Prepare Smart for Success Free Fortinet NSE6_FSM_AN-7.4 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 6 - FortiSIEM 7.4 Analyst exam PDF questions now. Get authentic NSE6_FSM_AN-7.4 dumps packed with verified answers and secure your certification success with PrepBolt NSE6_FSM_AN-7.4 exam pdf questions and answers.

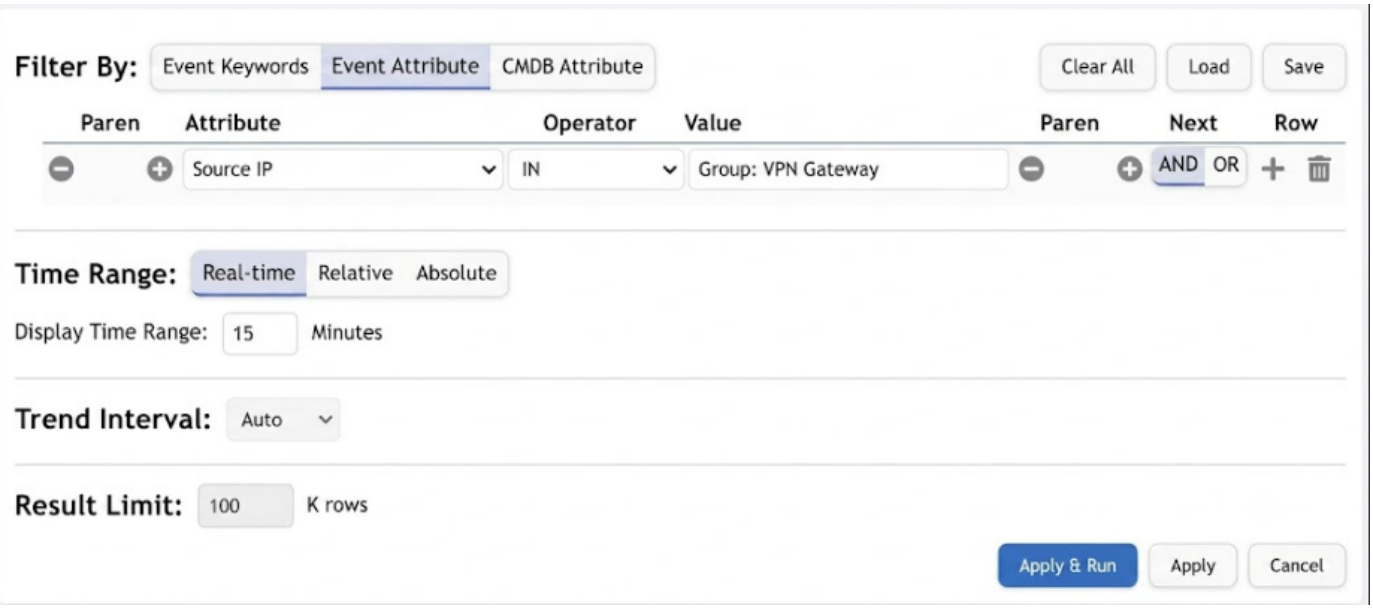
Thank you for Downloading NSE6_FSM_AN-7.4 exam PDF Demo

https://prepbolt.com/NSE6_FSM_AN-7.4.html

Question 1

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:

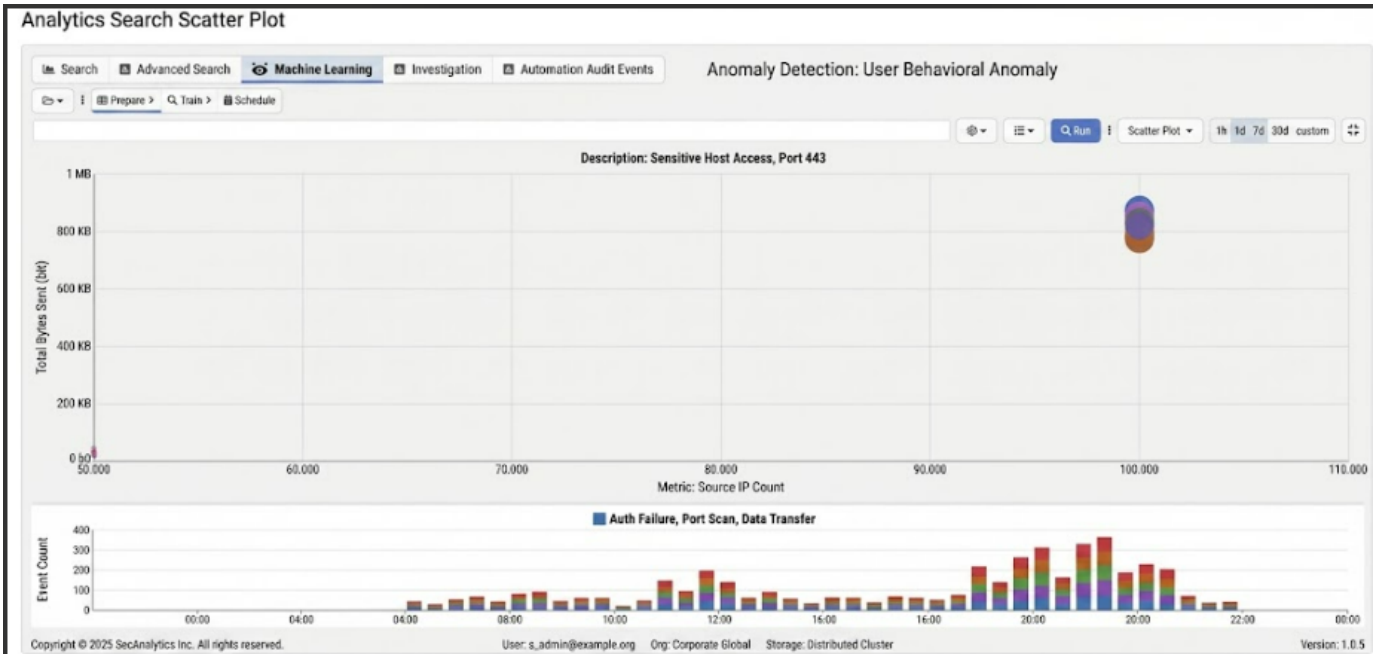
The correct answer is A. A configuration management database (CMDB) device group. In the exhibit, the analytics filter uses Source IP IN Group: VPN Gateway. In FortiSIEM analytics, values shown as Group: for IP/device-related attributes commonly reference FortiSIEM CMDB groups, not firewall address groups 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 2

Question Type: MultipleChoice

Refer to the exhibit.



An analyst wants to perform a KMeans machine learning (ML) job on this data. How many N clusters would be a good fit for the data? (Choose one answer)

Options:

A- Two
B- 50
C- 100
D- One

Answer:

A

Explanation:

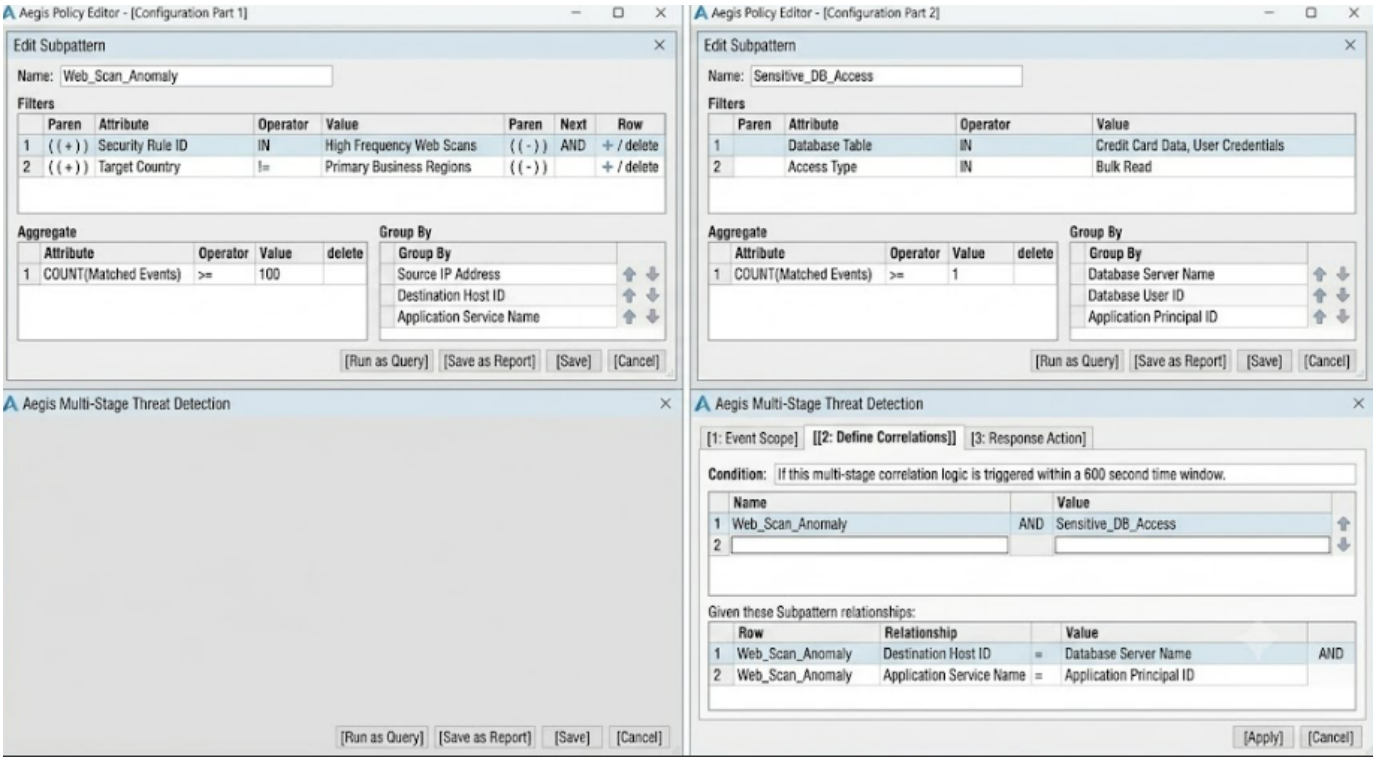
The best answer is A. Two. The exhibit shows an Analytics Search scatter plot with two visually distinct groups of data points: one isolated group around the lower-left area of the chart and another dense group near the upper-right area. For KMeans clustering, the analyst must provide the number of clusters based on the observed structure of the data. The FortiSIEM 7.4 User Guide describes KMeans as ''an unsupervised clustering algorithm that groups data points into user specified K groups so that each data point belongs to one group.'' It also states that KMeans ''tries to iteratively minimize intra-cluster distance and maximize inter-cluster distance'' and notes that the user must ''specify the number of clusters based on user's knowledge of data.''

The same FortiSIEM guide explains that during Clustering Local Mode training, the analyst chooses the algorithm and, ''for KMeans choose the cluster size as a guess.'' In this exhibit, the natural guess is 2, because the scatter plot separates into two obvious groups. Fifty or 100 clusters would overfit the small number of visible groups, while one cluster would merge two clearly separate behaviors into a single cluster.

Question 3

Question Type: MultipleChoice

Refer to the exhibits.



You are troubleshooting why the rule shown in the exhibit is generating incidents for successful Remote Desktop Protocol (RDP) connections with correct logins. It should only be triggering when a person fails to log in three or more times to the target device when connecting with RDP.

What is causing the rule to be triggered by correct login events? (Choose one answer)

Options:

A- The subpattern relationship RDP_Connection:User = Failed_Logon:User never matches.
B- The Boolean between the subpatterns is incorrect.
C- The attribute types in the subpatterns do not match.
D- The RDP login is different from the login used to access the target device.

Answer:

B

Explanation:

The rule is triggering on successful RDP connection events because the Next operator between the two subpatterns is set to OR. The FortiSIEM Study Guide explains that multiple subpattern rules are used when patterns must occur within a specific time period or when one of several patterns proves that an incident condition exists. It lists the OR operator as: ''Subpattern X OR Subpattern Y occurred within the Time Window.'' The same Study Guide further explains that if multiple patterns are used, FortiSIEM requires a next operator, and in the OR example, ''an event that matches either'' subpattern will trigger. It also states that because the next operator is OR, the constraint between the two subpatterns is not enforced.

In the exhibit, Subpattern 1 matches RDP traffic on TCP/UDP port 3389 from FortiGate traffic-forward events, while Subpattern 2 matches logon failure events with COUNT(Matched Events) >= 3. Because the rule uses OR, FortiSIEM can trigger when only the RDP connection subpattern matches, even if the failed-logon subpattern does not match. The correct logic should require both subpatterns to match with the intended relationship constraints, not either subpattern independently.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

Which two actions can you select in an automation policy to trigger an API call to block an IP address on a FortiGate? (Choose two.)

