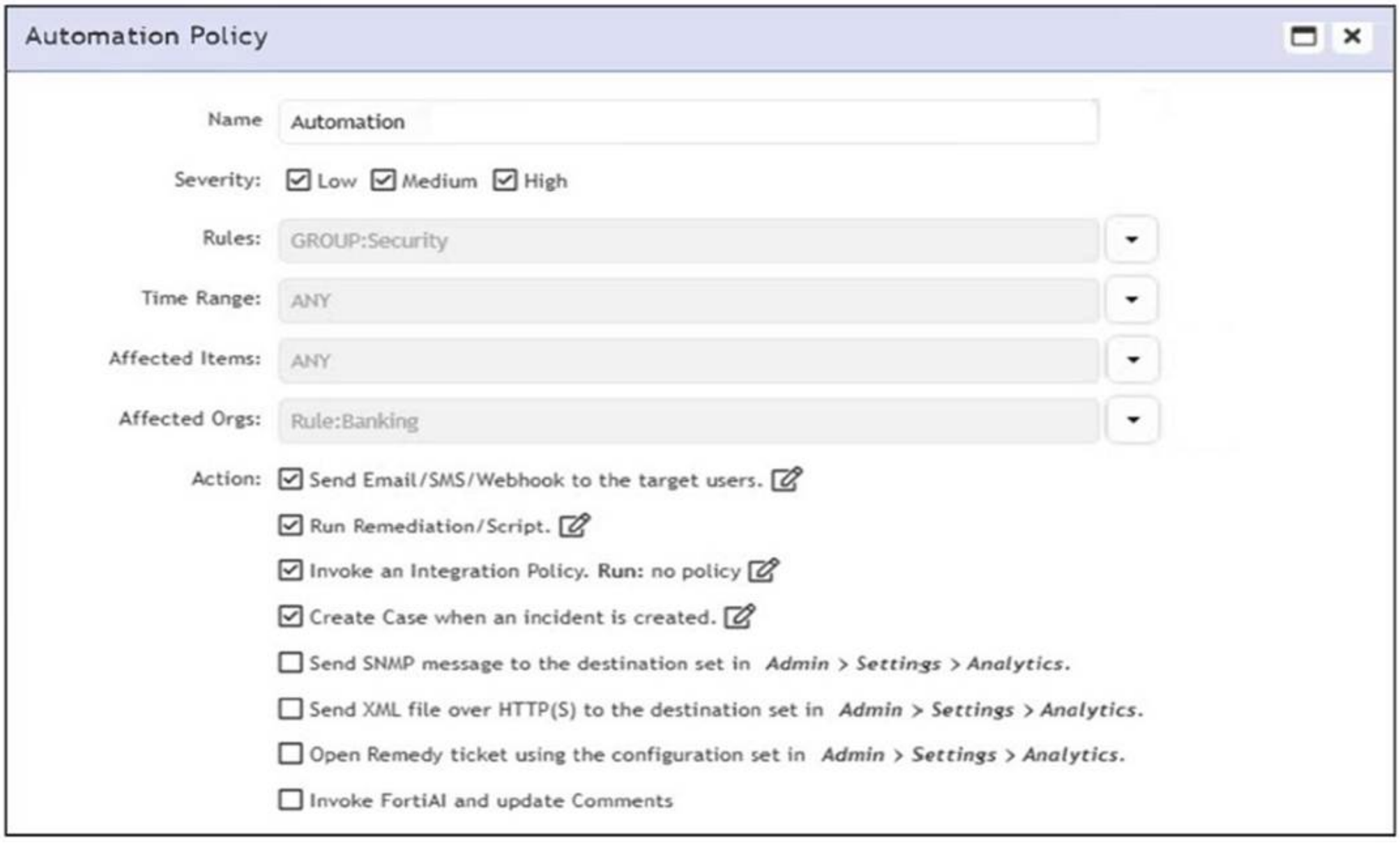
Exam Questions FCP_FSM_AN-7.2

FCP - FortiSIEM 7.2 Analyst

https://www.2passeasy.com/dumps/FCP_FSM_AN-7.2/

NEW QUESTION 1
Refer to the exhibit.

