Fortinet

Exam Questions FCP_FSM_AN-7.2

FCP - FortiSIEM 7.2 Analyst

NEW QUESTION 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

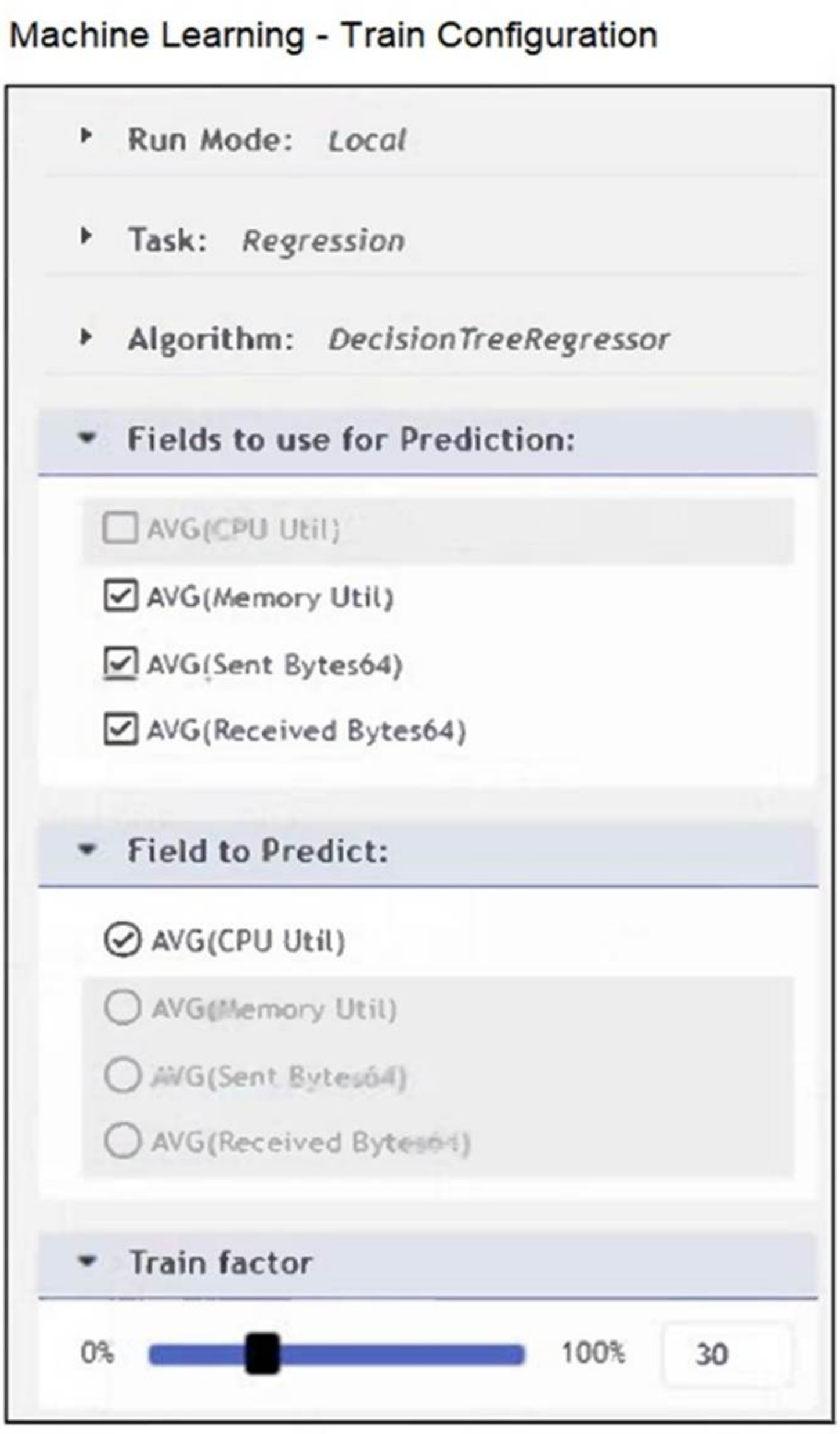
NEW QUESTION 2
Refer to the exhibit.