Options:

A- Open Remedy ticket using the configuration set in Analytics.
B- Send Email/SMS/Webhook to the target users.
C- Invoke an Integration Policy.
D- Run Remediation/Script.
E- Run Playbook on Incident Trigger.

Answer:

D, E

Explanation:

The correct answers are D. Run Remediation/Script and E. Run Playbook on Incident Trigger. FortiSIEM can block an IP address on a FortiGate through a remediation script or through a FortiSOAR playbook/connector workflow. The FortiSIEM Analyst Study Guide explains that for automatic remediation, you define a remediation script for a scenario, and that mitigation scripts can ''block an IP address in a firewall'' or disable a user in Active Directory. It also states that, when an automation policy is triggered and the remediation script option is enabled, FortiSIEM uses incident data and runs the script to quarantine or block the offending IP address on FortiGate.

FortiSIEM 7.4 also supports automatic playbook execution from an automation policy. The 7.4 User Guide states that under Admin > Settings > Automation Policy, you can choose Run Playbook on Incident Trigger and select a playbook. The same guide explains that FortiSOAR playbooks can call connectors, and the Fortinet FortiOS connector can perform actions such as Block IP Address on a FortiGate firewall.

Email, Remedy tickets, and generic integration policies are notification/ticketing workflows, not the direct FortiGate IP-block actions.

Question 5

Question Type: MultipleChoice

You want to create a rule with multiple subpatterns but trigger an incident only if three different subpatterns are matched over a 24-hour period.

Where must you define the time period that the rule uses to evaluate all the subpatterns? (Choose one answer)

Options:

A- Define the time window in each individual subpattern.
B- Define the time window under the General tab of the rule.
C- Define the time window under the Define Condition tab of the rule.
D- Define the time window in the Define Action section of the rule.

Answer:

C

Explanation:

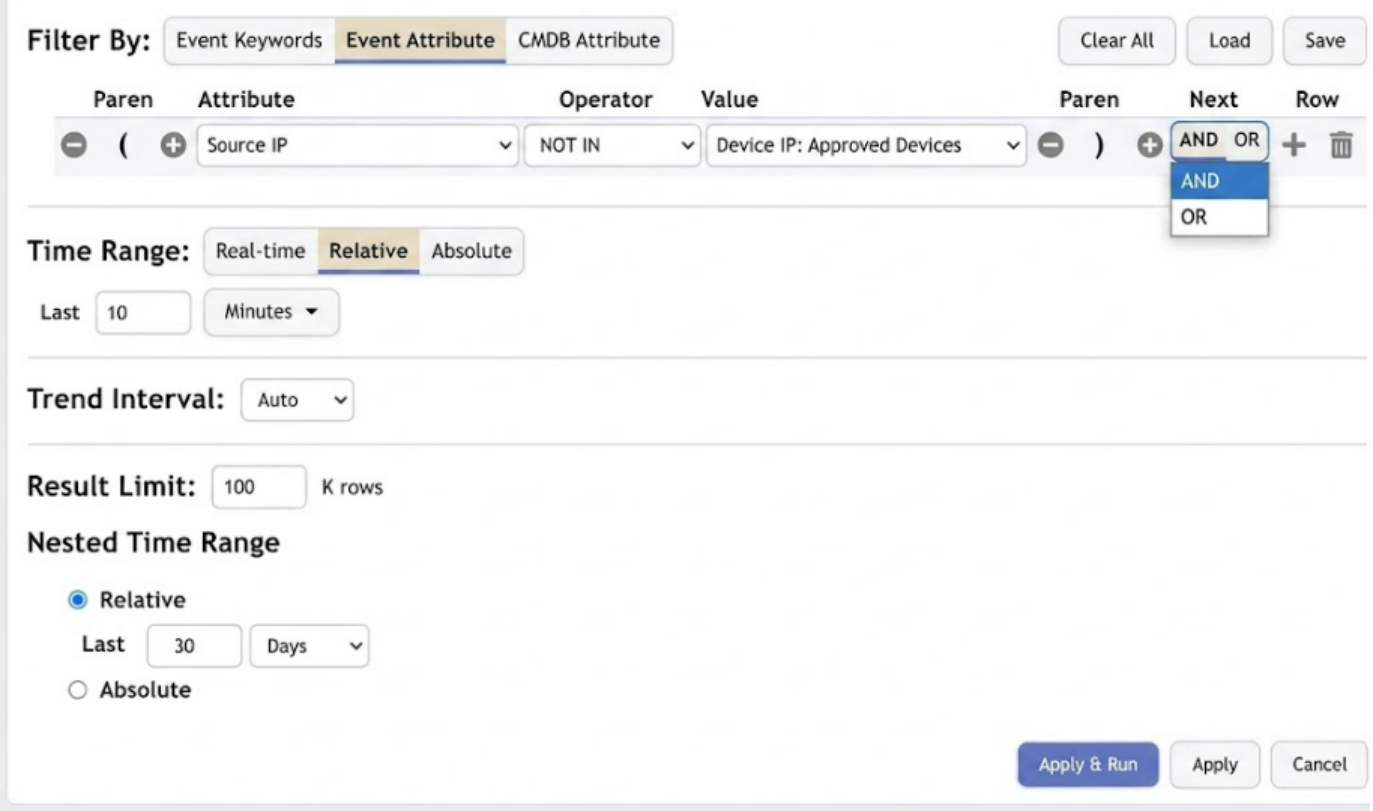
The time period must be defined under the Define Condition tab of the rule. The FortiSIEM Study Guide states that a rule has three components: General, Condition, and Action. The General section defines the overall purpose and scope of the rule, the Condition section specifies which conditions trigger the rule, and the Action section configures what happens after the rule is triggered. The Study Guide further explains that on the Define Condition page, FortiSIEM specifies ''the conditions---event attributes and thresholds---that will trigger the rule and create an incident,'' including ''the time window'' within which the subpatterns must match for the rule condition to be satisfied. It also states that when there is more than one subpattern, you must define the logic between subpatterns and their relationships or constraints.

