Fortinet

Exam Questions FCP_FSM_AN-7.2

FCP - FortiSIEM 7.2 Analyst

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

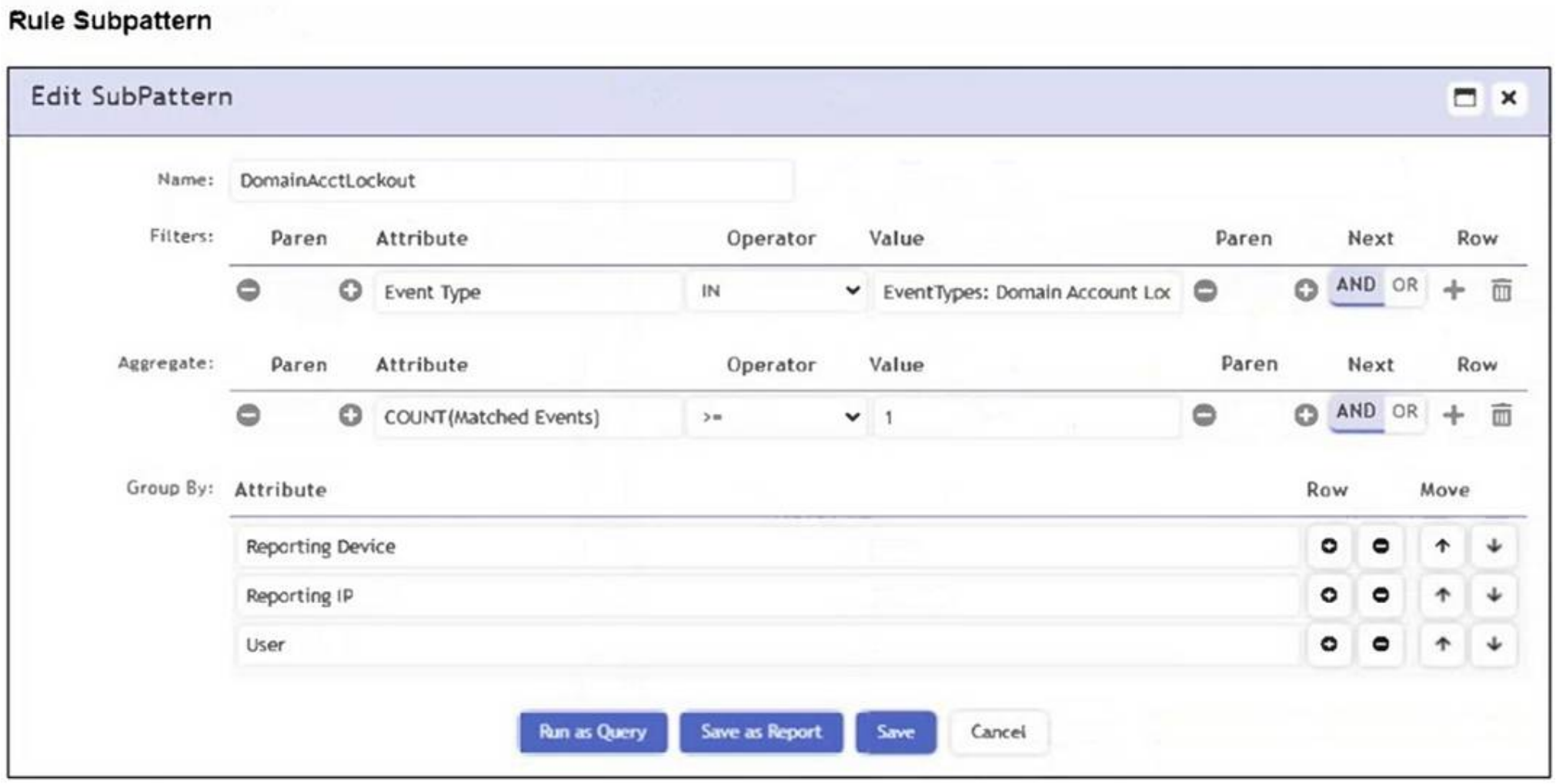
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Refer to the exhibit.