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 3
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 4

Refer to the exhibit.

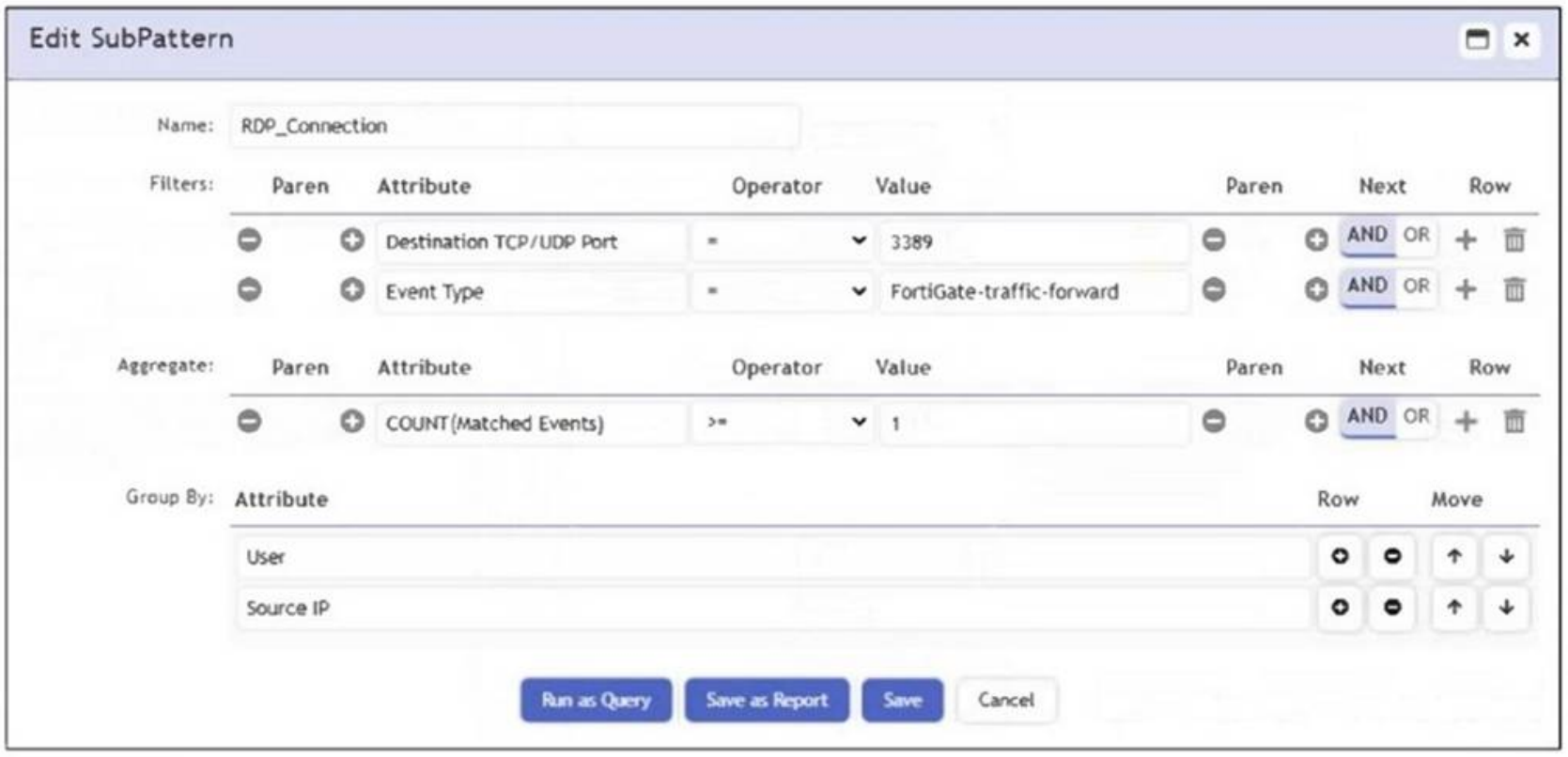
The analyst is troubleshooting the analytics query shown in the exhibit. Why is this search not producing any results?

