Fortinet NSE6_FSM_AN-7.4 NSE 6 Practice Questions

Shared by Rogers on 17-08-2026

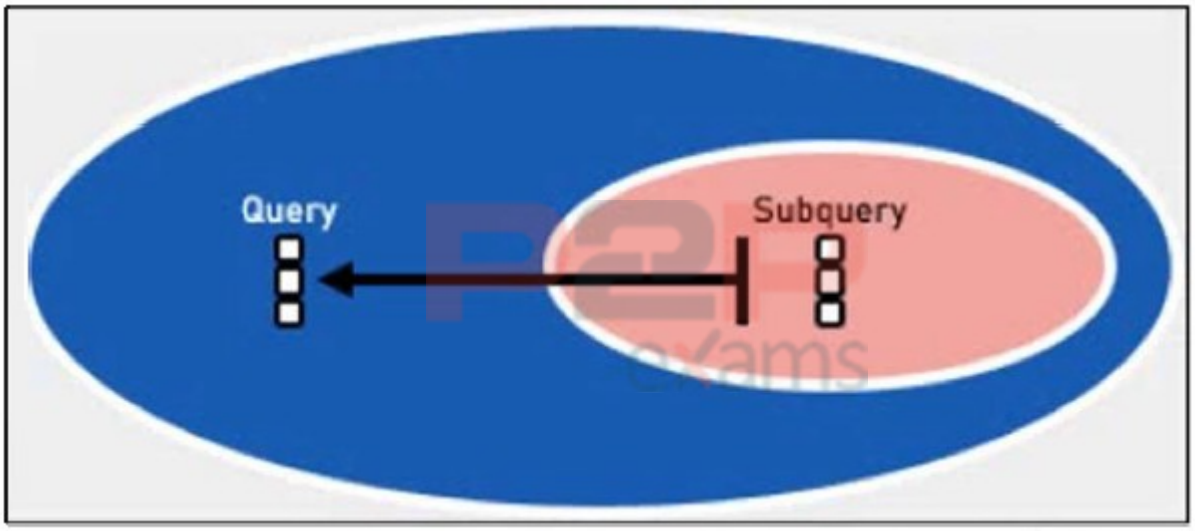
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



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

Options:

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

Answer:

B, D

Explanation:

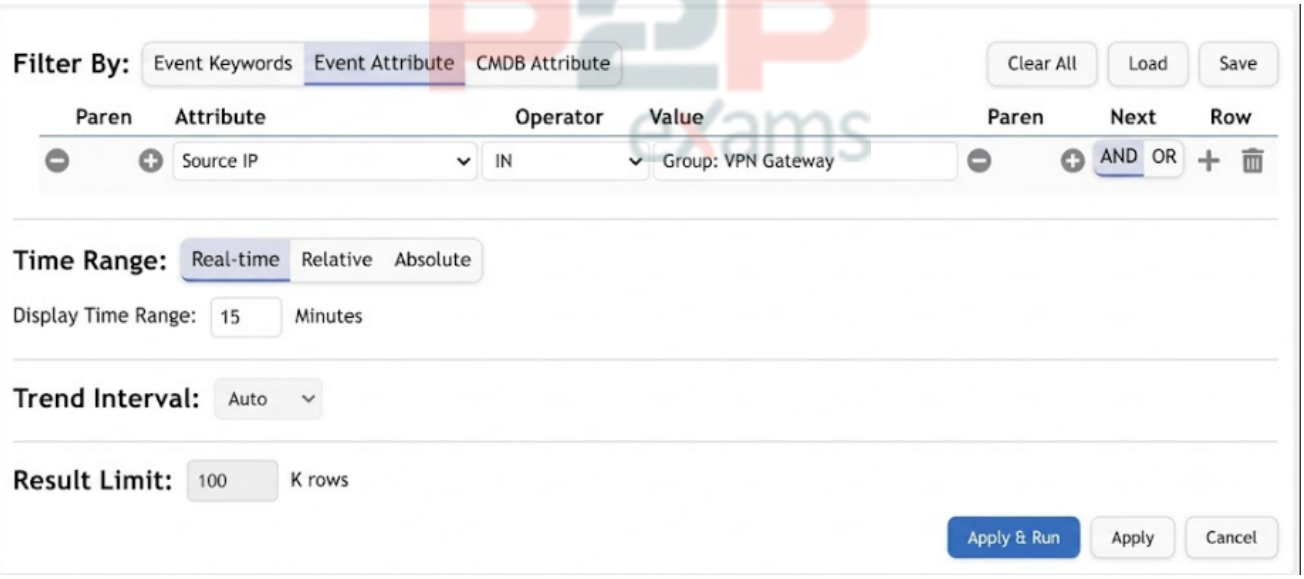
The FortiSIEM Study Guide defines a nested query as a query that has another query embedded within it, where the embedded query is known as the subquery. The FortiSIEM 7.4 User Guide lists the supported nested search scenarios: Outer CMDB Query, Inner Event Query; Outer Event Query, Inner Event Query; and Outer Event Query, Inner CMDB Query. These supported combinations prove that the inner or subquery can be either an Event Query or a CMDB Query. LDAP Query and SNMP Query are not listed as supported nested analytics subquery types. LDAP may be used for user discovery or authentication, and SNMP may be used for monitoring or discovery, but neither is referenced as a nested analytics query type. The User Guide also explains that the outer query uses Select from Report to reference the saved inner query and