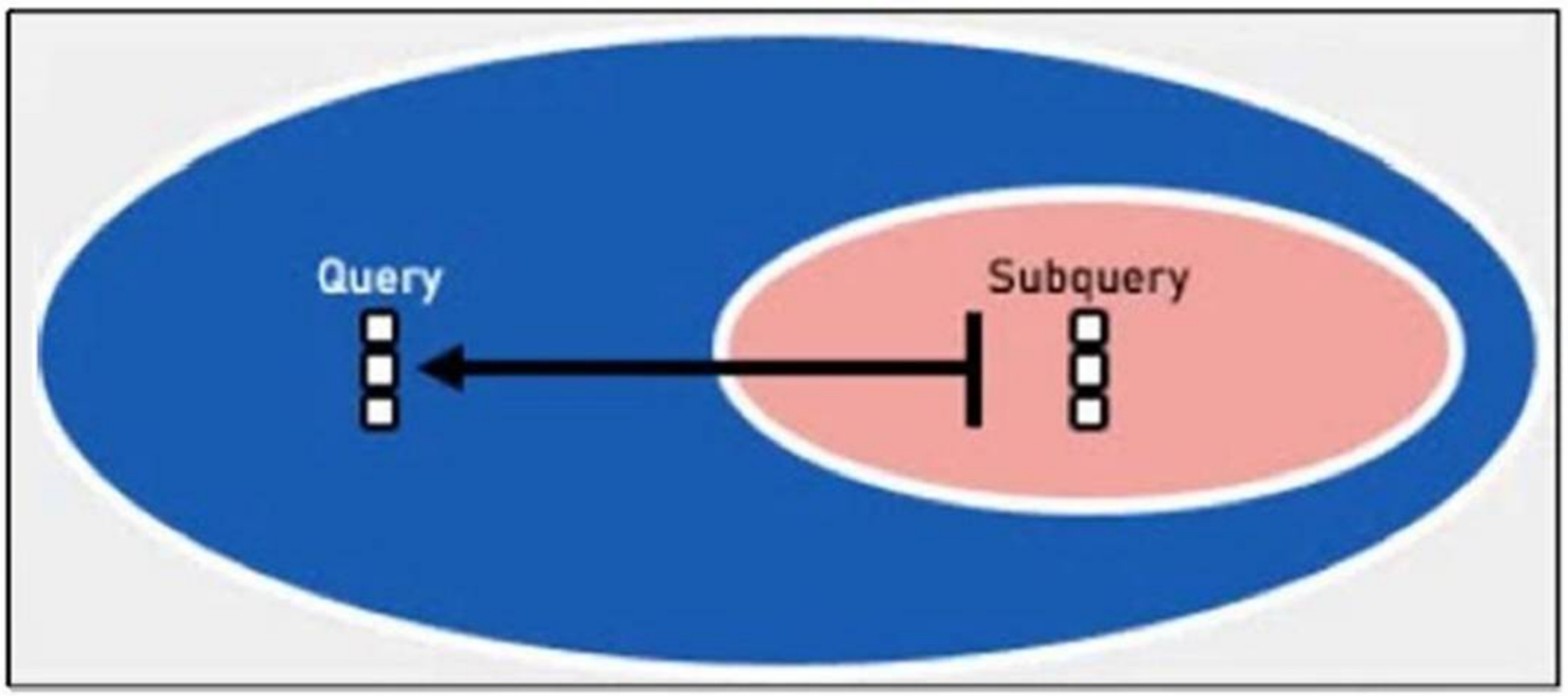


Which section contains the subpattern configuration that determines how many matching events are needed to trigger the rule?

A. Aggregate
B. Group By
C. Actions
D. Filters

Answer: A

NEW QUESTION 2
Refer to the exhibit.



Which two lookup types can you reference as the subquery in a nested analytics query? (Choose two.)

