KillTest

更に上のクオリティ　更に上のサービス

問題集

http://www.killtest.jp

1年で無料進級することに提供する

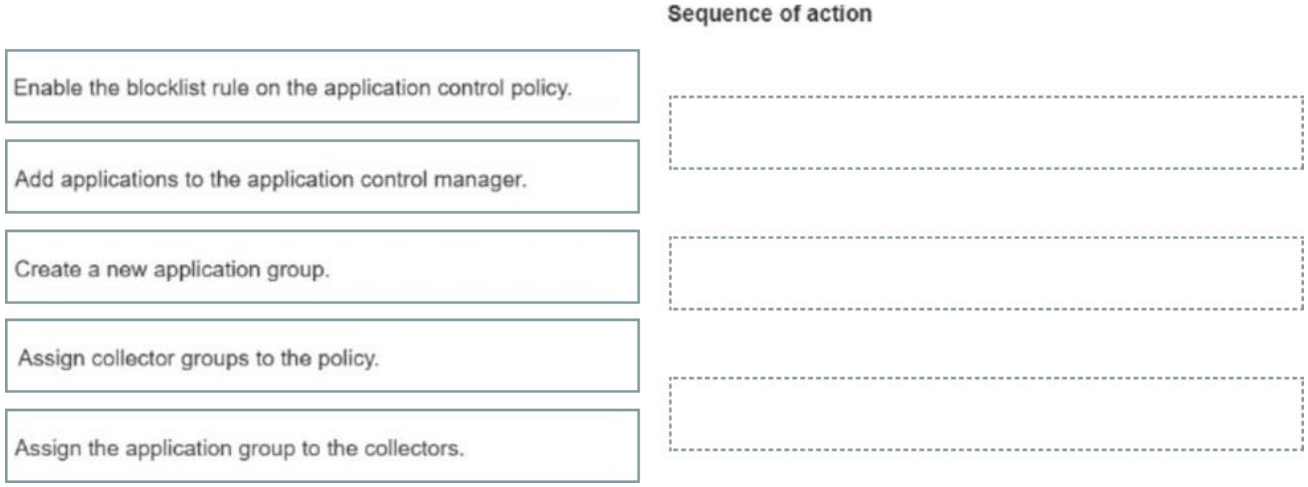
Exam : **NSE6_EDR_AD-7.0**

Title : Fortinet NSE 6 - FortiEDR 7.0 Administrator

Version : DEMO

1.You discovered that a newly installed collector does not display on the Inventory tab in the central manager.
Which two troubleshooting steps must you perform? (Choose two.)
A. Check whether the FortiEDR services are running on the collector device.
B. Verify that the central manager can resolve the collector hostname through DNS.
C. Export and review the collector logs from the Central Manager for connection errors.
D. Verify that TCP ports 8081 and 555 are open between the collector and the central manager.
Answer: A, D
Explanation:
The collector must have FortiEDR services running to establish communication with the central manager. If the services are not running, the collector cannot register or appear in the Inventory tab.
Communication between the collector and the central manager also requires specific ports to be open, including TCP ports 8081 and 555, which are used for management and communication between the components.

2.When implementing an application block policy in FortiEDR, which three actions, in order, reflect the correct operational sequence?
Select an action in the left column and hold and drag it to a blank position in the column on the right. Place the three correct actions in order, starting with the first action at the top of the column. After you place an action, you can move it again if you want to change your answer before proceeding to the next question. You must drop three actions in the work area.
Select and drag the screen divider to change the viewable area of the source and work areas.



Answer:

	Sequence of action
Enable the blocklist rule on the application control policy.	Add applications to the application control manager.
Add applications to the application control manager.	Create a new application group.
Create a new application group.	Enable the blocklist rule on the application control policy.
Assign collector groups to the policy.	
Assign the application group to the collectors.	

Explanation:

Add applications to the application control manager.