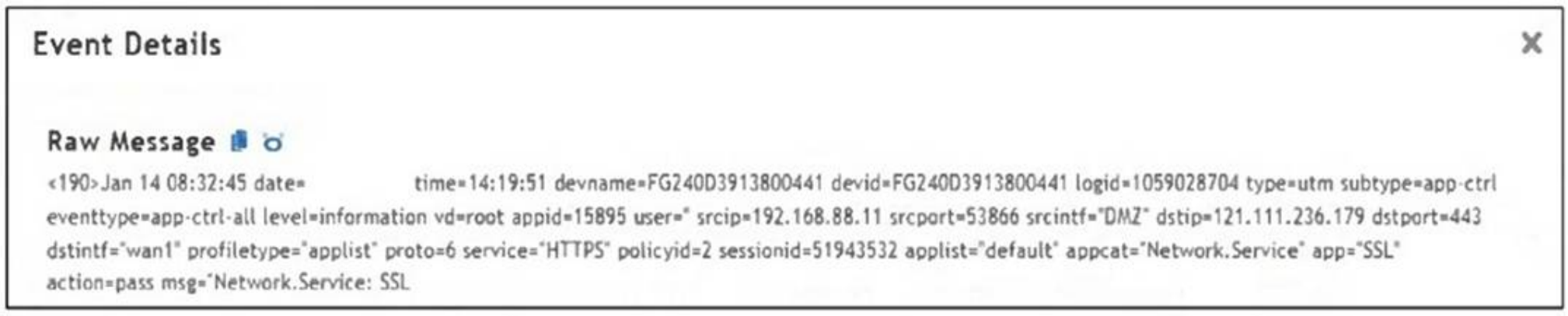


According to the automation policy configuration shown in the exhibit, what happens if an associated rule triggers?

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 2
Refer to the exhibit.



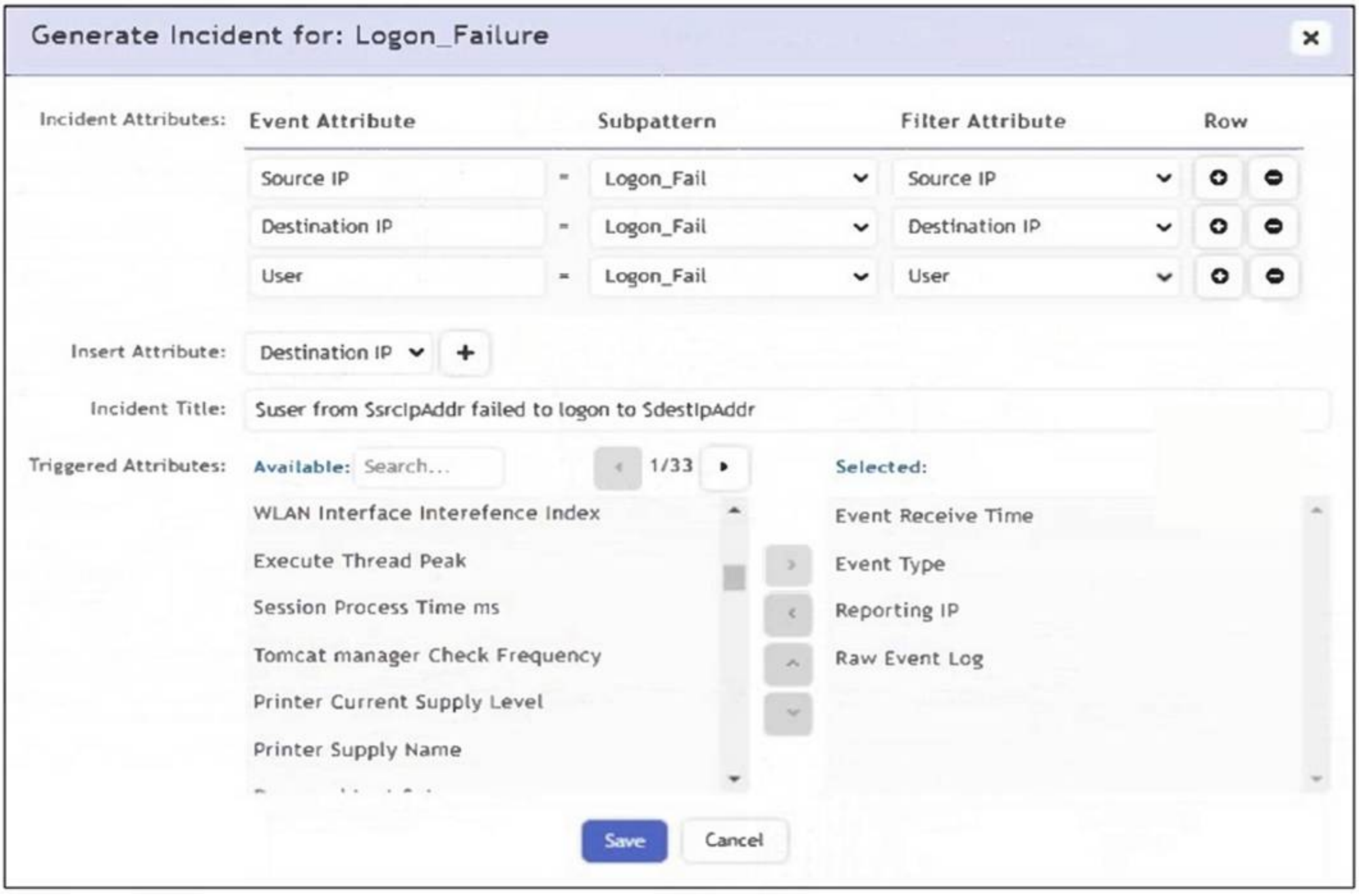
Which value would you expect the FortiSIEM parser to use to populate the Application Name field?