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.

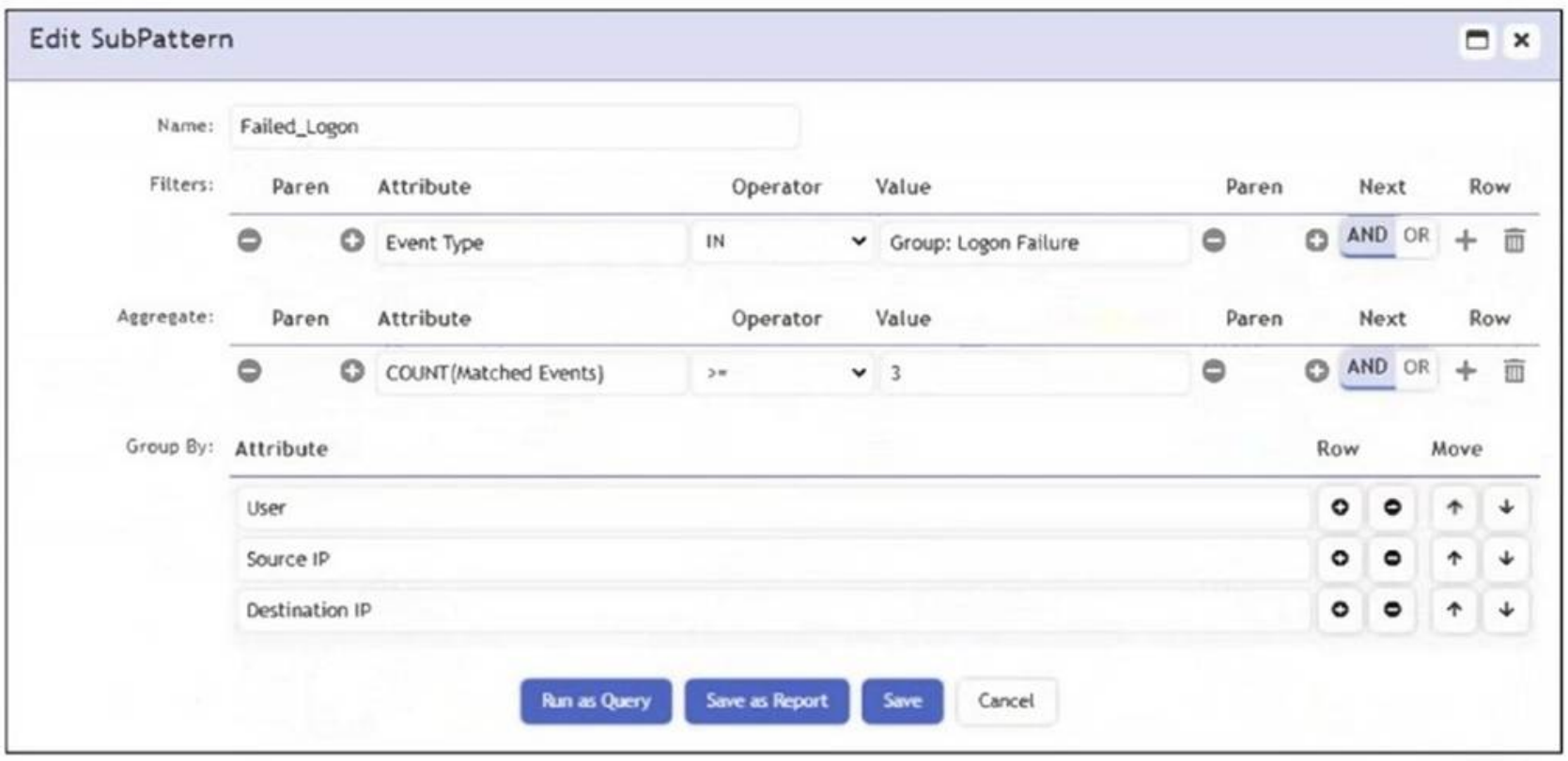
Answer: B

NEW QUESTION 5
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 6
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 7
How can you query the configuration management database (CMDB) in an analytics search?