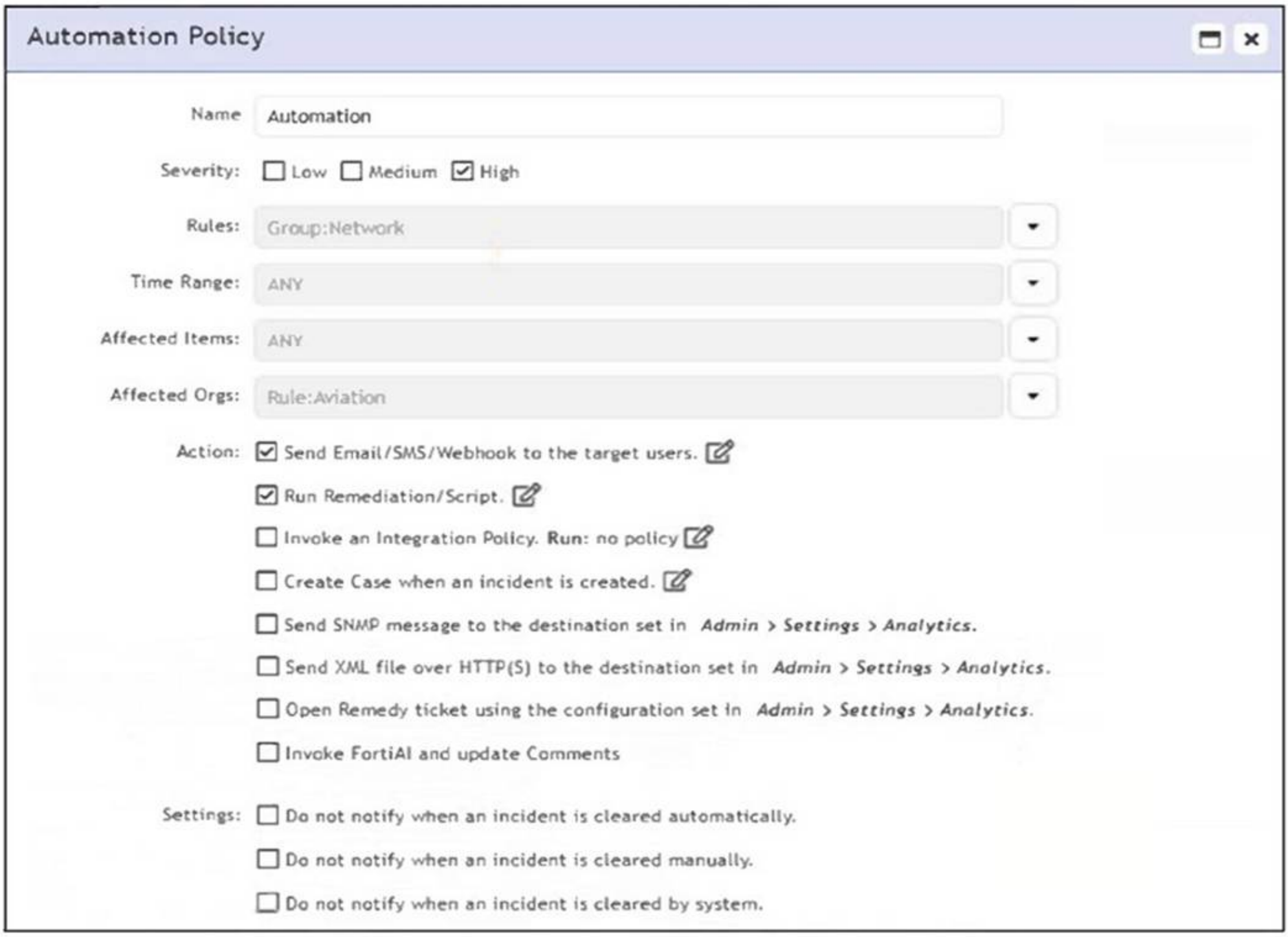
A. LDAP Query
B. CMDB Query
C. SNMP Query
D. Event Query