that the matching attribute data types must align between the outer query and the selected display column in the inner query.

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



What is the Group: VPN Gateway value a reference to? (Choose one answer)

Options:

A- A configuration management database (CMDB) device group
B- A FortiSIEM rule folder
C- A FortiSIEM watchlist
D- A FortiGate address group

Answer:

A

Explanation:

The correct answer is A. A configuration management database (CMDB) device group. In the exhibit, the analytics filter uses Source IP IN Group: VPN Gateway. In FortiSIEM analytics, values shown as Group: for IP/device-related attributes commonly reference FortiSIEM CMDB

groups, not firewall address groups or rule folders. The FortiSIEM 7.4 User Guide explains how CMDB groups are inserted into queries: to add a CMDB group, the user selects an attribute, selects an operator such as IN, and then selects a value from CMDB. The guide gives a direct example where a reporting IP is matched using a firewall device group, expressed as a condition equivalent to ''reptDevIpAddr IN Firewall group.''

This matches the exhibit's structure: Source IP is the event attribute, IN is the operator, and Group: VPN Gateway is the selected CMDB group value. A FortiSIEM watchlist is different; the Study Guide describes watchlists as containers of similar items that can be referenced in searches, rules, and reports, but they are managed under Resources > Watch Lists, not shown here as a CMDB-style device group value. A FortiGate address group exists on FortiGate, not as this FortiSIEM analytics CMDB group reference.

Question 3

Question Type: MultipleChoice

When selecting multiple rules at once on FortiSIEM, what actions can you perform?

Options:

A- You can change the severity of multiple rules, and activate or deactivate them.
B- You can only view, edit, and activate a single rule at one time.
C- You can only change the severity of multiple rules.
D- You can only activate or deactivate multiple rules.

Answer:

A

Explanation:

The correct answer is A. FortiSIEM supports bulk rule operations for selected rules. The FortiSIEM 7.4 User Guide states that if you have permission to activate a rule, you can activate or deactivate multiple rules with a single click. The procedure instructs the user to go to Resources > Rules, click the edit icon, select Multiple Rules, choose the rules, and then use the Select Actions panel. In that panel, the guide states that you can select a Severity from the Severity drop-down list to change the selected rules, and you can also select or deselect active status options for new or existing organizations to make the selected rules active or inactive. This proves that both operations are available: severity changes and activation/deactivation changes. Option B is too restrictive because FortiSIEM allows multiple-rule selection. Option C is incomplete because activation/deactivation is also supported. Option D is incomplete because severity changes are also supported. Therefore, the correct answer is that you can change

severity and activate or deactivate multiple selected rules.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

What is the Group: FortiSIEM Analysts value referring to?