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

Answer: C

NEW QUESTION 3
Refer to the exhibit.

Incident generator window



An analyst is trying to generate an incident with a title that includes the Source IP, Destination IP, User, and Destination Host Name. They are unable to add a Destination Host Name as an incident attribute.
What must be changed to allow the analyst to select Destination Host Name as an attribute?

A. The Destination Host Name must be selected as a Triggered Attribute.
B. The Destination Host Name must be set as an aggregate item in a subpattern.
C. The Destination Host Name must be added as an Event type in the FortiSIEM.
D. The Destination IP Event Attribute must be removed.

Answer: A

NEW QUESTION 4
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

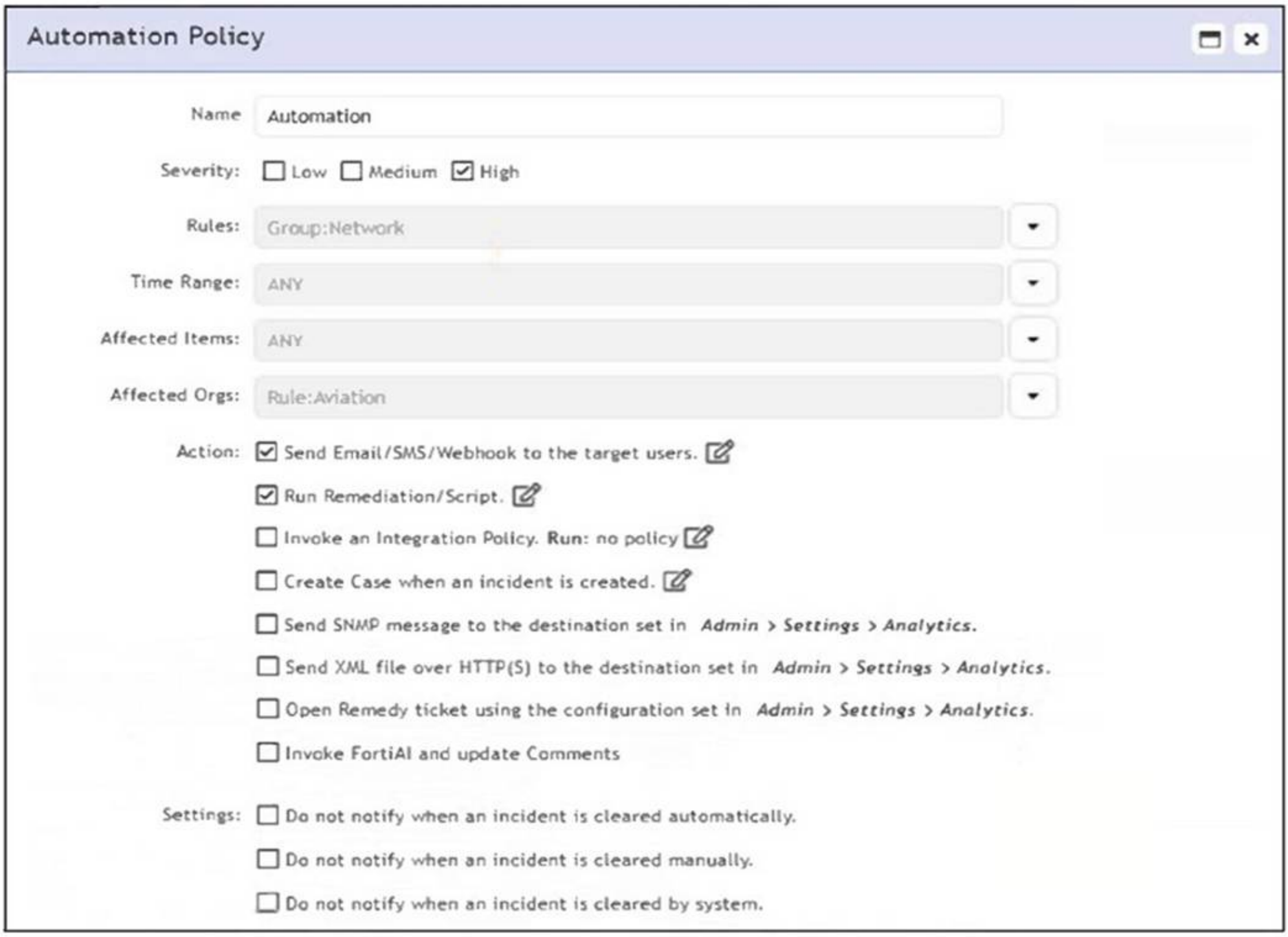
NEW QUESTION 5
How does FortiSIEM update the incident table if a performance rule triggers repeatedly?