For a 24-hour multiple-subpattern rule, the guide gives an example using an 86400-second time window, which equals 24 hours, and shows it under Resource > Rules > Define Condition. Therefore, the time period is not configured inside each individual subpattern, not under General, and not under Define Action.

Question 6

Question Type: MultipleChoice

Refer to the exhibit.



Which statement about the time range settings defined in the nested query is accurate? (Choose 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 7

Question Type: MultipleChoice

When configuring machine learning (ML), in which step can you modify how the model fits the training data set?

Options:

A- Prepare Data
B- Train
C- Statistics
D- Design

Answer:

B

Explanation:

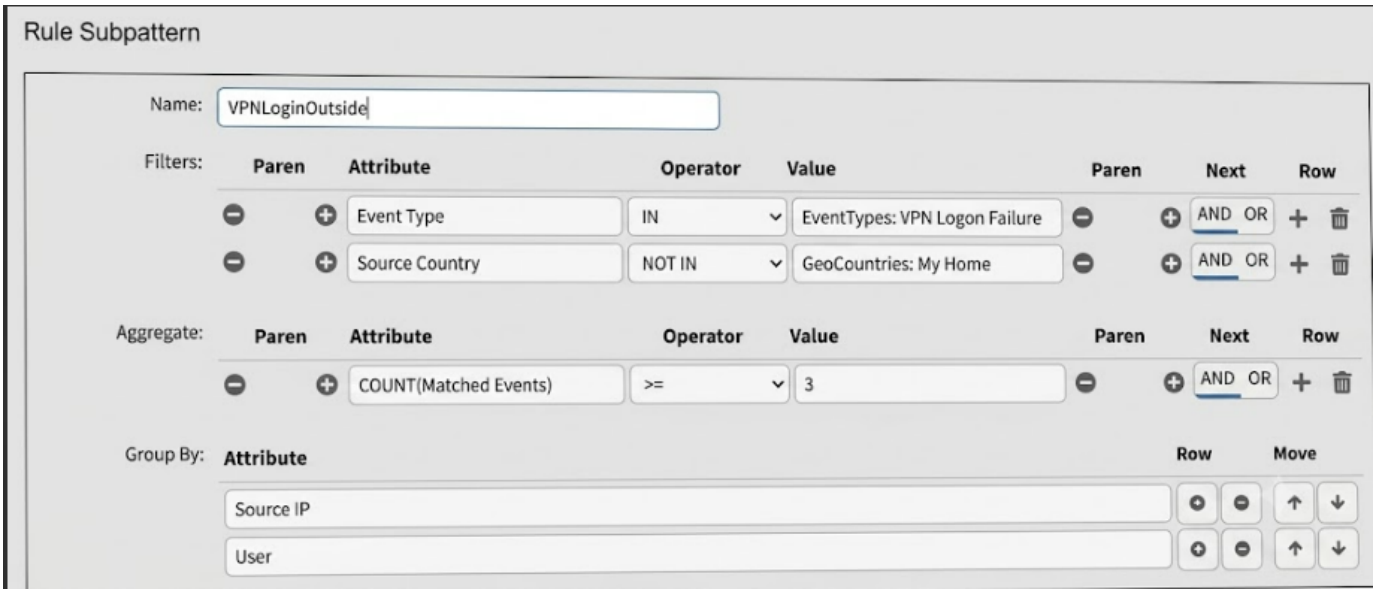
The correct answer is B. Train. In FortiSIEM machine learning, the Train step is where the model is built from the prepared dataset and where model-fitting behavior can be adjusted. The FortiSIEM 7.4 User Guide explains that after preparing data, the analyst goes to Analytics > Machine Learning > Train, selects the machine learning task, chooses the algorithm, selects the prediction/target fields when required, and chooses the Train factor, which determines how much data is used for training versus testing. The guide states that the Train factor should be greater than 70%, meaning 70% of the data is used for training and 30% for testing. It also explains that model quality metrics show how accurately

