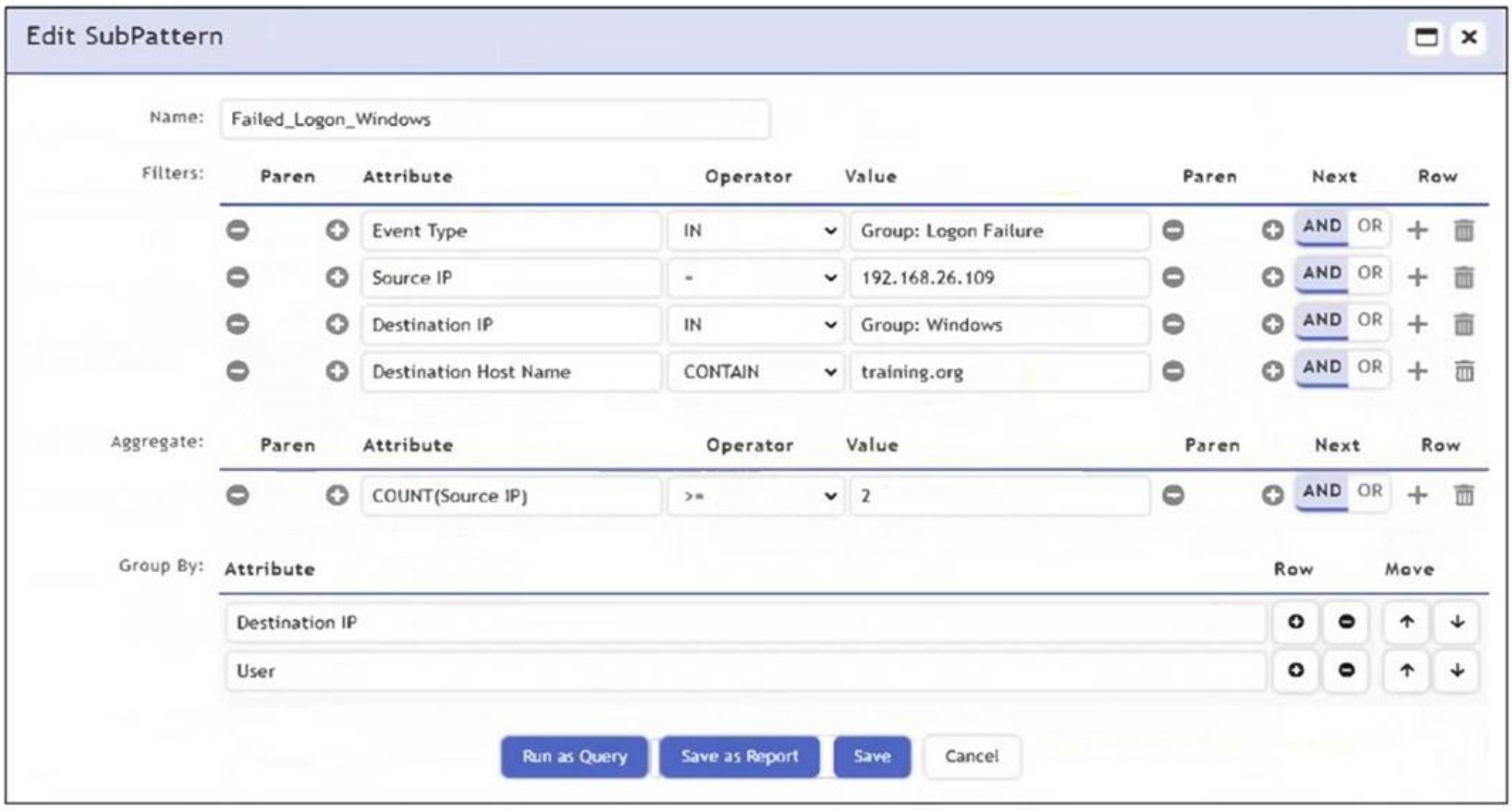
Fortinet

Exam Questions FCP_FSM_AN-7.2

FCP - FortiSIEM 7.2 Analyst

NEW QUESTION 1
Refer to the exhibit.