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.

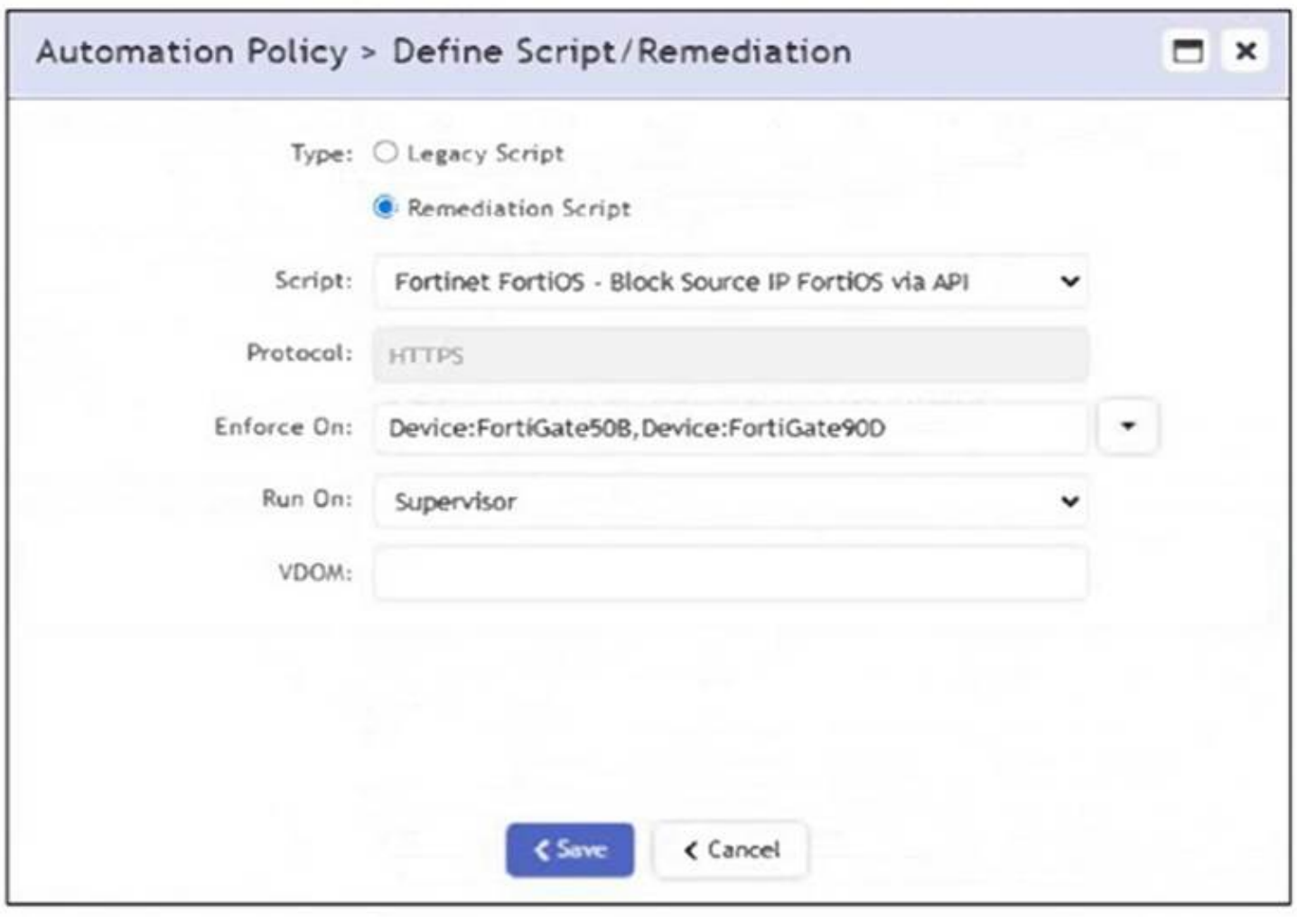
Answer: B

NEW QUESTION 6
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 7
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 8
Which information can FortiSIEM retrieve from FortiClient EMS through an API connection?