Options:

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

Answer:

C

Explanation:

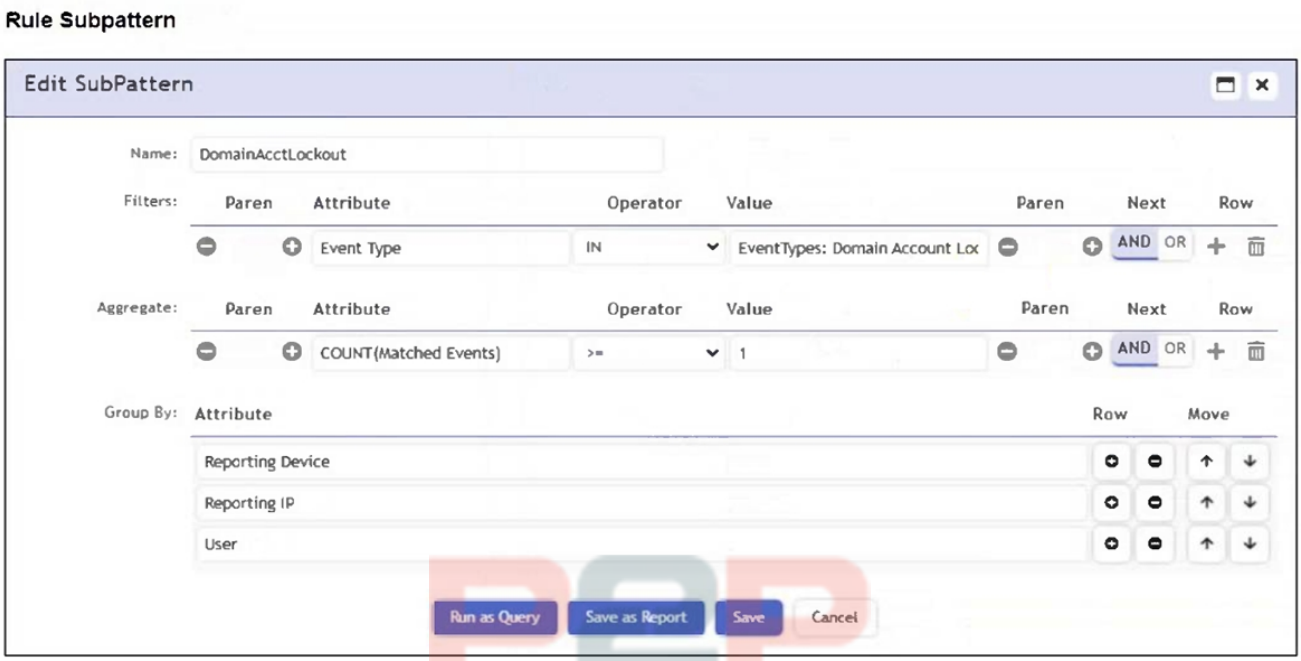
The correct answer is C. CMDB user group. In FortiSIEM, users and user groups are maintained as CMDB objects and can be referenced in analytics filters and rule logic. The FortiSIEM 7.4 User Guide table of contents explicitly includes CMDB management for users, viewing user information, adding users, editing or deleting users, performing operations on users, and

working with user groups. This confirms that user groups are part of the FortiSIEM CMDB data model. The query shown in the exhibit uses the Analytics filter with the User attribute and the value Group: FortiSIEM Analysts. That syntax indicates that FortiSIEM is referencing a FortiSIEM-defined user group from CMDB, not an LDAP group directly and not an Active Directory group directly. LDAP and Active Directory can be used to discover or authenticate users, but once referenced as a FortiSIEM analytics group value, the object is a CMDB user group. FortiSIEM organization groups are tenant/organization constructs and are not the same as CMDB user groups.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.



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

Options:

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

Answer:

A

Explanation:

The Aggregate section contains the condition COUNT(Matched Events) >= 1, which defines how many events must match the filter criteria for the rule to trigger. This is the subpattern configuration that determines the event threshold.