SubPattern edit window

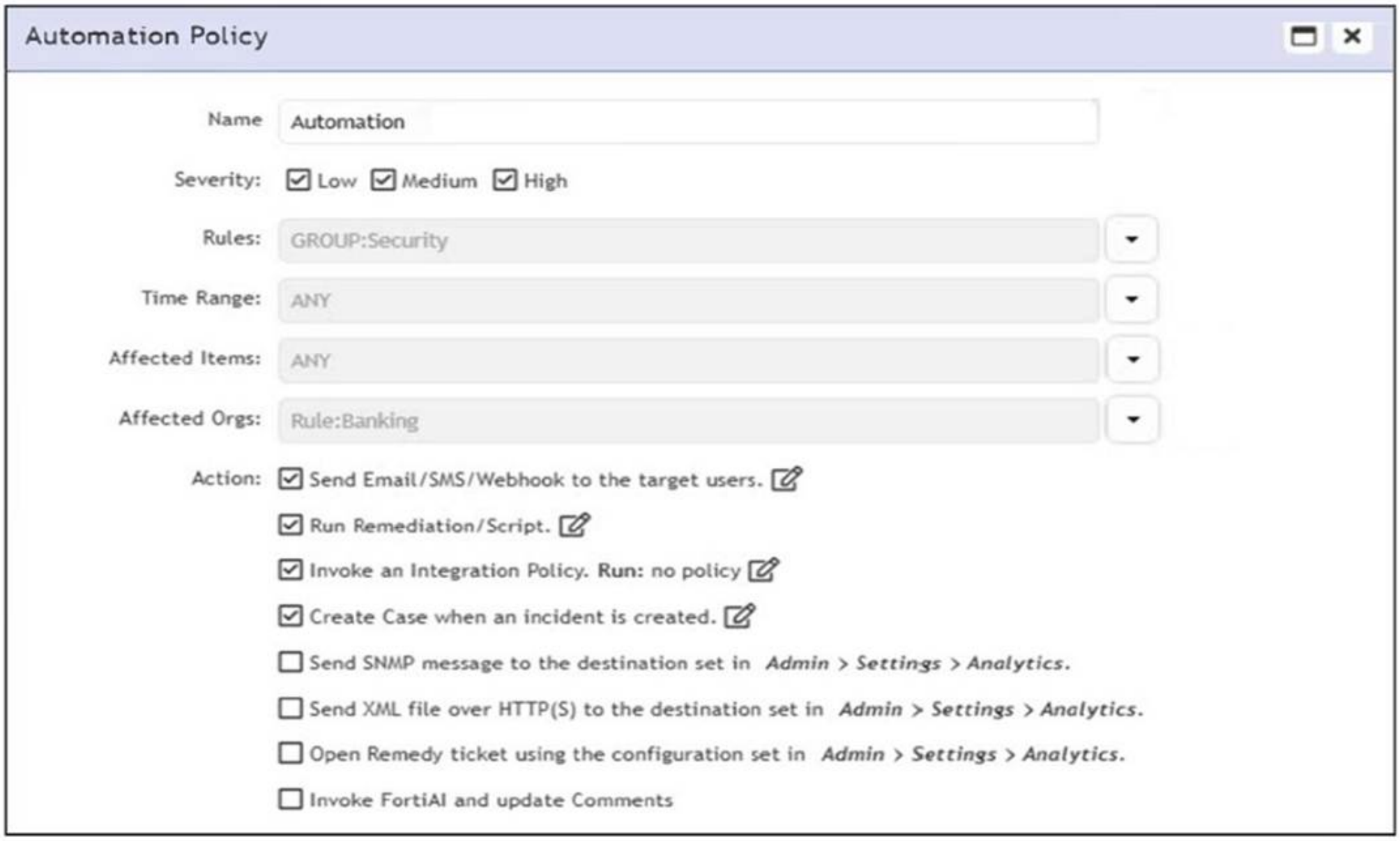


An analyst is troubleshooting the rule shown in the exhibit. It is not generating any incidents, but the filter parameters are generating events on the Analytics tab. What is wrong with the rule conditions?

A. The Event Type refers to a CMDB lookup and should be an Event lookup.
B. The Destination Host Name value is not fully qualified.
C. The Group By attributes restricts which events are counted.
D. The Aggregate attribute is too restrictive.

Answer: C

NEW QUESTION 2
Refer to the exhibit.