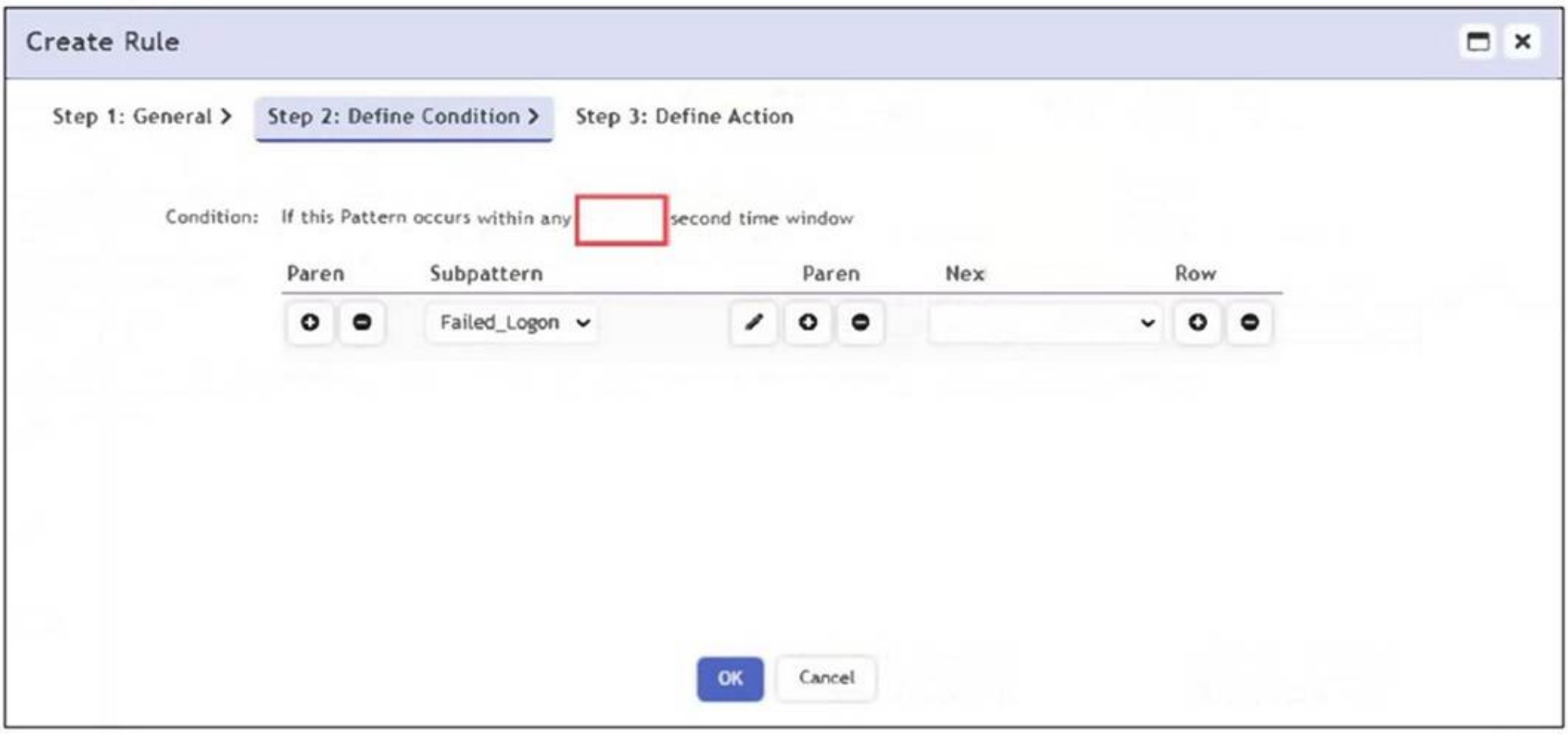
A. Host software versions
B. FortiSIEM license
C. Host login credentials
D. ZTNA tags