A. Click Value > Select from CMDB.
B. On the CMDB tab, select an entry, and then click Create Search.
C. On the Admin tab, click CMDB Search.
D. Click Attribute > Select from CMDB.

Answer: A

NEW QUESTION 8
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 9
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

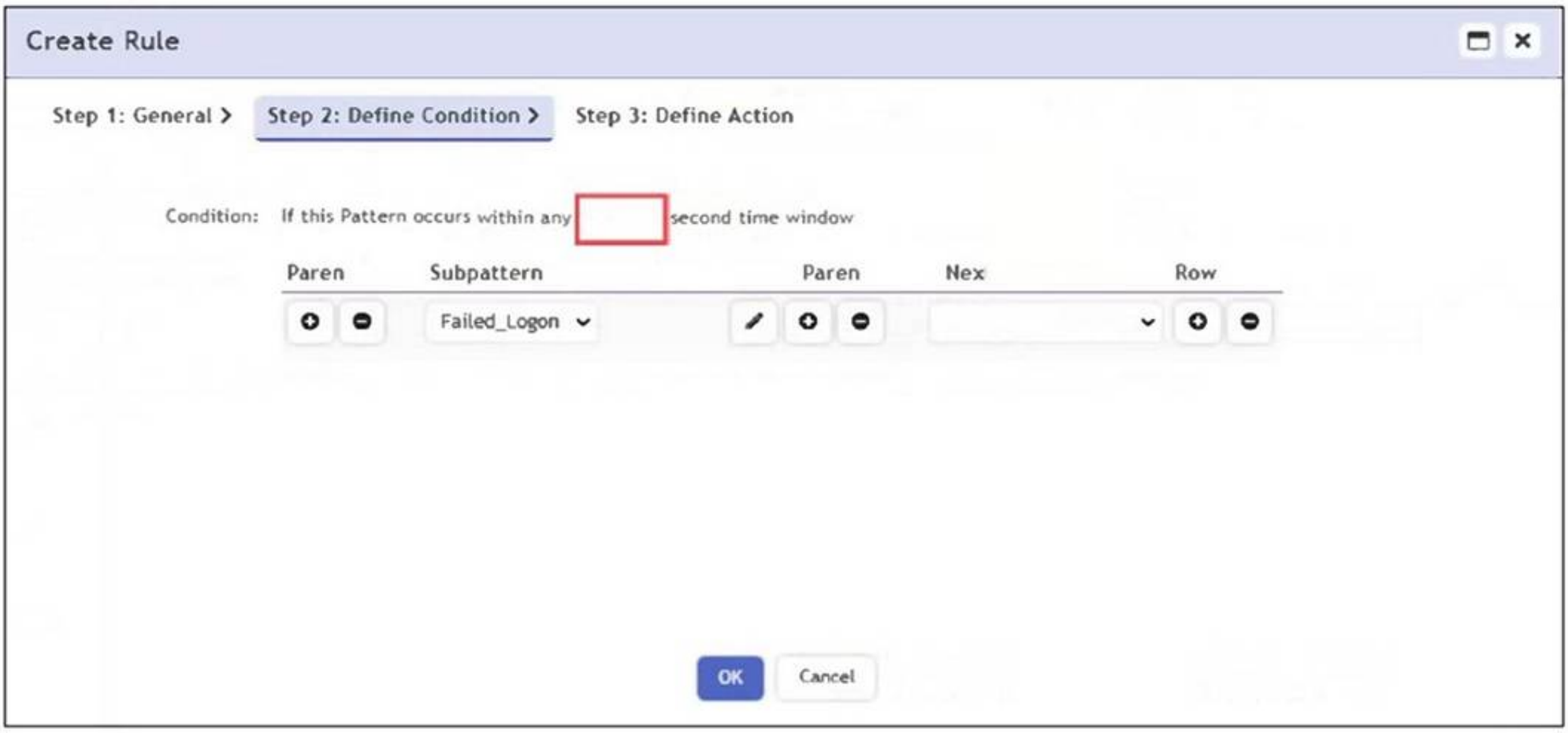
Answer: A

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

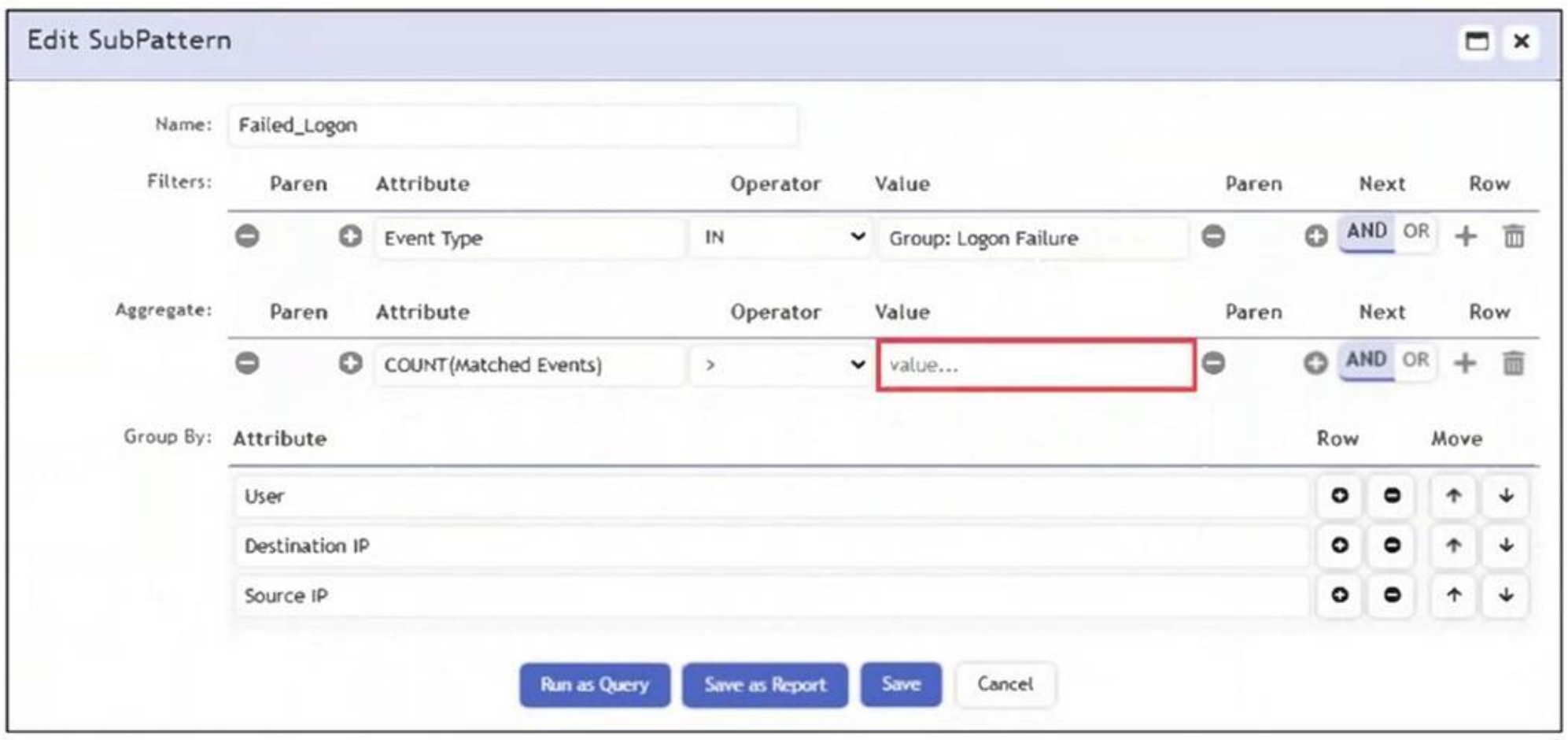
attributes to segment data for evaluation. These three components collectively determine how the subpattern functions.