Answer: BD

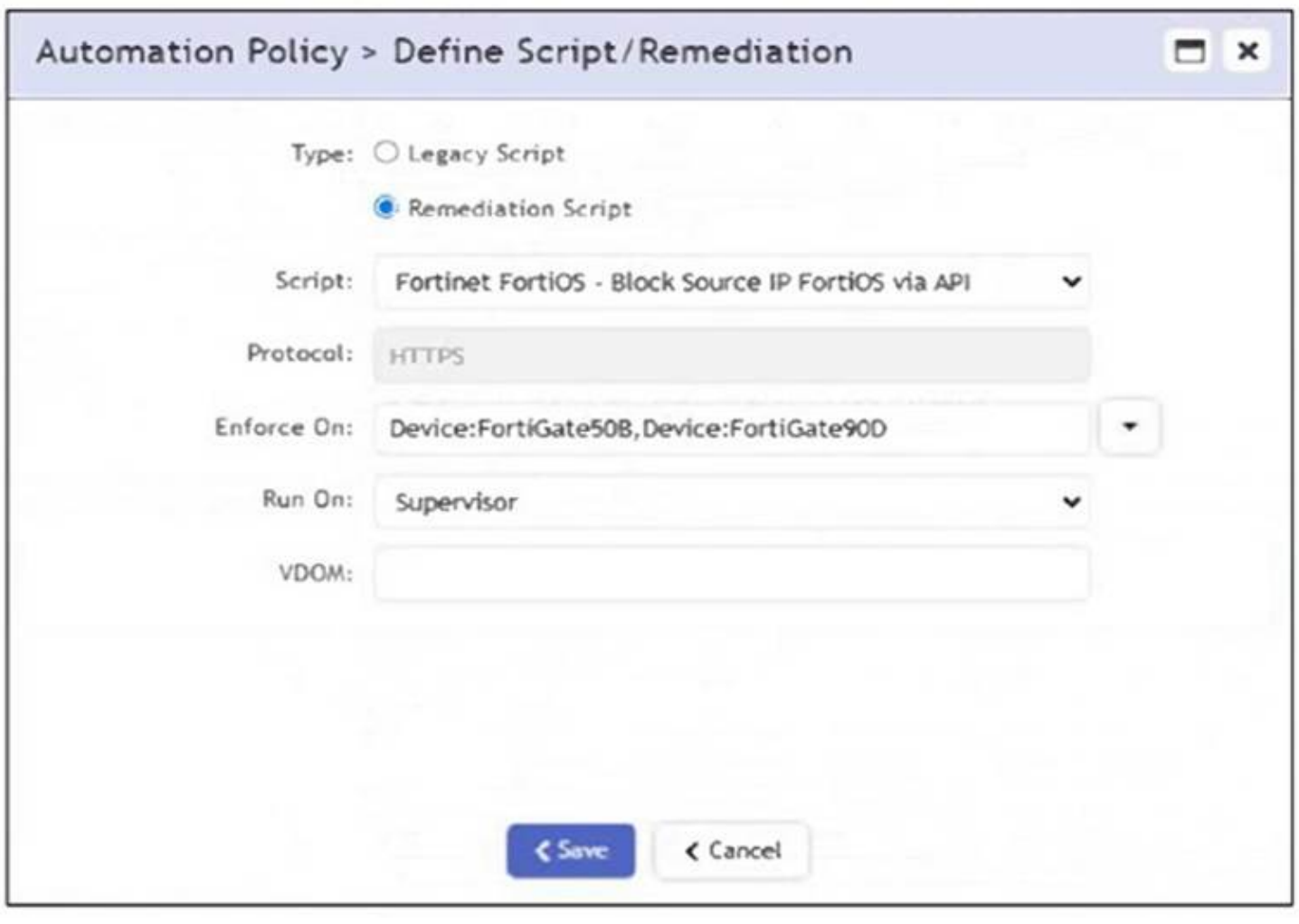
NEW QUESTION 3

Refer to the exhibit.

Automation Policy



Remediation/Script Options



If a rule containing the automation policy shown in the exhibit triggers, what will happen?

A. Associated source IP addresses will be blocked on devices in the Aviation organization.
B. Associated source IP addresses will be blocked on all FortiGate firewalls.

C. Associated source IP addresses will be blocked on devices in the Network CMDB group.
D. Associated source IP addresses will be blocked on two FortiGate firewalls.