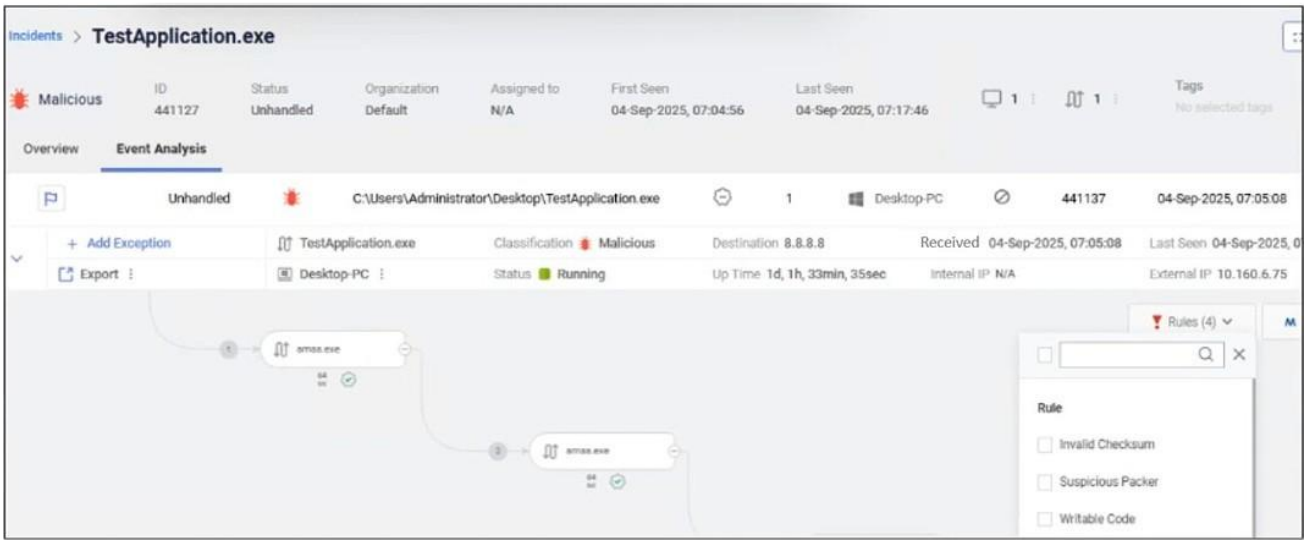
Create a new application group.

Enable the blocklist rule on the application control policy.

To implement an application block policy, the applications must first be defined in the application control manager so FortiEDR can identify them. After defining the applications, they are organized into an application group that can be referenced by policies. Finally, the blocklist rule is enabled in the application control policy to enforce blocking of the defined applications on endpoints.

3.Refer to the exhibit.

Event



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

A. The user was able to launch TestApplication.exe

B. The event is marked as Handled.

C. FCS classified the event as malicious.

D TestApplication.exe is sophisticated malware.

Answer: A,C

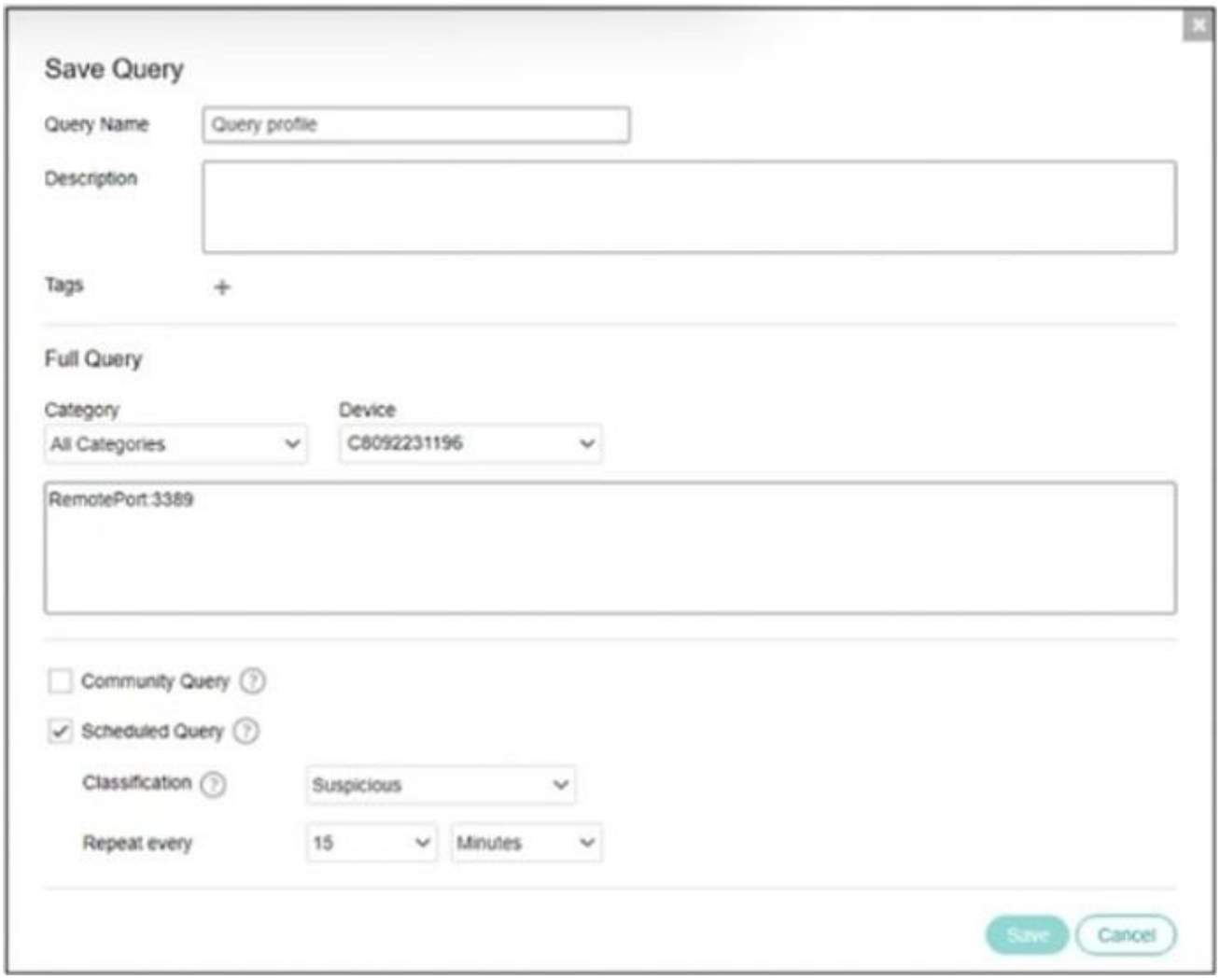
Explanation:

The event view shows the process TestApplication.exe with status Running, indicating the application

was successfully launched on the endpoint. The classification label indicates the event is marked as malicious and the classification source is FortinetCloud Services, confirming that FCS performed the malicious classification.

4.Refer to the exhibit.

Threat hunting query



Based on the exhibit, which statement about this treat hunting query is true?

A. RDP connections will be automatically blocked and classified as suspicious.

B. A security incident will be generated whenever the device attempts an RDP connection.

C. The query is limited to detecting network activity and does not inspect process behavior.

D. The query is configured as a global hunting rule and is automatically visible across all organizations.

Answer: B

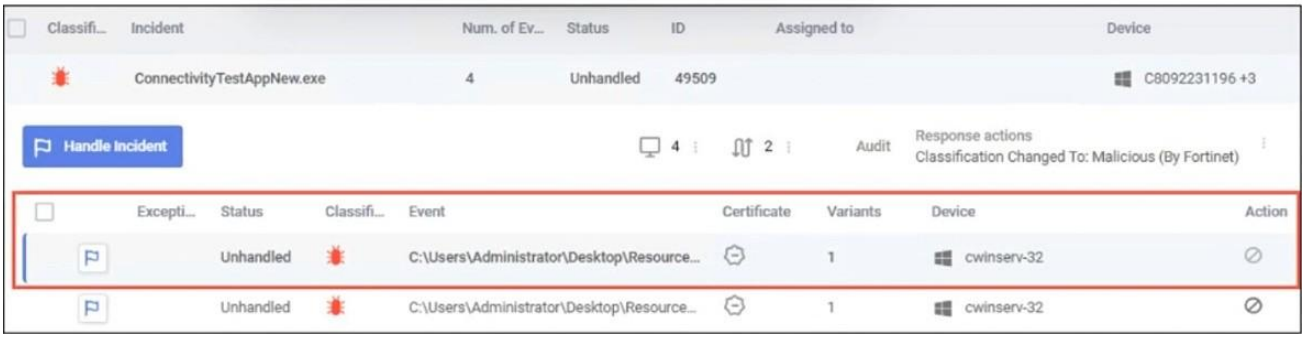
Explanation:

The query searches for network activity where the remote port is 3389, which corresponds to RDP traffic. The query is configured as a scheduled threat hunting query with a suspicious classification and runs repeatedly at a defined interval.

When the query condition is matched, FortiEDR generates a security event for that activity, resulting in a security incident being created when the device attempts an RDP connection.

5.Refer to the exhibit.

ConnectivityTestAppNew.exe Incident



What observation can you make about the Connectivity TestAppNew.exe incident?

A. The incident was archived from the console unhandled.

B. A rule assigned action is set to block but the policy is in simulation mode.

C. The incident was handled automatically by the communication control policy.

D. The incident has not been handled by a console administrator.

Answer: D

Explanation:

The incident status in the incident handler view is clearly marked as Unhandled. This indicates that no console administrator has taken action to investigate, resolve, or close the incident from the FortiEDR management console.