NSE6_FSM_AN-7.4 Schulungsangebot - NSE6_FSM_AN-7.4 Online Prüfungen

Wünschen Sie jetzt die früheren Prüfungsfragen und Nachschlagebücher von Fortinet NSE6_FSM_AN-7.4 Zertifizierungsprüfungen? Sie haben nicht genug Zeit, die Fortinet NSE6_FSM_AN-7.4 Zertifizierungsprüfung vorzubereiten, wenn Sie sich mit der Arbeit beschäftigt sind. Deshalb ist es sehr wichtig für Sie, hocheffektive Prüfungsunterlagen auszuwählen. Deshalb ist es sehr wichtig, ein richtiges Lerngerät zu wählen. Wählen Sie bitte Fortinet NSE6_FSM_AN-7.4 Dumps von EchteFrage.

Fortinet NSE6_FSM_AN-7.4 Exam Syllabus Topics:

Section	Objectives
FortiEDR Security Settings and Policies	- Security configuration • 1. Configure communication control policy • 2. Configure playbooks • 3. Configure security policies • 4. Explain Fortinet Cloud Service (FCS)
Rules and Subpatterns	- Analytics rules configuration • 1. Configure FortiSIEM analytics rules • 2. Use rule subpatterns, aggregation, and group by • 3. Identify rule components
Incidents, Notifications, and Remediation	- Incident management • 1. Configure remediation options • 2. Configure notification policies • 3. Manage and tune incidents
Machine Learning, UEBA, and ZTNA	- Advanced analytics integration • 1. Describe ZTNA integration in FortiSIEM operations • 2. Configure ML configuration tasks • 3. Integrate UEBA data into rules and dashboards

Analytics	- Query and event analysis • 1. Build queries from search results and events • 2. Perform nested query lookups • 3. Apply group by and data aggregation on search results • 4. Perform CMDB and lookup table queries

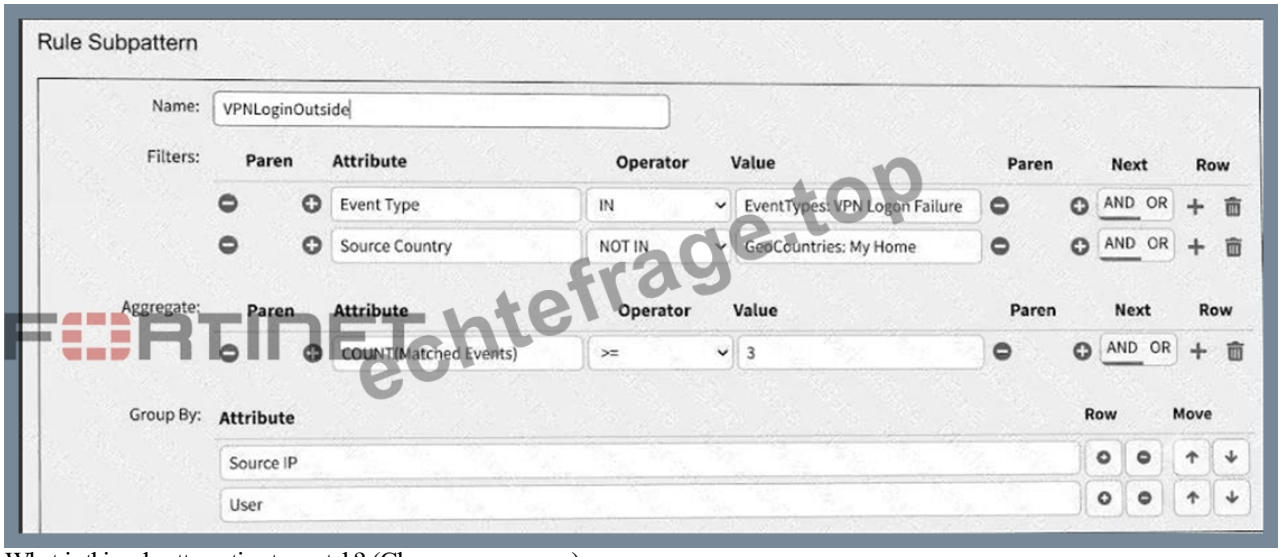
>> NSE6_FSM_AN-7.4 Schulungsangebot <<

NSE6_FSM_AN-7.4 Studienmaterialien: Fortinet NSE 6 - FortiSIEM 7.4 Analyst & NSE6_FSM_AN-7.4 Zertifizierungstraining

