   0.0.0.0:49692           0.0.0.0:*               LISTENING
TCP   10.160.6.110:139        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:*               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

Answer: B

Explanation:

Question No: 9

Refer to the exhibits.

www.VCEplus.io

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)				



The screenshot shows the 'APPLICATION DETAILS' interface. It is divided into two main sections: 'Policies' and 'ASSIGNED COLLECTOR GROUPS'.

Policies

Policy	Action	Reason
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

Answer: D

Explanation:

Question No: 10

Refer to the exhibit.

www.VCEplus.io



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

Answer: B

Explanation:

Question No: 11

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

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

Answer: B, C

Explanation:

Question No: 12

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

www.VCEplus.io

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

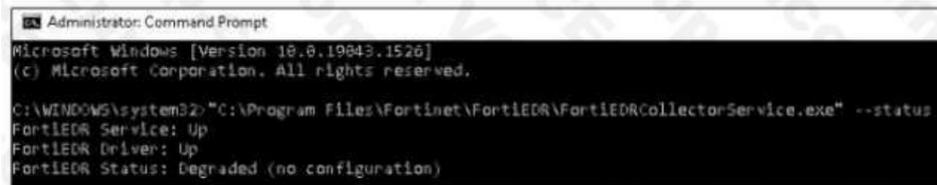
D. FCS is responsible for all classifications

Answer: C

Explanation:

Question No: 13

Refer to the exhibit.



```
Administrator: Command Prompt
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

Answer: B, D

Explanation:

Question No: 14

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

Answer: C

Explanation:

Question No: 15

Refer to the exhibit.

www.VCEplus.io



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

Answer: A, C

Explanation:

Question No: 16

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.

Answer: B, C

Explanation:

Question No: 17

Exhibit.



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 in the stacks view
- C. The device has been isolated
- D. The exfiltration prevention policy has blocked this event

Answer: C, D

Explanation:

Question No: 18

The FortiEDR axe classified an event as inconclusive, but a few seconds later FCS revised the classification to malicious. What playbook actions were 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

Answer: D

Explanation:

Question No: 19

Which threat hunting profile is the most resource intensive?

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

Answer: A

Explanation:

Question No: 20

Which two types of remote authentication does the FortiEDR management console support?

(Choose two.)

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

Answer: A, D

Explanation:

Question No: 21

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

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

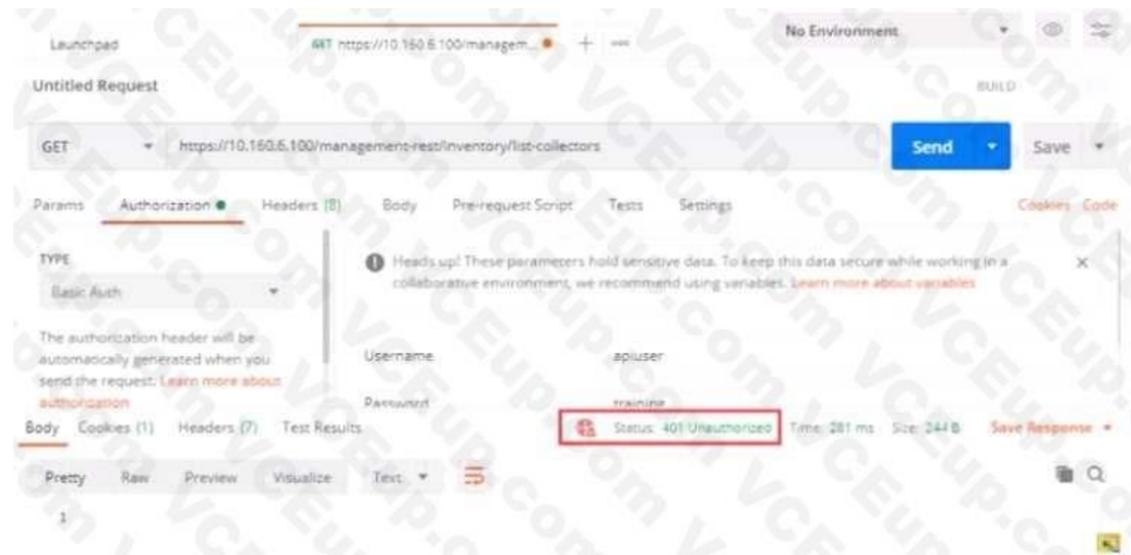
Answer: B

Explanation:

Question No: 22

Refer to the exhibit.

www.VCEplus.io



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

Answer: A

Explanation:

Question No: 23

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

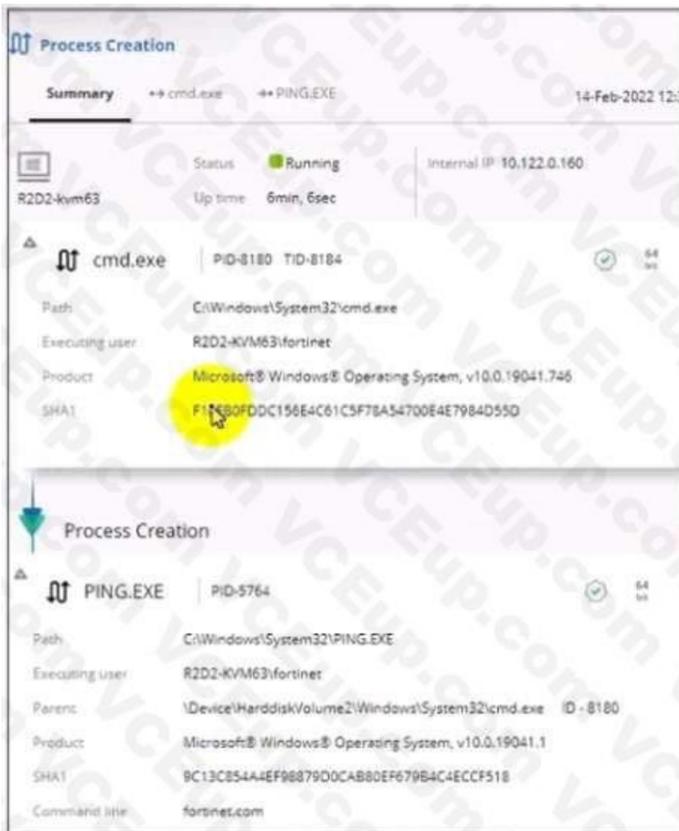
- A. A collector blocks unsafe applications from running
- B. A collector is used to change the reputation score of any application that collector runs
- C. A collector records applications that communicate externally
- D. A collector can quarantine unsafe applications from communicating

Answer: A

Explanation:

Question No: 24

Refer to the exhibit.



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

www.VCEplus.io

- C. The activity event is associated with the file action
- D. There are no MITRE details available for this event

Answer: A, D

Explanation:

Question No: 25

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 ignored as the reputation score is acceptable by the security policy
- C. The application has not made any connection attempts
- D. The application is blocked by the security policies

Answer: A, D

Explanation:

Question No: 26

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

Answer: C

Explanation:

Question No: 27

Which scripting language is supported by the FortiEDR action manager?

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

Answer: A

Explanation:

Question No: 28

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

- A. FortiEDR Aggregator

www.VCEplus.io

- B. FortiEDR Central Manager
- C. FortiEDR Threat Hunting Repository
- D. FortiEDR Core

Answer: A

Explanation:

Question No: 29

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

- A. Device Control
- B. Ransomware Prevention
- C. Execution Prevention
- D. Exfiltration Prevention

Answer: B

Explanation:

Question No: 30

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

- A. It provides pre-infection and post-infection protection
- B. It is Windows OS only
- C. It provides central management
- D. It provides point-to-point protection

Answer: A, D

Explanation:

www.VCEplus.io