DBCLOUD
EXAMS

# QUESTIONS & ANSWERS

verified



**Technology Provider:** Fortinet

**Exam:** Fortinet NSE 6 - FortiSIEM 7.4 Analyst

**Number of questions in the database:** 63

**Exam Version:** NOV.2026

Question #1Topic 1

Which data collection method generates the most comprehensive information for FortiSIEM user entity and behavior analytics (UEBA) models?

A. FortiSIEM Linux agent

B. Windows UEBA agent

C. Windows Sysmon

D. Linux log

**Correct Answer: B**

Question #2Topic 1

When selecting multiple rules at once on FortiSIEM, which actions can you perform?

A. You can change the severity, activate, or deactivate multiple rules at a time.

B. You can view, edit, or activate only one rule at a time

C. You can only activate or deactivate multiple rules at a time.

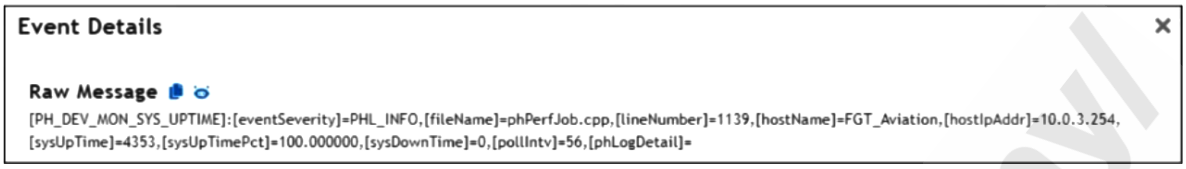
D. You can only change the severity of multiple rules at a time.

**Correct Answer: A**

https://dbcloud.academy/

Question #3*Topic 1*

Refer to the exhibit.




Which event type attribute value will the FortiSIEM parser save for this event?

A. sysUpTime

B. PH_DEV_MON_SYS_UPTIME

C. phLogDetail

D. PHL_INFO

**Correct Answer: B**

Question #4*Topic 1*

Refer to the exhibit.

| Source IP | Reporting Device | Reporting IP | Event Type | User | Count |
|---|---|---|---|---|---|
| 15.2.3.4 | FW01 | 10.1.1.1 | Logon | Mike | 4 |
| 21.3.4.5 | FW01 | 10.1.1.1 | Logon | Bob | 3 |
| 14.12.3.1 | FW01 | 10.1.1.1 | Logon | Alice | 2 |
| 192.168.1.5 | FW01 | 10.1.1.1 | Logon | Alice | 2 |
| 10.1.1.1 | FW01 | 10.1.1.1 | Logon | Bob | 6 |
| 123.123.1.1 | FW01 | 10.1.1.1 | Logon | Mike | 5 |

If you group these events by the Reporting IP, Event Type, and User attributes, how many results will FortiSIEM display?

A. Five

B. Two

C. Six

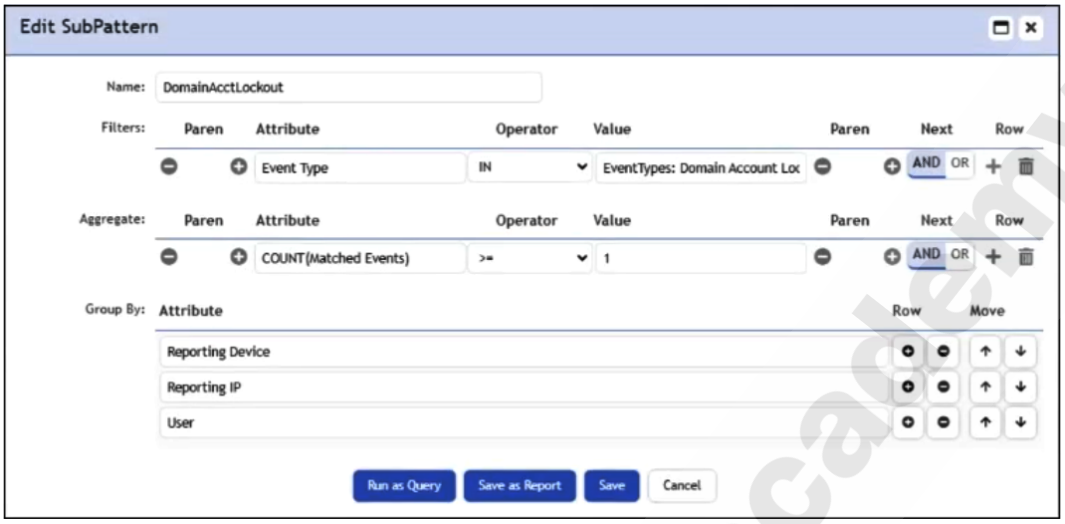
D. Three

**Correct Answer: D**

https://dbcloud.academy/

Question #5*Topic 1*

Refer to the exhibit.




Which two items can be referenced in the incident details when this rule is triggered and creates an incident? (Choose two.)

A. User

B. Reporting Device

C. Domain Account Lockout

D. Event Type

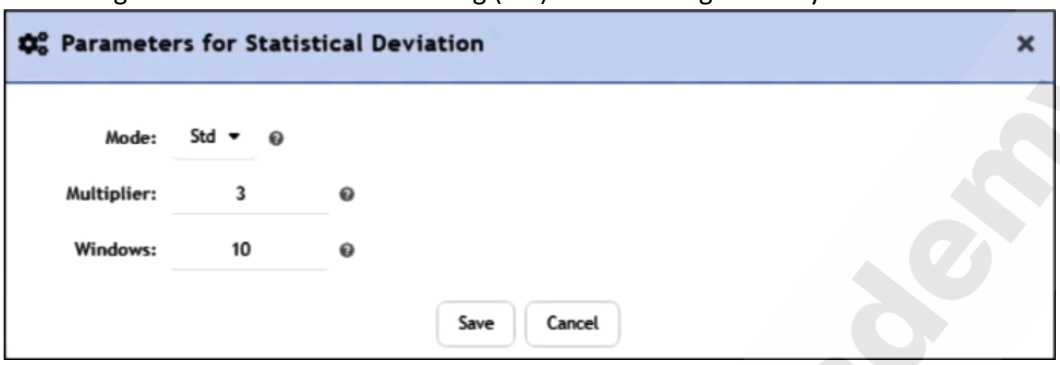
E. COUNT(Matched Events)

**Correct Answer: AB**

https://dbcloud.academy/

Question #6*Topic 1*

Refer to the exhibit.
The configuration for a machine learning (ML) dataset using anomaly detection is shown.




If data for this model is generated every hour, how long must the FortiSIEM device be up before it can produce a valid training set?

A. 3 hours

B. 10 hours

C. 24 hours

D. 30 hours

**Correct Answer: B**

Question #7Topic 1

Several new internal servers are generating incidents and must be excluded from several FortiSIEM rules.

How must you tune rules to exclude several undiscovered devices from rules?

A. Add the devices to a rule exclusion automation policy.

B. Add their associated discovery credentials.

C. Add them to the global exclusion list.

D. Add them to a device group that is being filtered by the rules.

**Correct Answer: D**

https://dbcloud.academy/