DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Fortinet

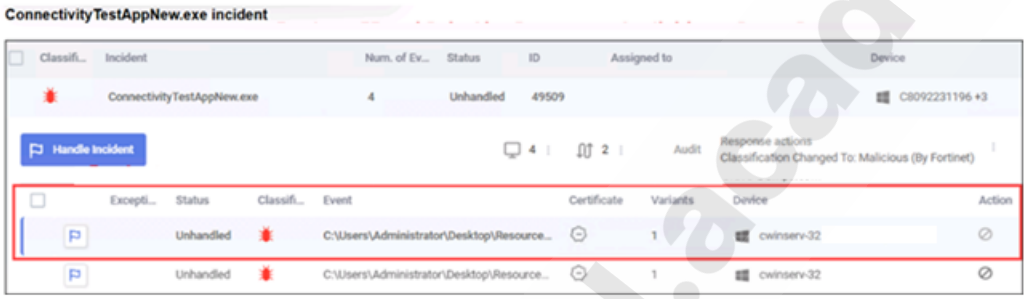
Exam: Fortinet NSE 6 - FortiEDR 7.0 Administrator

Number of questions in the database: 34

Exam Version: NOV.2026

Question #1Topic 1

Refer to the exhibit.



What observation can you make about the ConnectivityTestAppNew.exe incident?

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

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

C. The incident was archived from the console unhandled.

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

Correct Answer: B

https://dbcloud.academy/

Question #2Topic 1

Refer to the Exhibit:



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

A. An exception was created for this incident.

B. The exfiltration prevention policy blocked this event.

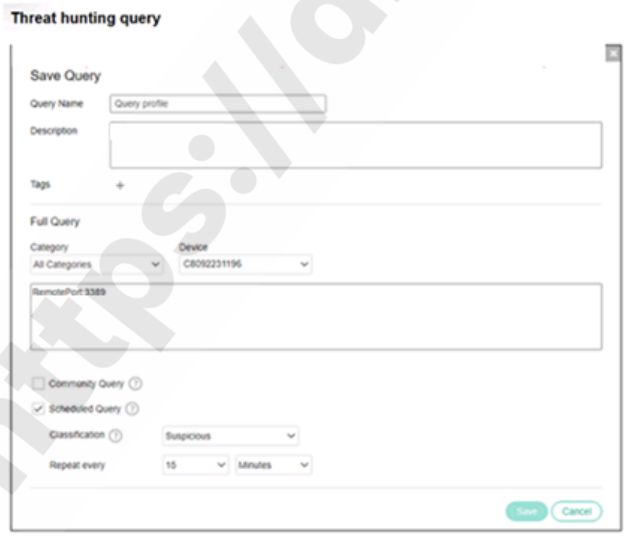
C. The raw data is displayed in the stacks view.

D. The device has been isolated.

Correct Answer: AC

Question #3Topic 1

Refer to the exhibit.



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

https://dbcloud.academy/

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

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

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

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

Correct Answer: A

Question #4Topic 1

Which two Python commands are supported when using FortiEDR Connect to directly access a protected device shell? (Choose two answers)

A. %upload_file

B. %ipconfig_all

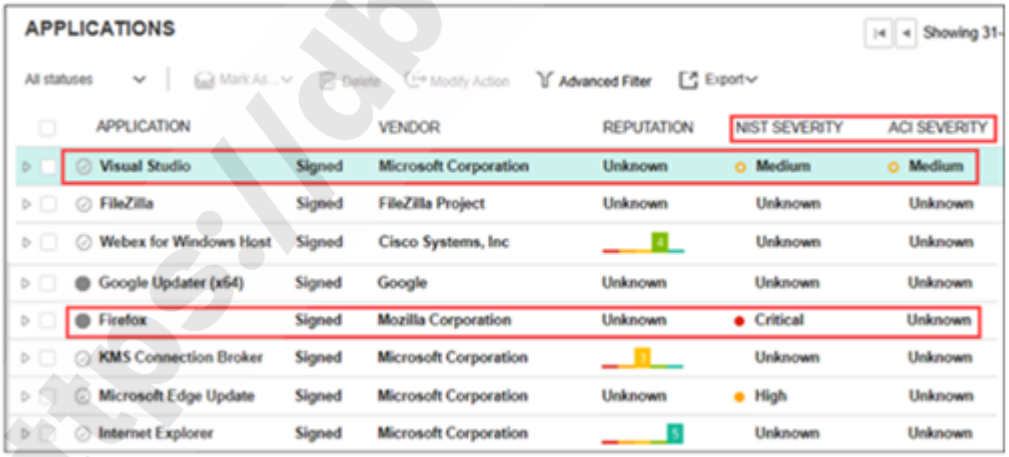
C. %psexec

D. %timestamp

Correct Answer: AB

Question #5Topic 1

Refer to the Exhibit:



A FortiEDR analyst is prioritizing response efforts. One application has a vulnerability score of Critical but an Unknown ACI rating, while another has a Medium vulnerability score with active ACI evidence of adversary targeting. Which application must be addressed first?

A. Both applications should be treated equally because patching is necessary.

https://dbcloud.academy/

B. The application with the Critical vulnerability score should be addressed first.

C. The decision depends only on asset criticality, not scores.

D. The application with the Medium vulnerability score and ACI evidence should be addressed first.

Correct Answer: D

Question #6Topic 1

A company requires a global communication policy for a FortiEDR multi-tenant environment. Which recommendation must you make? (Choose one answer)

A. Create a separate communication control policy for each organization.

B. Create a new communication control policy and apply it to multiple organizations.

C. Create a new communication control policy and delegate it to other organizations.

D. Create a new communication control policy and assign it globally to all organizations.

Correct Answer: A

Question #7Topic 1

A playbook is configured with two actions: terminate process and isolate device. The terminate process action fails because the process is protected by Windows. What is the expected behavior for the second action, isolate device? (Choose one answer)

A. The playbook execution pauses and requires administrator intervention.

B. The playbook generates a notification email and execution stops.

C. The playbook execution stops because the action fails.

D. The playbook continues and executes the second action.

Correct Answer: D

Question #8Topic 1

Which two statements correctly describe the IoT probing process on FortiEDR? (Choose two.)

A. Collectors running on servers are always used for IoT probing.

B. It identifies nearby devices by retrieving details such as hostname and IP address.

C. Only healthy collectors participate in IoT probing.

D. It captures all traffic from neighboring devices for deep packet inspection.

Correct Answer: BC

https://dbcloud.academy/