KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **NSE6_FSM_AN-7.4**

Title : Fortinet NSE 6 - FortiSIEM 7.4 Analyst

Version : DEMO

1.Which statement about thresholds is true?
A. FortiSIEM uses fixed, hardcoded global and device thresholds for all performance metrics.
B. FortiSIEM uses only device thresholds for security metrics.
C. FortiSIEM uses global and per-device thresholds for performance metrics.
D. FortiSIEM uses only global thresholds for performance metrics.
Answer: C
Explanation:
FortiSIEM supports both global thresholds and per-device/per-device-object thresholds for some performance events. The Study Guide states that FortiSIEM can define “per-device-object thresholds or global thresholds” for performance events, and separately explains that global thresholds are referenced by the rules engine by default.
Therefore, the correct statement is that FortiSIEM uses global and per-device thresholds for performance metrics.
Options A, B, and D are too restrictive or false because FortiSIEM does not use only one fixed threshold model.

2.Which run mode takes the most time to perform machine learning tasks?
A. Local Auto
B. Local
C. Forecasting
D. Regression
Answer: A
Explanation:
The correct answer is Local Auto. The uploaded answer was right, but its explanation was sloppy because it incorrectly described Local mode as the most time-consuming mode. In FortiSIEM machine learning, Local Auto mode selects the best algorithm by evaluating multiple candidate algorithms. The User Guide states that in Local Auto mode, “FortiSIEM picks the best algorithm” and that the Max Run Time parameter limits how long the job can run; longer runtime can produce better results. That is why Local Auto can take the most time. Forecasting and Regression are task types, not run modes.

3.Refer to the exhibit.

The analyst is troubleshooting the analytics query shown in the exhibit.
Why is this search not producing any results?

A. The Time Range is set incorrectly.
B. The inner and outer nested query attribute types do not match.
C. You cannot reference User and Event Type attributes in the same search.
D. The Boolean operator is wrong between the attributes.
Answer: B
Explanation:
The search fails because nested analytics queries require the outer query attribute type to match the inner query display-column data type. The FortiSIEM Study Guide explicitly explains this rule in the Nested Query section: “Another important aspect to understand is that the data value types must match.” It further explains that each inner query display column has a data value type, such as IP, string, or integer, and the outer query attribute must match that type. The FortiSIEM 7.4 User Guide states the same operational requirement: for a nested query to work correctly, “the data type of the filter attribute in the outer query must match up with the data type of one certain display column in the inner query.” Therefore, if the inner query returns a string attribute but the outer query compares it against an IP-type attribute, FortiSIEM cannot produce a valid match. The issue is not the time range, not the use of User and Event Type together, and not the Boolean operator. It is an attribute type mismatch between the query and subquery.

4.Refer to the exhibit.

Source IP	Reporting Device	Reporting IP	Event Type	User	Application Category
15.2.3.4	FW01	10.1.1.1	Logon	Mike	DB
21.3.4.5	FW02	10.1.1.2	Logon	Bob	WebApp
14.12.3.1	FW01	10.1.1.1	Logon	Alice	SSH
192.168.1.5	FW03	10.1.1.3	Logon	Alice	DB
10.1.1.1	FW01	10.1.1.1	Logon	Bob	DB
123.123.1.1	FW04	10.1.1.4	Logon	Mike	SSH

If you group the events by Reporting Device, Reporting IP, and Application Category, how many results will FortiSIEM display?
A. Four
B. Five
C. One
D. Six
E. Two
Answer: B
Explanation:
FortiSIEM grouping works by combining events that have the same values for all selected Group By attributes. The Study Guide’s rule and subpattern example states that when multiple events have the same Group By values, “they are grouped together in one row, and the count column tracks the number of events for each of those rows.” In the exhibit, the selected grouping fields are Reporting Device,

Reporting IP, and Application Category. The table contains six raw rows, but two rows share the same grouped combination: FW01 /10.1.1.1 /DB. Those two rows are collapsed into one grouped result. The other combinations are unique: FW02 /10.1.1.2 /WebApp, FW01 /10.1.1.1 /SSH, FW03 /10.1.1.3 /DB, and FW04 /10.1.1.4 /SSH. That creates five grouped rows in total. FortiSIEM does not display six because grouping removes duplicate combinations, and it does not display four because only one duplicate combination exists.

5.Which analytics search can be used to apply a user and entity behavior analytics (UEBA) tag to an event for a failed login by the user JSmith?
A. User = smith
B. Username NOT END WITH jsmith
C. User IS jsmith
D. Username CONTAIN smit
Answer: D
Explanation:
The best matching analytics search is Username CONTAIN smit. The FortiSIEM Analytics lesson explains keyword and attribute matching by using the CONTAIN operator for searching values inside raw logs or attributes. The Study Guide gives a direct example of FortiSIEM translating keyword logic into a condition such as “Raw Event Log CONTAIN TCP.” That shows the operator is designed for substring-style matching rather than full-value equality. For a user such as JSmith, the string fragment smit is contained inside the username value, so the condition can match events where the username appears as JSmith, jsmith, or possibly in a longer identity string such as a domain-qualified username.
Option A is wrong because smith is not the complete username and uses an equality-style comparison.
Option B is wrong because it excludes usernames ending in jsmith.
Option C uses the wrong operator form for this context.
Therefore, the practical FortiSIEM analytics condition that can match the target failed-login event is Username CONTAIN smit.