Answer: D

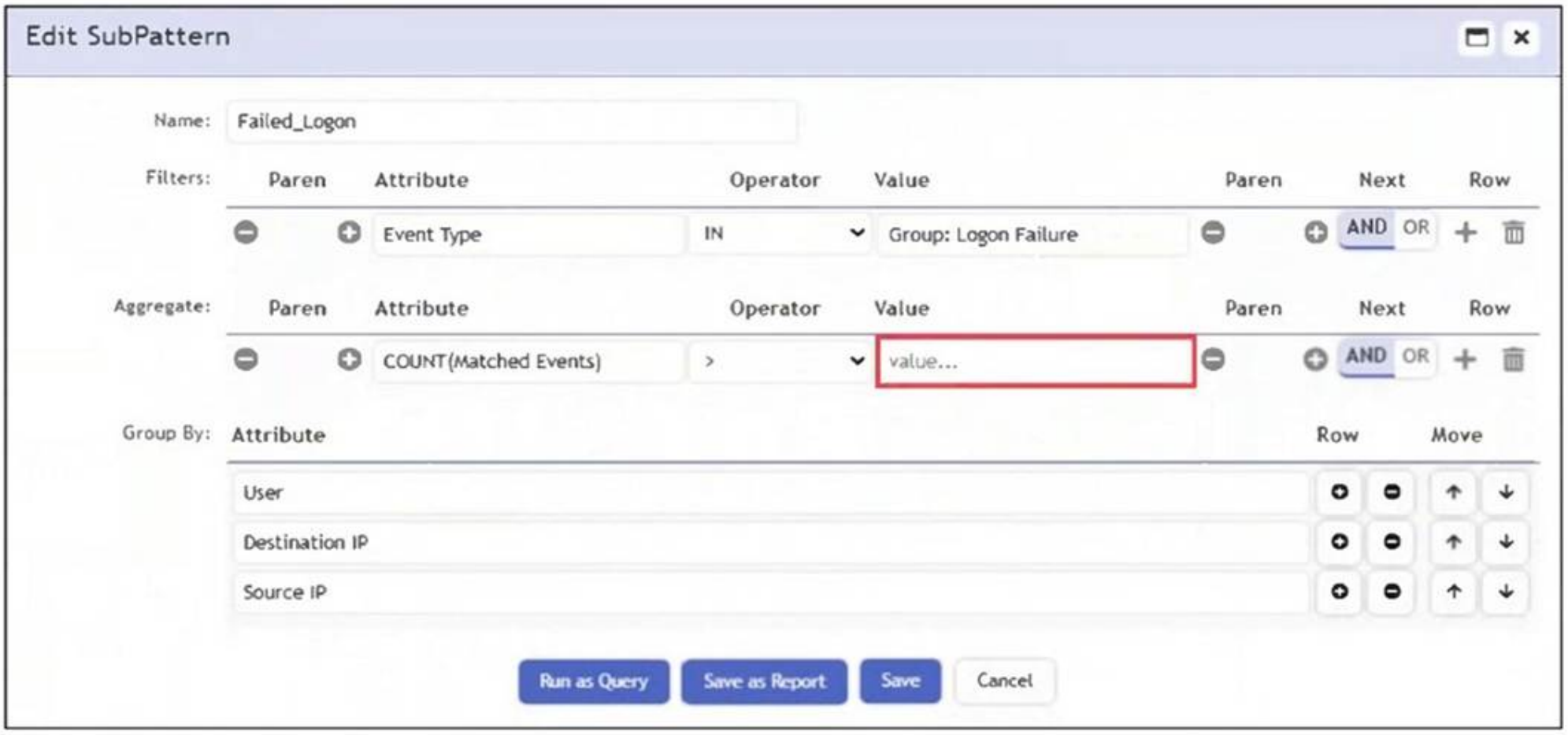
Explanation:
FortiSIEM can retrieve ZTNA tags from FortiClient EMS through an API connection, enabling dynamic user and device classification for policy enforcement and incident response.

NEW QUESTION 9
Refer to the exhibit.