NEW QUESTION 10
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 10
Refer to the exhibit.

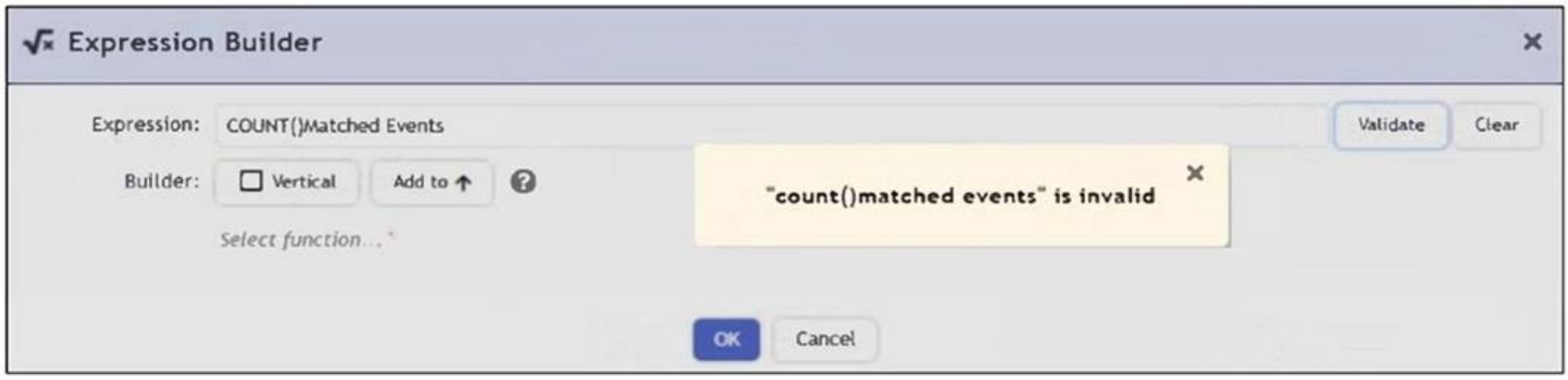
Source IP	Reporting Device	Reporting IP	Event Type	User	Count
15.2.3.4	FW01	10.1.1.1	Logon	Mike	4
21.3.4.5	FW01	10.1.1.1	Logon	Bob	3
14.12.3.1	FW01	10.1.1.1	Logon	Alice	2
192.168.1.5	FW01	10.1.1.1	Logon	Alice	2
10.1.1.1	FW01	10.1.1.1	Logon	Bob	6
123.123.1.1	FW01	10.1.1.1	Logon	Mike	5

If you group the events by User and Count attributes, how many results will FortiSIEM display?

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

Answer: D

NEW QUESTION 12
Refer to the exhibit.