The correct answer is A. Aggregate. In FortiSIEM rule subpatterns, the Filter section defines which events are eligible for matching, but the Aggregate section defines the statistical or threshold condition that must be satisfied before the subpattern is considered matched. The Study Guide explains that rule conditions are built from subpatterns of event attribute filters and aggregation functions. It also states that a single-subpattern rule is formed by three fields: filters, aggregate, and group by. In the exhibit, the aggregate line is COUNT(Matched Events) >= 1. That expression directly specifies the number of matching events required to satisfy the subpattern. Group By only controls how matching events are partitioned into separate evaluation groups. Actions define what happens after a rule triggers, such as incident generation or notification. Filters define the event type or attribute criteria, but they do not define the required count threshold. Therefore, the section that determines how many matching events are needed is the Aggregate section.

Question 6

Question Type: MultipleChoice

You need to model for predicting a target based on other fields in the dataset and then trigger an anomaly if the value does not match the prediction.

Which machine learning algorithm will build this type of model?

Options:

A- Classification
B- Clustering
C- Regression
D- Forecasting

Answer:

C

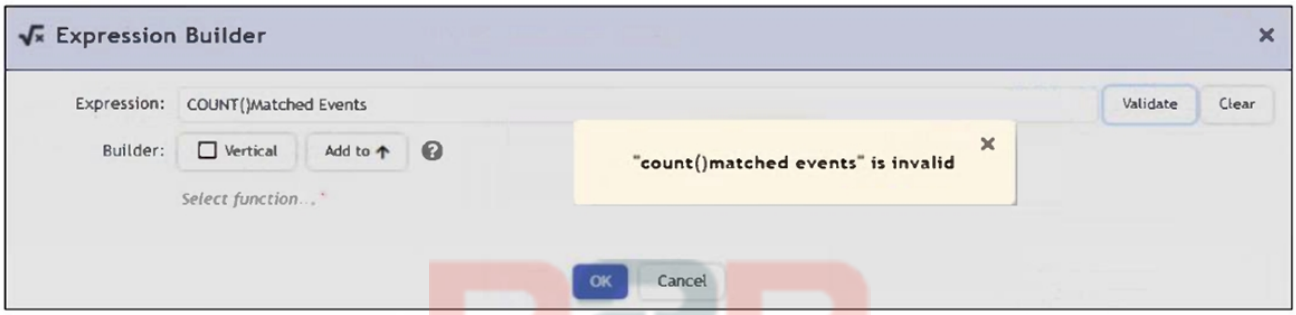
Explanation:

The correct answer is C. Regression. Regression is the machine learning task used when a model predicts a target value based on other fields in a dataset. In FortiSIEM's machine learning workflow, regression configuration includes selecting Fields to use for Prediction and a Field to Predict. The User Guide explains that during regression training, the analyst chooses the fields used for prediction and the field being predicted, then trains the model with a Train factor. This matches the question exactly: the model predicts a target based on other fields, and the inference phase can identify anomalies when observed values differ significantly from predicted values. Classification is used to assign records to discrete classes or categories, not to predict a continuous target metric from other variables. Clustering groups similar observations without a predefined target field. Forecasting predicts future values over time, normally based on time-series behavior. Because the question specifically describes predicting a target field from other dataset fields and detecting mismatch from the prediction, the correct machine learning method is Regression.

Question 7

Question Type: MultipleChoice

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?

Options:

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

Answer:

A

Explanation:

The correct syntax is COUNT(Matched Events) - with proper capitalization and spacing - to generate a total count of matched events. The error in the exhibit likely stems from a formatting issue (e.g., lowercase count() or incorrect spacing), not the logical structure of the expression.

COUNT(Matched Events). FortiSIEM uses aggregate functions inside rule subpatterns and analytics display fields to calculate values such as the number of matched events. The Study Guide explains that rule conditions are built from subpatterns of event attribute filters and aggregation functions. It also shows that the Aggregate section is where expressions such as COUNT(Matched Events) are used to define event-count thresholds. In the exhibit, the expression is intended to generate a total count of matched events. The proper function format is the aggregate function name followed by the target field inside parentheses. Therefore, COUNT(Matched Events) is syntactically valid. Options B, C, and D are invalid because they place the function name outside the standard function-call format or attach the argument incorrectly. This matters because FortiSIEM's Expression Builder validates expressions according to function syntax. To count matched events, the function must be written as an aggregate operation over the Matched Events field.