Rule Properties



SubPattern Properties

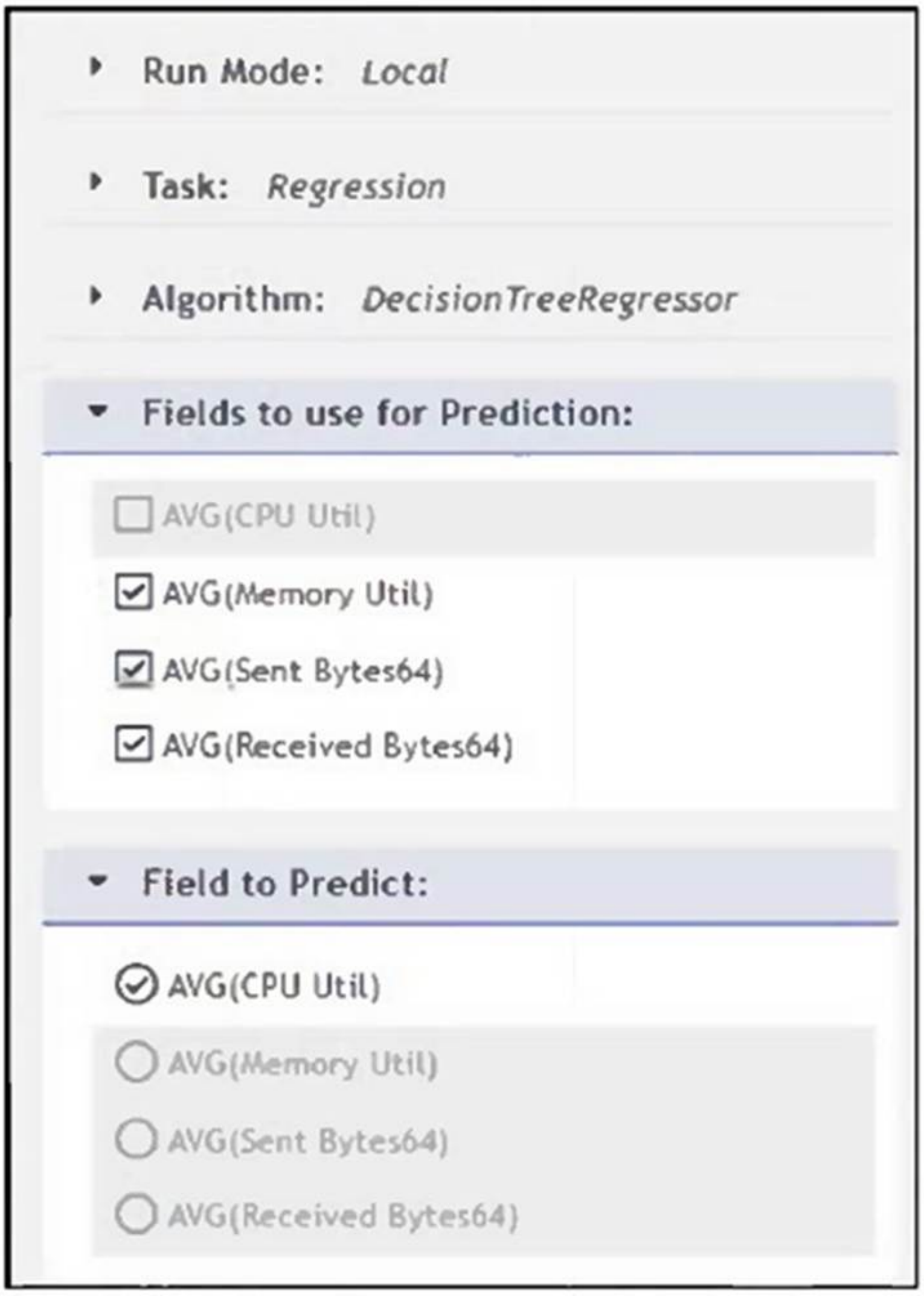


An analyst wants the rule shown in the exhibit to trigger when three failed login attempts occur within three minutes.
What should the values be for the condition time window and aggregate count?

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.

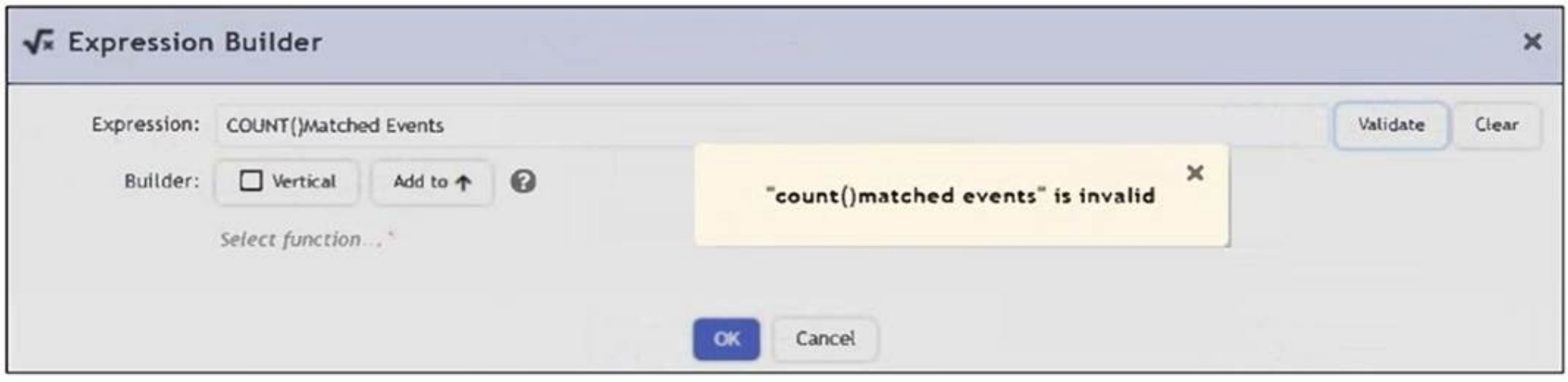


What will happen when a device being analyzed by the machine learning configuration shown in the exhibit has a consistently high memory utilization?