Answer: D

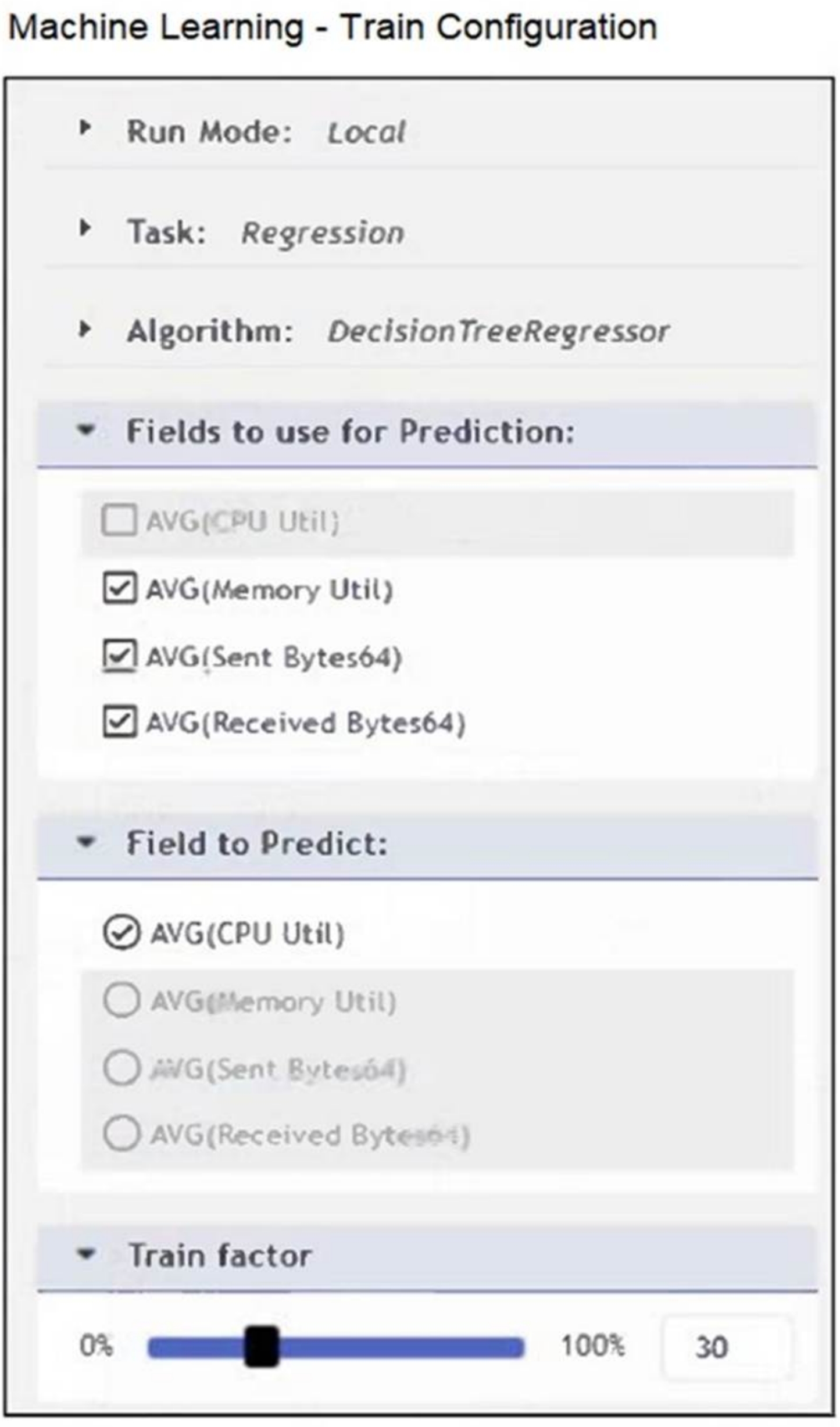
Explanation:
The automation policy is configured to run a remediation script named " Fortinet FortiOS - Block Source IP FortiOS via API " . It specifies enforcement on two FortiGate devices: FortiGate508 and FortiGate90D. Therefore, associated source IP addresses will be blocked on those two FortiGate firewalls only.

NEW QUESTION 4
What are two required components of a rule? (Choose two.)

A. Exception policy
B. Subpattern
C. Detection Technology
D. Clear policy

Answer: BC

NEW QUESTION 5
Refer to the exhibit.



The configuration shown in the exhibit is incorrect.
What must you change to allow this configuration to be successfully applied to FortiSIEM?