Question 8

Question Type: MultipleChoice

Which statement about thresholds is true?

Options:

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

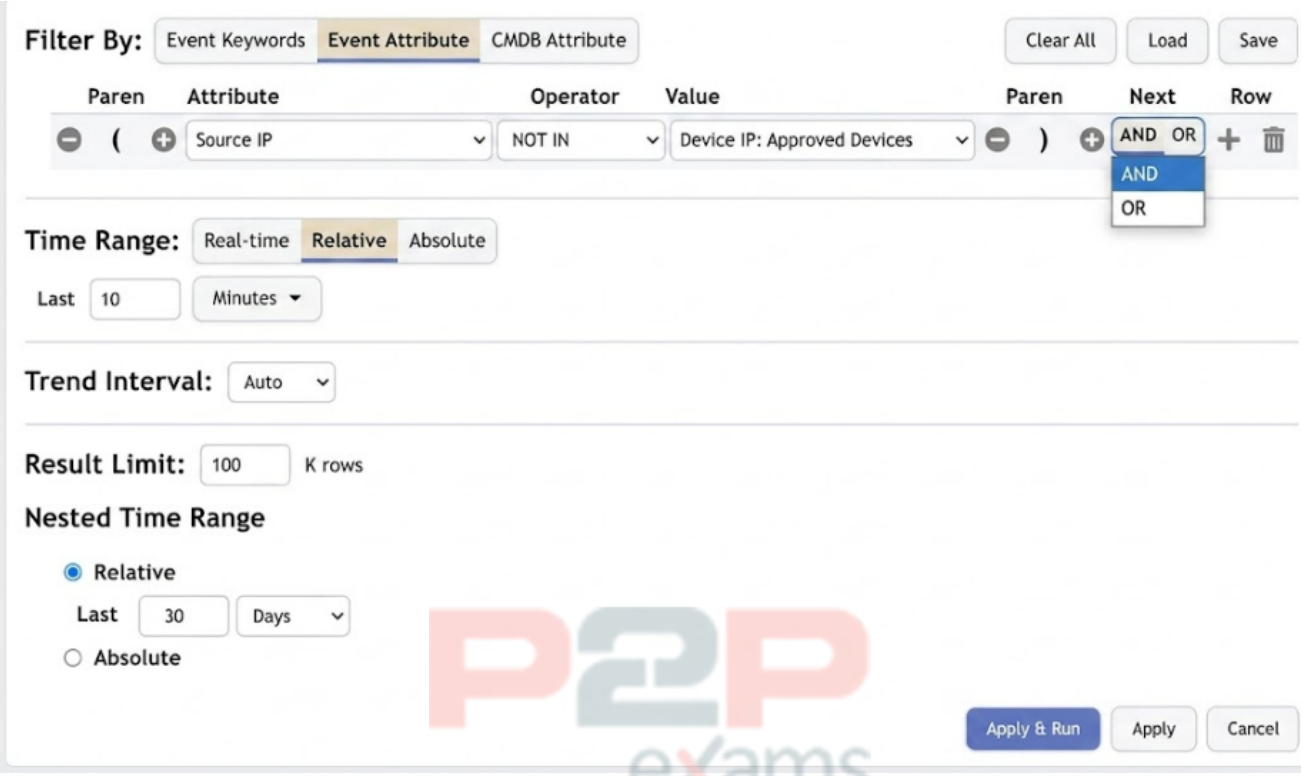
Explanation:

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.

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



Which statement about the time range settings defined in the nested query is accurate? (Select one answer)

Options:

A- FortiSIEM will list source IP addresses found in the last 10 minutes of events from each day in the Approved Devices report from the last 30 days.
B- FortiSIEM will search in real time using 10-minute blocks for a source IP address that is not in the Approved Devices report from the last 30 days.
C- FortiSIEM will search the last 30 days of events for a source IP address that is not in the

Approved Devices report.
D- FortiSIEM will search the last 10 minutes of events for a source IP address that is not in the Approved Devices report from the last 30 days.