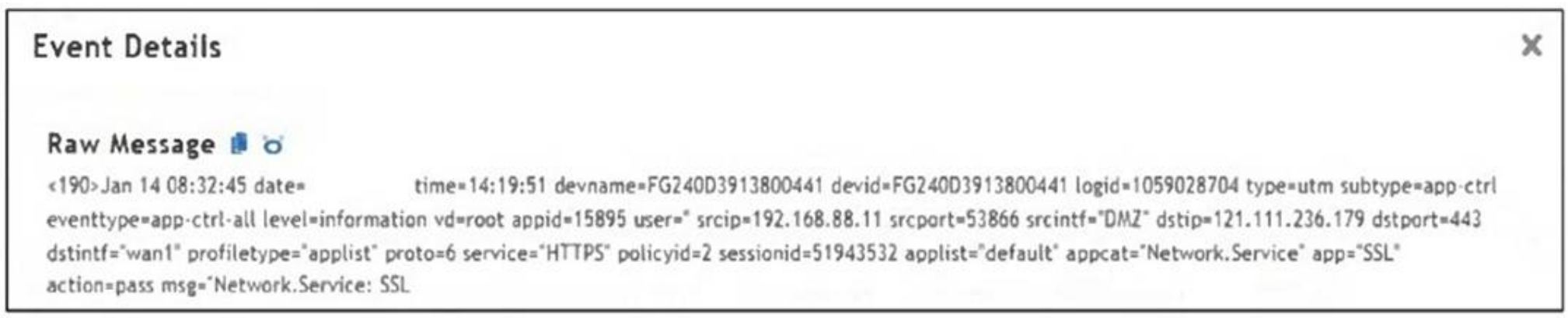


According to the automation policy configuration shown in the exhibit, what happens if an associated rule triggers?

A. FortiSIEM runs the remediation script, because that takes precedence over all other options.
B. FortiSIEM performs all selected actions.
C. FortiSIEM fails to the integration policy, because no policy is defined.
D. FortiSIEM sends an email, because that is first on the list.

Answer: B

NEW QUESTION 3
Refer to the exhibit.



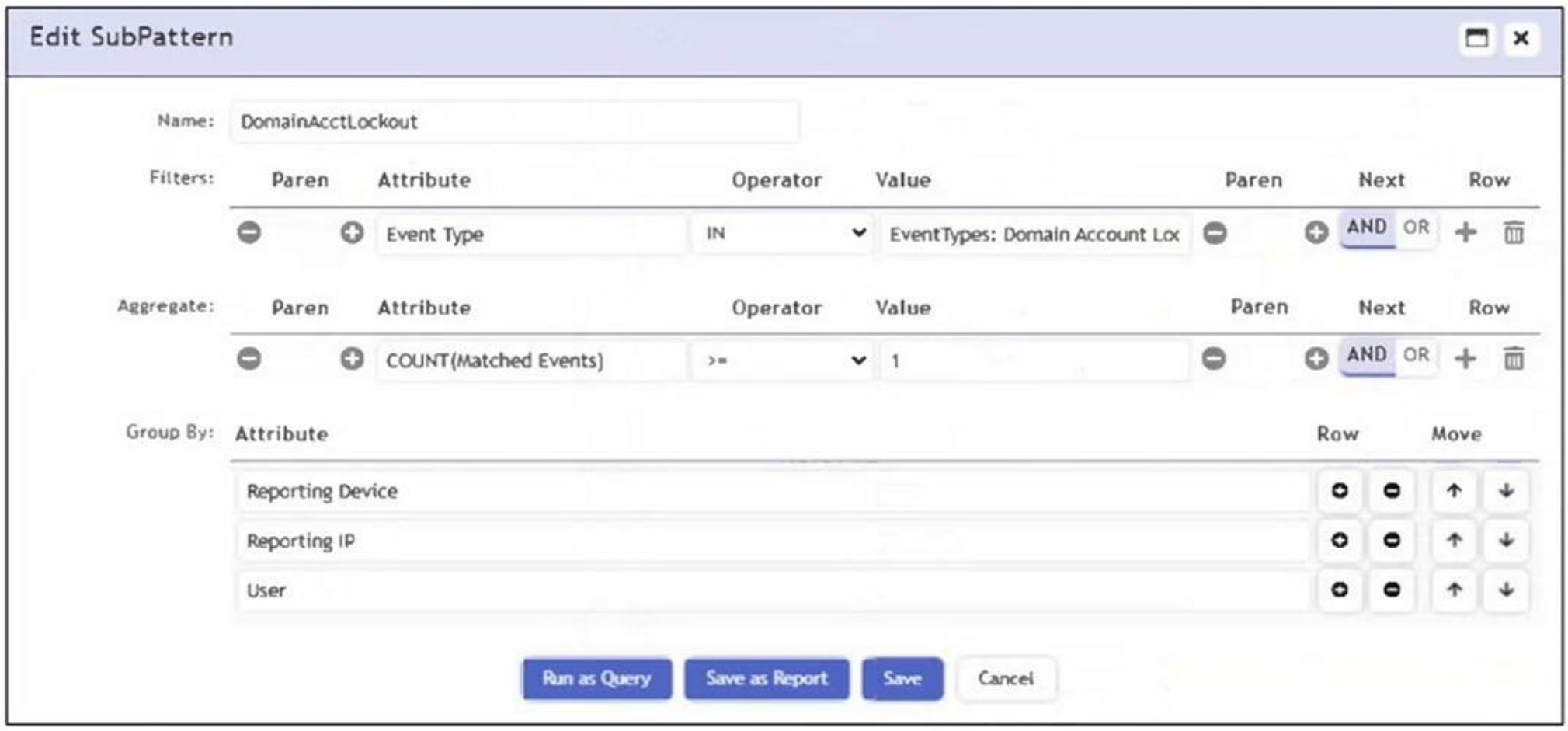
Which value would you expect the FortiSIEM parser to use to populate the Application Name field?