A. The Train factor must be 70% or greater.
B. Run Mode must be set to ML.
C. Only one AVG type field must be selected under Fields to use for Prediction.
D. The selection in Fields to use for Prediction and Field to Predict must match.

Answer: A

NEW QUESTION 6

Refer to the exhibit.

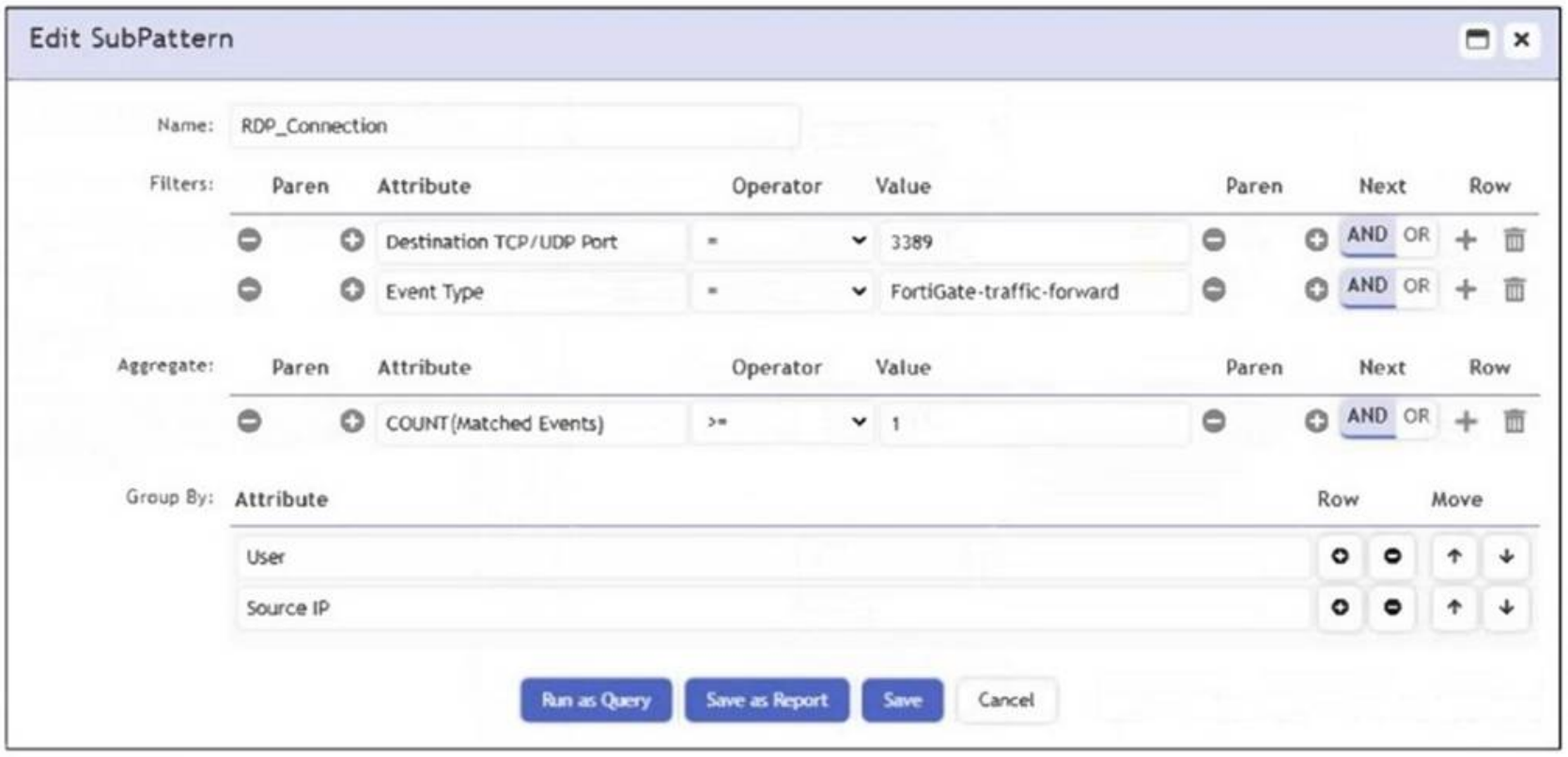
The analyst is troubleshooting the analytics query shown in the exhibit. Why is this search not producing any results?