Answer:

D

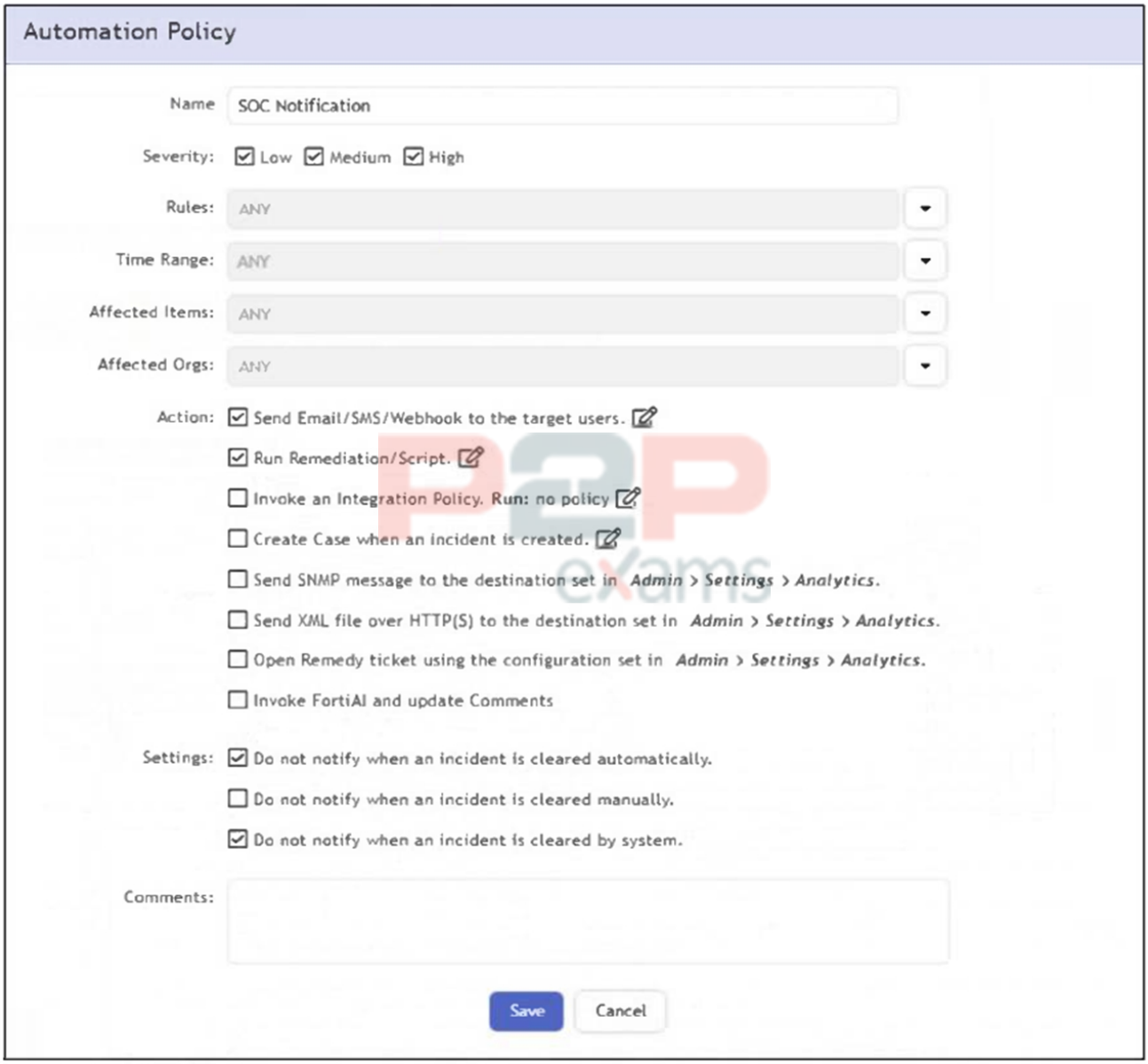
Explanation:

The correct answer is D. The exhibit shows an outer event query using the Event Attribute filter Source IP NOT IN Device IP: Approved Devices. The outer query time range is set to Relative --- Last 10 Minutes, so FortiSIEM searches only the event data from the last 10 minutes. The exhibit also shows a separate Nested Time Range set to Relative --- Last 30 Days. In FortiSIEM nested searches, the nested time range applies to the inner report/subquery, not to the outer event search. The FortiSIEM 7.4 User Guide states that nested query functionality lets one query refer to results from another query, and for outer event / inner event nested searches, it instructs the user to ''choose the time range for outer query'' and separately ''choose Nested Time Range for the inner query.'' It also states that when an existing query is used as an inner query, ''time range would be set separately'' in the outer query configuration. Therefore, FortiSIEM searches the last 10 minutes of outer events and compares their Source IP values against the Device IP values returned by the Approved Devices report using the last 30 days nested time range.

Question 10

Question Type: MultipleChoice

Refer to the exhibit.



What happens when an analyst clears an incident generated by a rule containing the automation policy shown in the exhibit?

Options:

A- No notification is sent.
B- An email is sent to the SOC manager.
C- The remediation script is run.
D- A notification is sent to the SOC manager dashboard.

Answer:

B

Explanation:

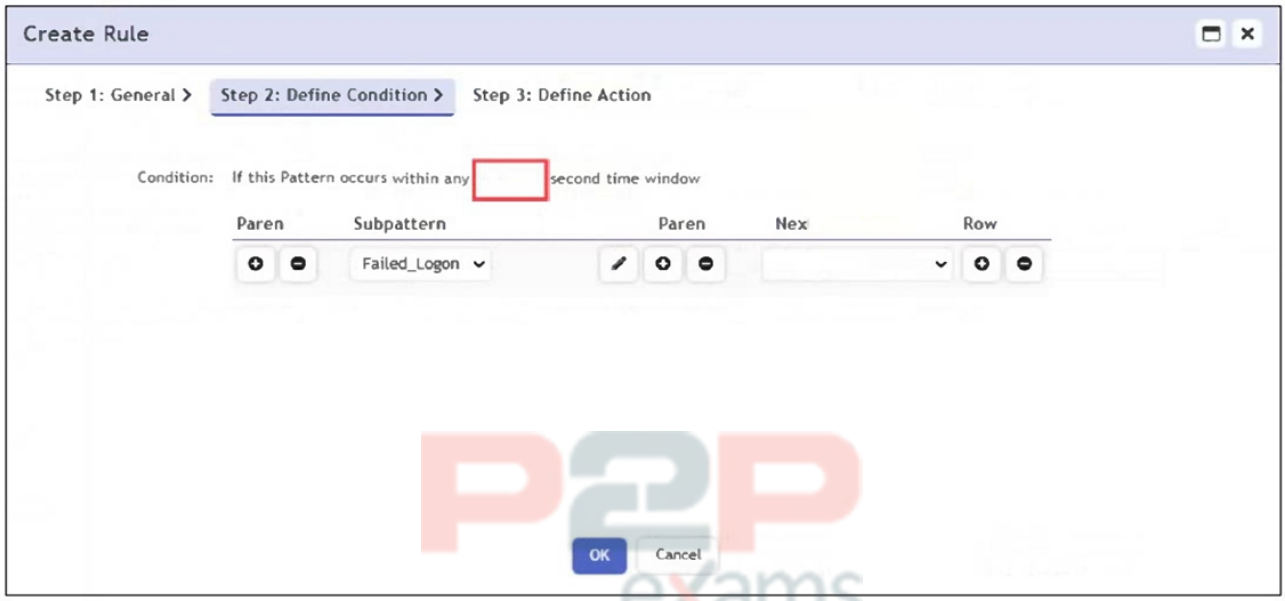
The correct answer is B because the automation policy shown has the email/SMS/webhook notification action enabled, and the setting that suppresses notification for manual incident clearing is not selected. The FortiSIEM Study Guide explains that automation policies define actions taken when incident-related policy criteria match. It states that notification policies are defined by criteria such as severity, associated rules, time range, affected items, and actions. The guide also states that FortiSIEM can send email notifications and SMS messages to individuals or groups as part of an automation policy. In the exhibit, the options Do not notify when an incident is cleared automatically and Do not notify when an incident is cleared by system are selected, but Do not notify when an incident is cleared manually is not selected. Because the analyst clears the incident manually, the suppression condition does not apply. Therefore, FortiSIEM sends the configured email notification to the target user, identified in the question as the SOC manager.