A. applist
B. Network.Service
C. SSL
D. wan1

Answer: C

NEW QUESTION 4
Refer to the exhibit.

Rule Subpattern



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 5
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

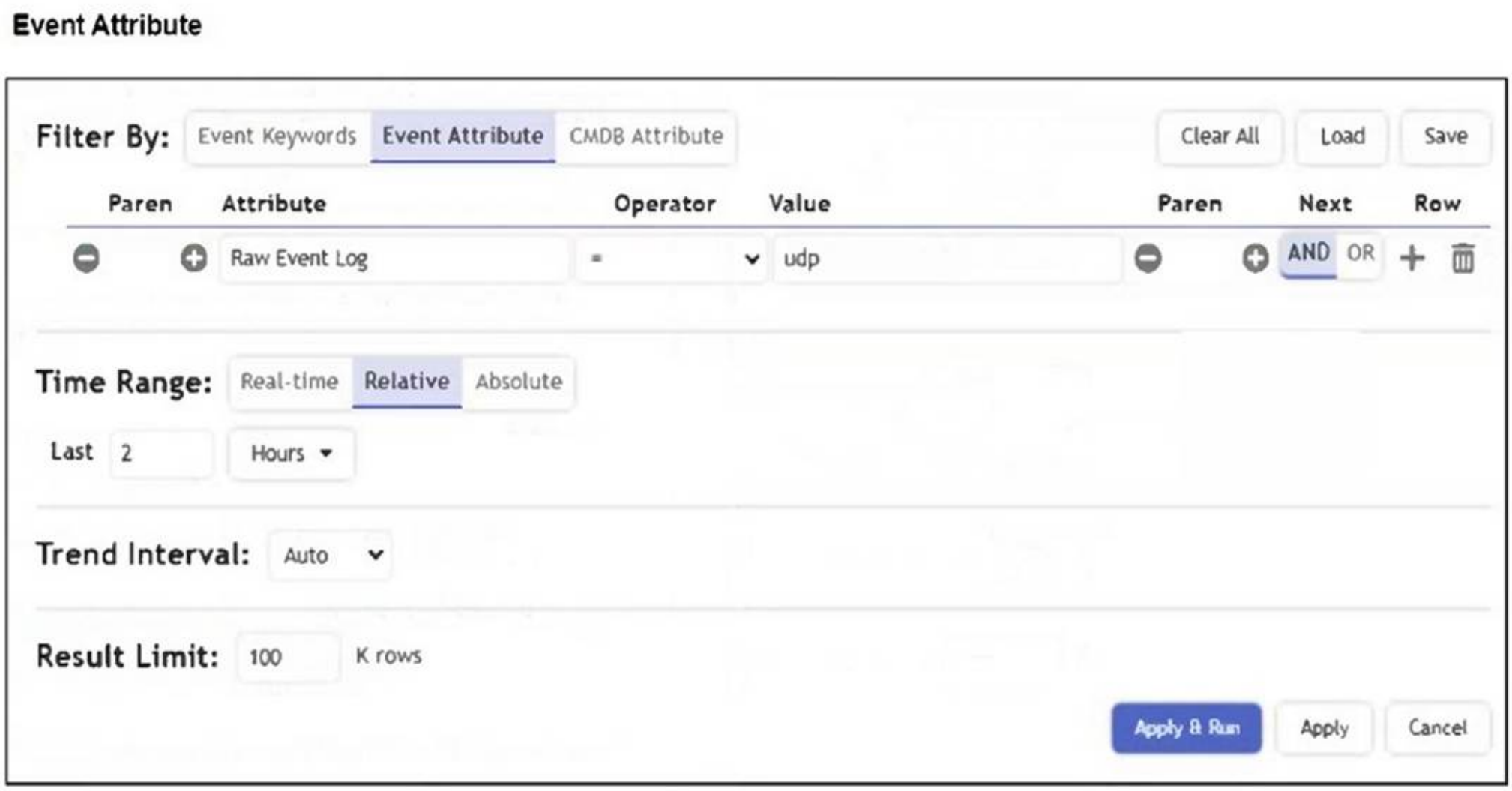
NEW QUESTION 6
Refer to the exhibit.