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.

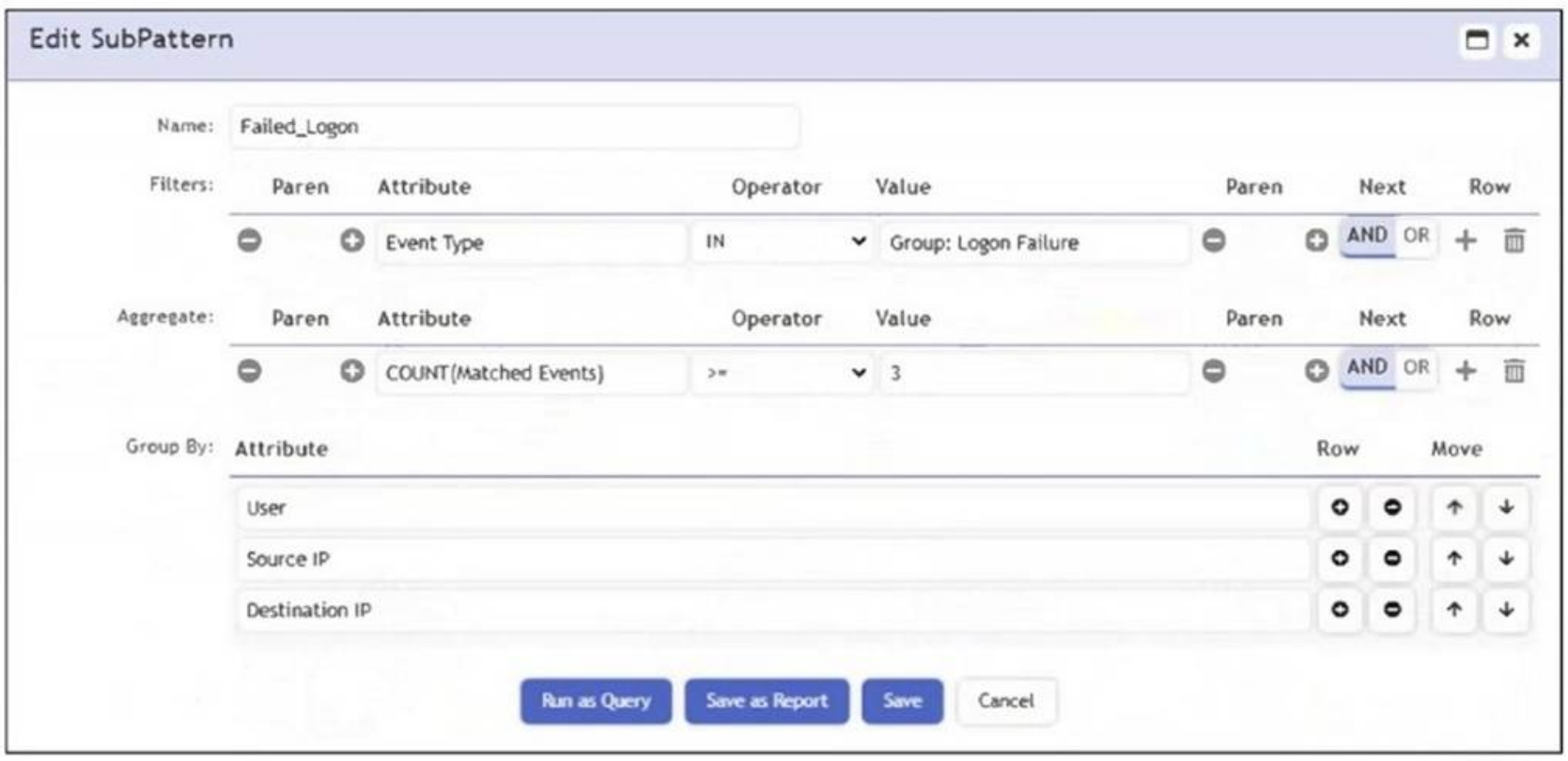
Answer: B

NEW QUESTION 7
Refer to the exhibit.