the algorithm predicts the field. For regression, lower MAE means a better fit, and R2 shows how well predictions approximate real data points. Most importantly, the guide states: ''If you want to change the algorithm parameters and re-train, then click Tune & Train, change the parameters and click Save & Train.'' This confirms that modifying how the model fits the training dataset is done in the Train step, not Prepare Data, Statistics, or Design.

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



What is this rule attempting to match? (Choose one answer)

Options:

A- Failed VPN logon attempts from three or more different outside countries.
B- Failed VPN logon events from a source outside the home country.
C- Failed VPN logon attempts from three or more different sources inside the home country.
D- Excessive VPN logon failures from a source inside the home country.

Answer:

B

Explanation:

The rule is matching VPN logon failure events where the Source Country is outside the configured

home country. In the exhibit, the filter section shows Event Type IN EventTypes: VPN Logon Failure and Source Country NOT IN GeoCountries: My Home. That means the source must be outside the home-country geo group. The aggregate condition shows COUNT(Matched Events) >= 3, so the rule is looking for at least three matching failed VPN logon events. The Group By section uses Source IP and User, so FortiSIEM evaluates the count per unique source IP and user combination, not by different countries.

The FortiSIEM Study Guide explains that a rule subpattern contains three components: Filter, Aggregate, and Group By. It states that the filter identifies the matching event group, the aggregate function specifies how many events must match, and Group By combines events with the same grouped attributes into one row while the count tracks those events.

Option A is wrong because the rule does not count different countries. Options C and D are wrong because the source country is explicitly NOT IN My Home, not inside the home country.

Question 9

Question Type: MultipleChoice

In an automation policy, which two methods can you use to notify analysts when an incident is triggered? (Choose two.)

Options:

A- Email
B- FortiSIEM Case
C- Syslog
D- Pop-up window

Answer:

A, B

Explanation:

The correct answers are A. Email and B. FortiSIEM Case. FortiSIEM automation policies can notify or route work to analysts when an incident is triggered. The Study Guide describes the incident notification email workflow and explains that when an incident triggers and an automation policy is defined, FortiSIEM can send a notification email using the default template. It also explains that notification frequency is configured per rule and that repeated incident notifications are controlled by the frequency timer. The FortiSIEM 7.4 User Guide also describes automated case creation through automation policy. It states that an automation policy can use the action Create Case when an incident

is created, and that a case management policy can assign FortiSIEM Analyst Teams in an ordered handling sequence. Syslog is not listed as one of the analyst notification methods in the automation policy options shown in this question; FortiSIEM supports SNMP and webhook-style actions, but not ''Syslog'' as the listed answer. A pop-up window is not an automation policy notification method. Therefore, the two correct analyst-notification/routing methods are Email and FortiSIEM Case.

Thank You for trying NSE6_FSM_AN-7.4 PDF Demo

To try our NSE6_FSM_AN-7.4 practice exam software visit link below

https://prepbolt.com/NSE6_FSM_AN-7.4.html

Start Your NSE6_FSM_AN-7.4 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE6_FSM_AN-7.4 preparation with actual exam questions.