As shown in the exhibit, why are some of the fields highlighted in red?

A. Unique values cannot be grouped
B. The attribute COUNT(Matched Events) is an invalid expression.
C. No RAW Event Log attribute information is available.
D. The Event Receive Time attribute is not available for logs.

Answer: A

NEW QUESTION 7
Refer to the exhibit.



A FortiSIEM device is receiving syslog events from a FortiGate firewall. The FortiSIEM analyst is trying to search the raw event logs for the last two hours that contain the keyword "udp". However, they are getting no results from the search, which they know should be available. Based on the filter shown in the exhibit, why are there no search results?

A. The analyst selected AND in the Next colum
B. This is the wrong Boolean operator.
C. The Time Range value should be set to Real-Time.
D. The keyword is case sensitiv
E. Instead of typing udp in the Value field, the analyst should type UDP.
F. The analyst selected = in the Operator colum
G. That is the wrong operator.

Answer: D

NEW QUESTION 8
How does FortiSIEM update the incident table if a performance rule triggers repeatedly?

A. FortiSIEM changes the incident status to Repeated, and updates the Last Seen timestamp.
B. FortiSIEM updates the Incident Count value and Last Seen timestamp.
C. FortiSIEM generates a new incident based on the Rule Frequency value, and updates the First Seen and Last Seen timestamps.
D. FortiSIEM generates a new incident each time the rule triggers, and updates the First Seen and Last Seen timestamps.

Answer: B

NEW QUESTION 9
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 the events by User, Source IP, and Count attributes, how many results will FortiSIEM display?

A. Two
B. Six
C. Three
D. Five
E. Four

Answer: B

NEW QUESTION 10
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 10
Which information can FortiSIEM retrieve from FortiClient EMS through an API connection?

A. Host software versions
B. FortiSIEM license
C. Host login credentials
D. ZTNA tags

Answer: D

Explanation:
FortiSIEM can retrieve ZTNA tags from FortiClient EMS through an API connection, enabling dynamic user and device classification for policy enforcement and incident response.