A. FortiSIEM will update the regression tables for memory utilization, and average sent and received bytes.
B. FortiSIEM will trigger an incident for high memory utilization.
C. FortiSIEM will lower the CPU utilization trigger requirement for CPU utilization.
D. FortiSIEM will update the model with a higher memory utilization average value.

Answer: D

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()

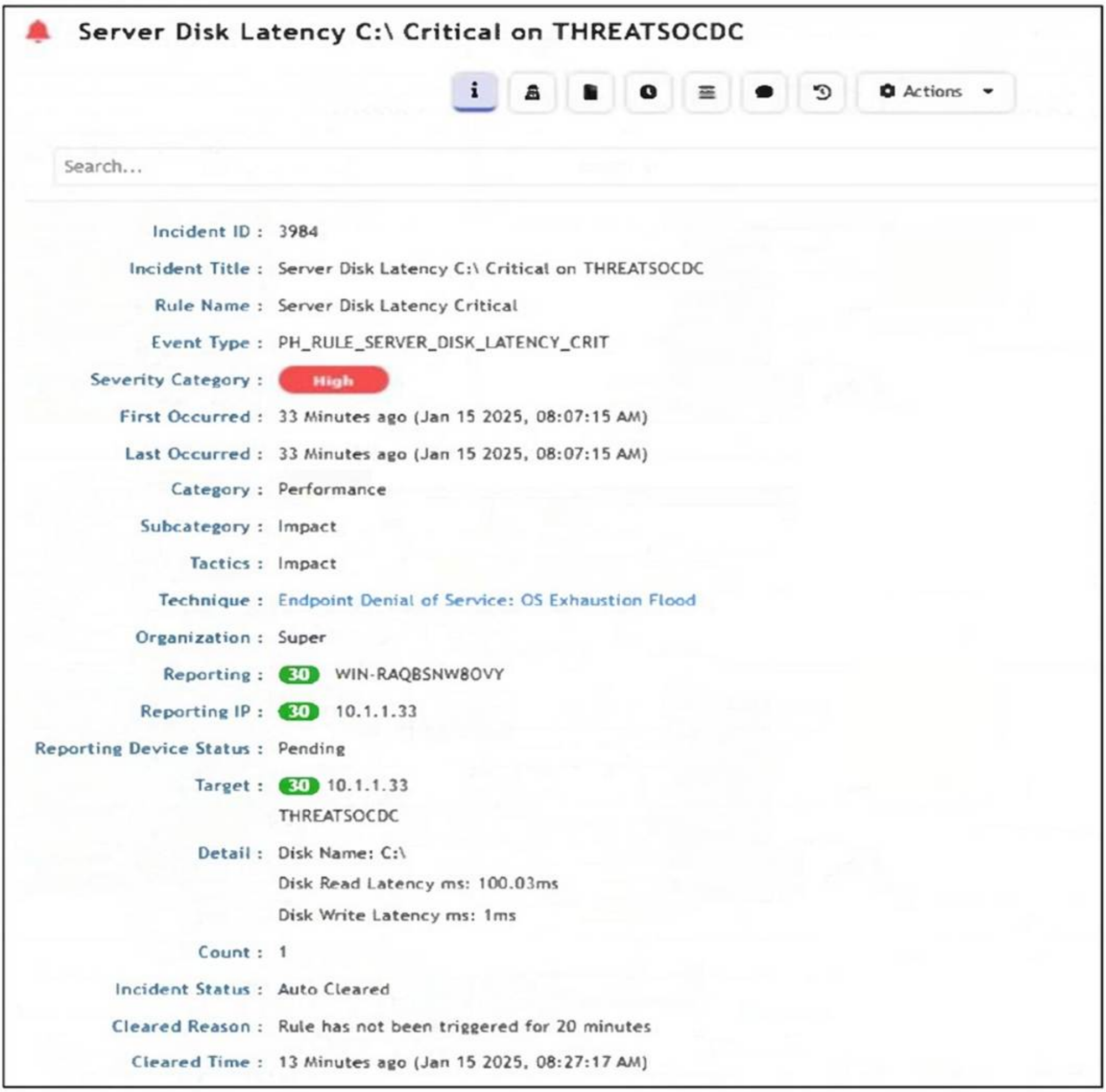
Answer: A

NEW QUESTION 11
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 12
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 14
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FSM_AN-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FSM_AN-7.2 Product From:

https://www.2passeasy.com/dumps/FCP_FSM_AN-7.2/

Money Back Guarantee

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