Subpattern 1



Subpattern 2



Rule Conditions

Which two conditions will match this rule and subpatterns? (Choose two.)

A. A user using RDP over SSL VPN fails to log in to an application five times.
B. A user runs a brute force password cracker against an RDP server.
C. A user fails twice to log in when connecting through RDP.
D. A user connects to the wrong IP address for an RDP session five times.

Answer: AB

Explanation:
The user initiates an RDP session (Subpattern 1) and then fails to log in multiple times (Subpattern 2 with COUNT(Matched Events) > = 3) - both from the same Source IP and User within 300 seconds.
The brute force attempts typically involve a successful RDP connection followed by multiple failed logins, satisfying the sequence and grouping conditions in the rule.

NEW QUESTION 8
Which items are used to define a subpattern?

A. Filters, Aggregate, Group By definitions
B. Filters, Aggregate, Time Window definitions
C. Filters, Group By, Threshold definitions
D. Filters, Threshold, Time Window definitions

Answer: A

Explanation:
A subpattern in FortiSIEM is defined using Filters to match specific events, Aggregate conditions to apply statistical thresholds (e.g., COUNT), and Group By attributes to segment data for evaluation. These three components collectively determine how the subpattern functions.

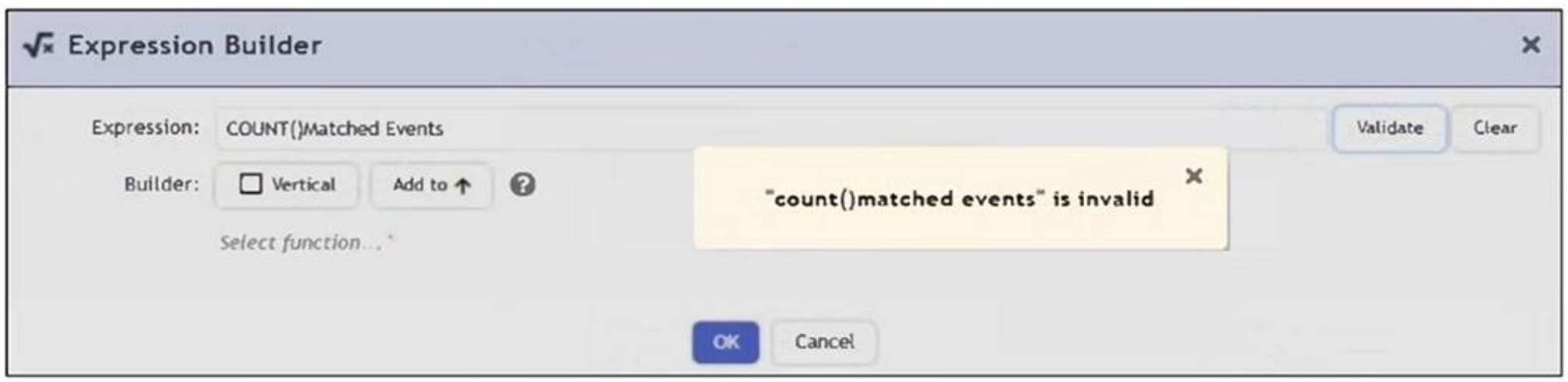
NEW QUESTION 9
Refer to the exhibit.

What is the Group: FortiSIEM Analysts value referring to?

A. FortiSIEM organization group
B. LDAP user group
C. CMDB user group
D. Windows Active Directory user group

Answer: C

NEW QUESTION 10
Refer to the exhibit.



An analyst is trying to identify an issue using an expression based on the Expression Builder settings shown in the exhibit; however, the error message shown in the exhibit indicates that the expression is invalid.
What is the correct syntax to create an expression that generates a total count of matched events?

A. COUNT(Matched Events)
B. (COUNT) Matched Events
C. Matched Events (COUNT)
D. Matched Events COUNT()

Answer: A

NEW QUESTION 10
Which running mode takes the most time to perform machine learning tasks?

A. Local auto
B. Local
C. Forecasting
D. Regression

Answer: A

NEW QUESTION 13
.....

Relate Links

100% Pass Your FCP_FSM_AN-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/FCP_FSM_AN-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/