NEW QUESTION 13

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

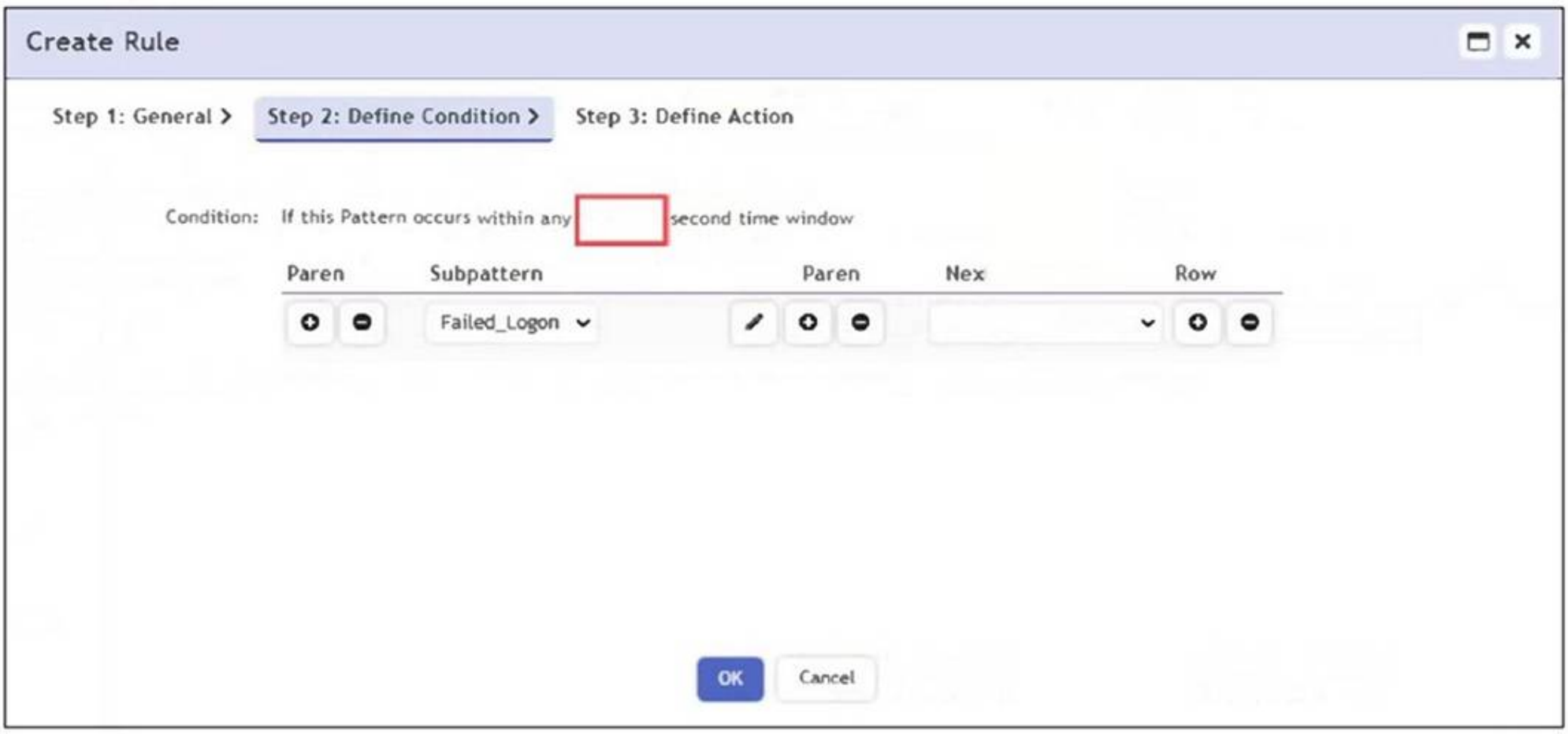
If you group the events by Reporting Device, Reporting IP, and Application Category, how many results will FortiSIEM display?