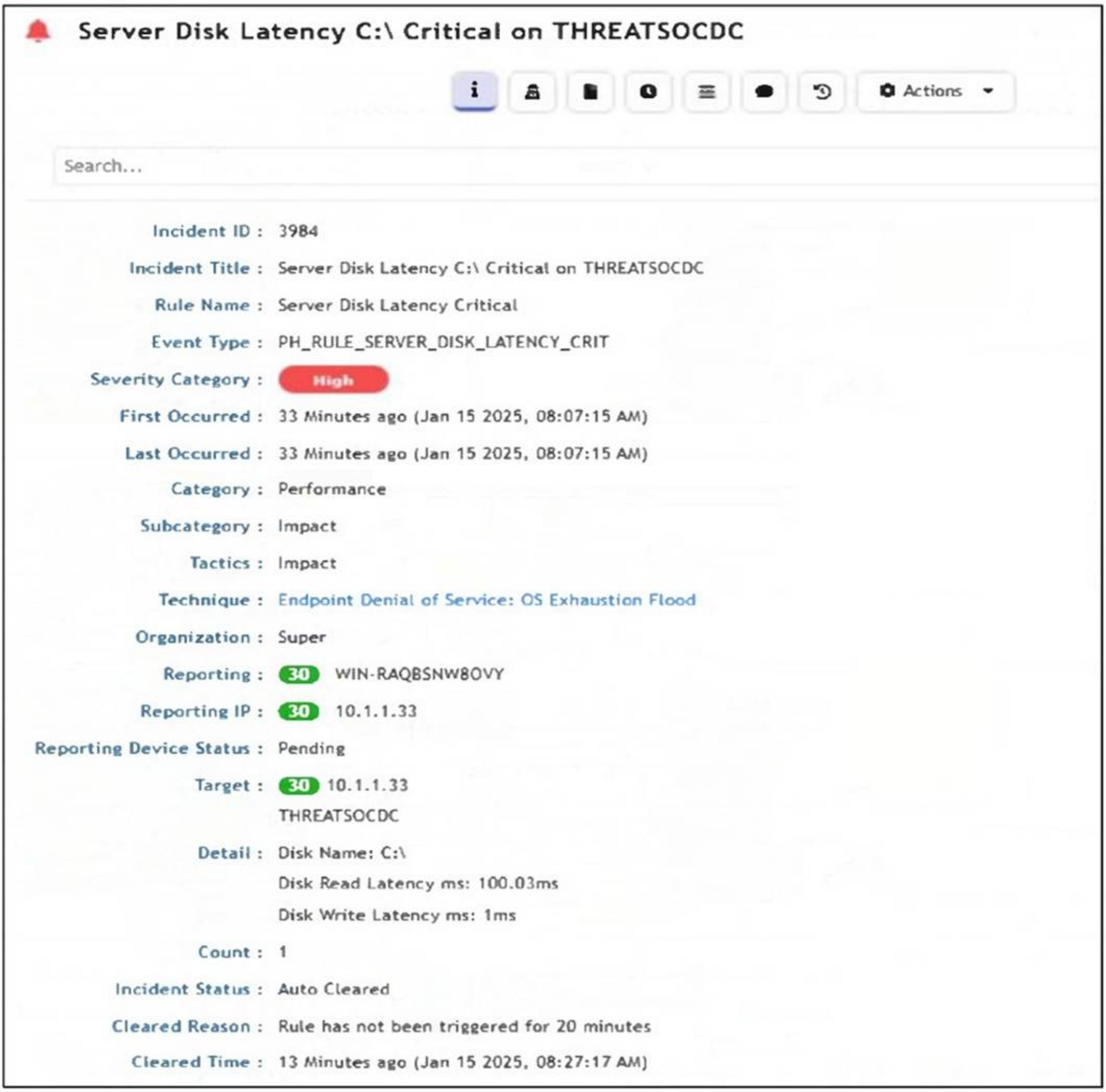


An analyst is trying to identify an issue using an expression based on the Expression Builder settings shown in the exhibit; however, the error message shown in the exhibit indicates that the expression is invalid.
What is the correct syntax to create an expression that generates a total count of matched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

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

Answer: A

NEW QUESTION 16
Refer to the exhibit.



How was this incident cleared?

A. The analyst manually cleared the incident from the incident table.
B. FortiSIEM cleared the incident automatically after 24 hours.
C. The incident was cleared automatically by the rule.
D. The endpoint was rebooted and sent an all-clear signal to FortiSIEM.

Answer: C

NEW QUESTION 17
.....

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