Question 11

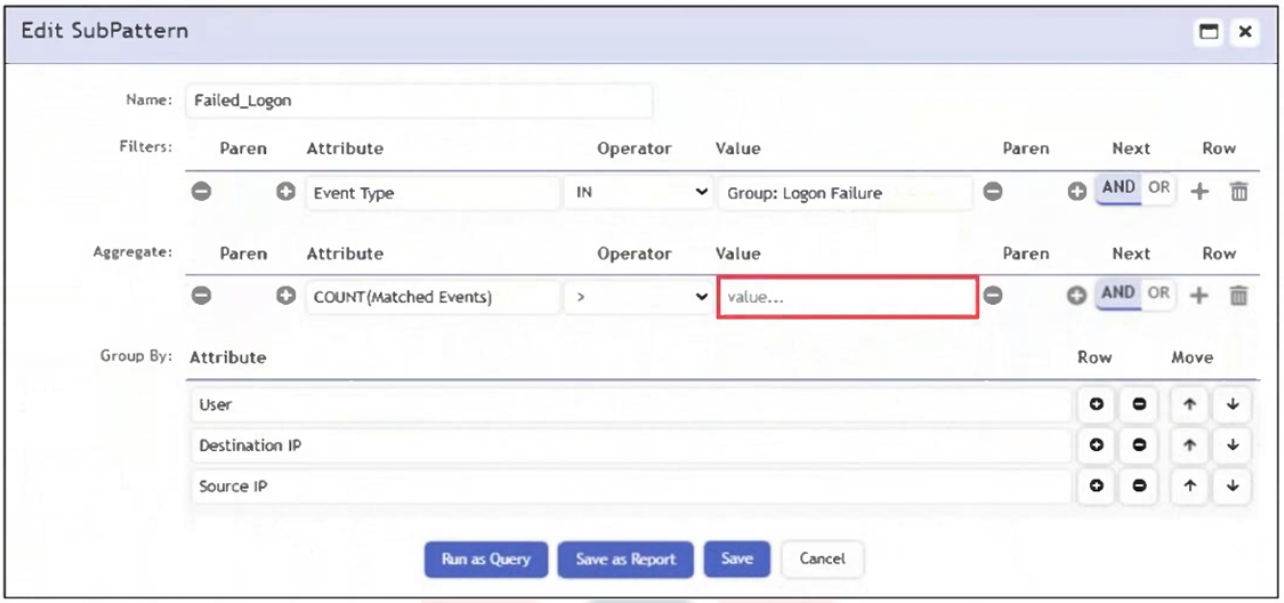
Question Type: MultipleChoice

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?

Options:

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

Explanation:

To detect three failed login attempts within three minutes, you must set the aggregate count to 3 in the subpattern and the time window to 180 seconds in the rule condition. This ensures the rule triggers only if three or more failed logins occur in that timeframe.

The correct answer is A because three minutes equals 180 seconds, and the aggregate threshold must be set to three matching events. The FortiSIEM Study Guide explains that rule conditions specify event attributes and thresholds that trigger the rule and create an incident. It further states that the time window defines the period within which the subpattern must match for the rule condition to be satisfied. The Study Guide's single-subpattern rule example shows the same principle: the condition has a configured time window, and the Aggregate section uses a function such as COUNT(Matched Events) to require a minimum number of matching events. In this question, the analyst wants the rule to trigger when three failed login attempts happen within three minutes. Therefore, the rule condition time window must be 180 seconds, and the aggregate count must be 3. A 90-second window would detect only events inside one and a half minutes, not the required three minutes. An aggregate count of 2 would trigger too early because the requirement is three failed attempts.