A. Four
B. Five
C. One
D. Six
E. Two

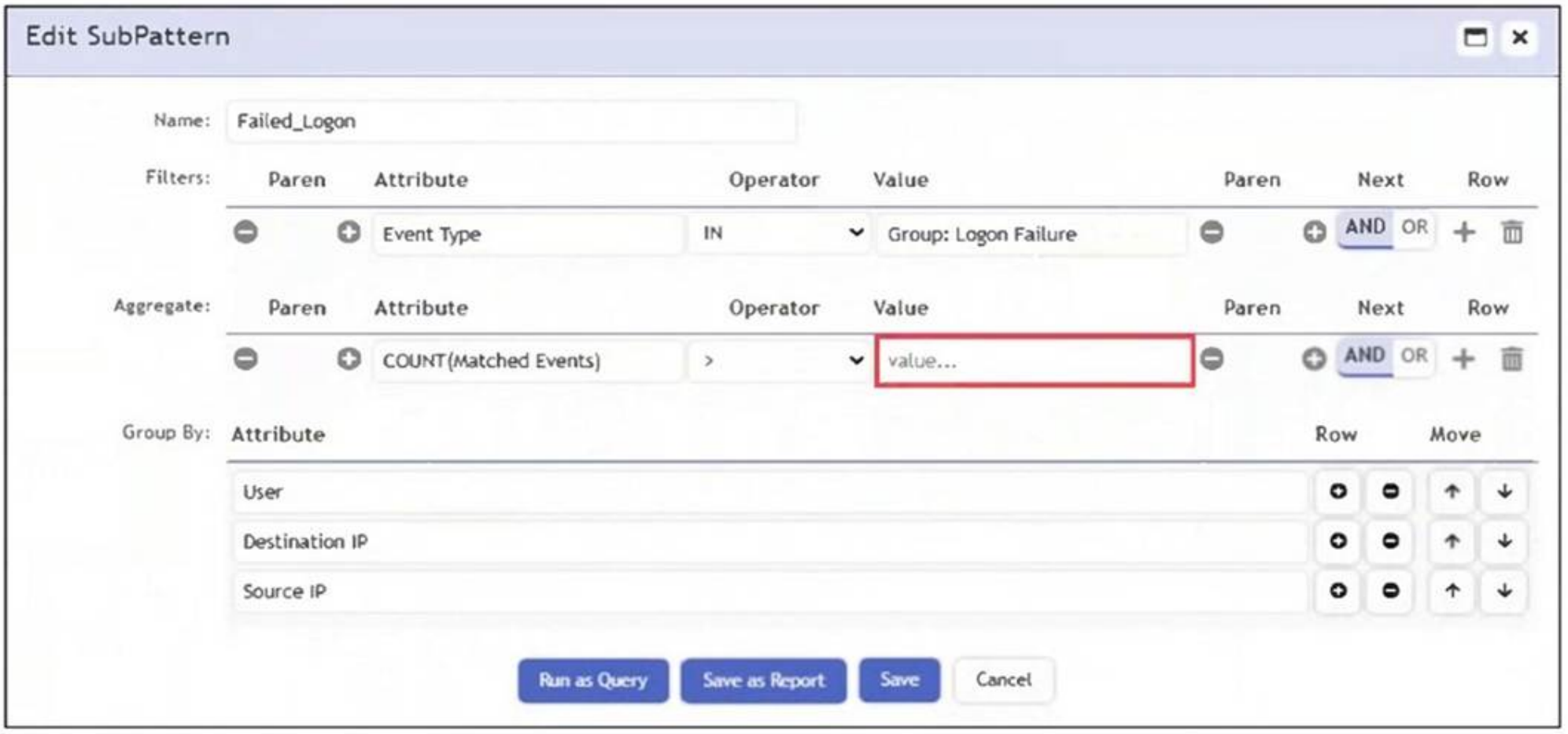
Answer: B

NEW QUESTION 16
Refer to the exhibit.

Rule Properties



SubPattern Properties



An analyst wants the rule shown in the exhibit to trigger when three failed login attempts occur within three minutes.
What should the values be for the condition time window and aggregate count?

A. Time window 180 seconds, aggregate count 3
B. Time window 180 seconds, aggregate count 2
C. Time window 90 seconds, aggregate count 3
D. Time window 90 seconds, aggregate count 2

Answer: A

NEW QUESTION 18
Which two settings must you configure to allow FortiSIEM to apply tags to devices in FortiClient EMS? (Choose two.)

A. FortiEMS API credentials defined on FortiSIEM
B. Remediation script configured
C. ZTNA tags defined on FortiSIEM
D. FortiSIEM API credentials defined on FortiEMS\

Answer: AC

NEW QUESTION 22

What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?

A. FortiSIEM agent
B. SSH
C. SNMP
D. FortiSIEM worker

Answer: A

NEW QUESTION 27
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 30
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FSM_AN-7.2 Practice Exam Features:

* FCP_FSM_AN-7.2 Questions and Answers Updated Frequently

* FCP_FSM_AN-7.2 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FSM_AN-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FSM_AN-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year