Manchmal muss man mit große Menge von Prüfungsaufgaben üben, um eine wichtige Prüfung zu bestehen. Die Fortinet NSE6_FSM_AN-7.4 von uns hat diese Forderung gut erfüllt. Und mit den fachlichen Erklärungen können Sie besser die Antworten verstehen. Die Demo der Fortinet NSE6_FSM_AN-7.4 von unterschiedlichen Versionen werden von uns gratis angeboten. Probieren Sie mal und wählen Sie die geeignete Version für Sie! Mit unserer gemeinsamen Arbeit werden Sie bestimmt die Fortinet NSE6_FSM_AN-7.4 Prüfung erfolgreich bestehen!

Fortinet NSE 6 - FortiSIEM 7.4 Analyst NSE6_FSM_AN-7.4 Prüfungsfragen mit Lösungen (Q68-Q73):

68. Frage
Refer to the exhibit.



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

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

Antwort: A

Begründung:
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.

69. Frage
You want to build an event query that displays only events to higher number destination ports (1024-65535). Which analytic search string is valid for this scenario?

- A. Destination TCP/UDP Port >= 1024 AND Destination TCP/UDP Port <= 65535
- B. Destination TCP/UDP Port > 1024
- C. Destination TCP/UDP Port = 1024-65535
- D. Destination TCP/UDP Port BETWEEN 1024-65535

Antwort: A

Begründung:
FortiSIEM analytic searches support explicit comparison operators. Using greater-than-or-equal- to and less-than-or-equal-to conditions correctly defines the valid destination port range from
1024 through 65535.

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

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

Antwort: B,D

Begründung:
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.

71. Frage
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. Five
- B. Four
- C. Three
- D. Two
- E. Six

Antwort: E

Begründung:
Grouping by User, Source IP, and Count means that each unique combination of those three attributes will be treated as a separate result. In the table, all six rows have distinct combinations of User, Source IP, and Count
- so FortiSIEM will display 6 results.
Six because grouping by User , Source IP , and Count creates a separate result for every unique combination of those three selected attributes. The FortiSIEM Study Guide explains this grouping behavior in the single- subpattern rule example: "If multiple VPN login failure events have the same source IP address, reporting device, reporting IP address, and user, they are grouped together in one row, and the count column tracks the number of events for each of those rows." Applying that rule here, FortiSIEM compares all selected Group By fields together. In the exhibit, every row has a unique Source IP address, even where the same user appears more than once. For example, Mike appears twice, but the Source IP and Count values are different. Alice appears twice with Count 2, but the Source IP values are different. Bob appears twice, but both Source IP and Count are different. Since no row has the same User, Source IP, and Count combination as another row, FortiSIEM displays all six rows.

72. Frage
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)

Antwort: A

Begründung:
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.

73. Frage
.....

Seit Jahren ist Fortinet NSE6_FSM_AN-7.4 Prüfung eine sehr populäre Prüfung. Heutzutage wird Fortinet Zertifizierung immer wichtiger. Als von IT-Industrie international anerkannte Prüfung wird NSE6_FSM_AN-7.4 eine der wichtigsten Prüfungen in Fortinet. Sie können viele Vorteile bekommen, wenn Sie das NSE6_FSM_AN-7.4 Zertifikat bekommen. Fortinet NSE6_FSM_AN-7.4 Dumps von EchteFrage gilt als das unentbehrliche Gerät, womit Sie die Fortinet NSE6_FSM_AN-7.4 Prüfung vorbereiten, weil es den besten Nachschlag für Fortinet NSE6_FSM_AN-7.4 Zertifizierungsprüfung ist.

- NSE6_FSM_AN-7.4 Fragen&Antworten □ NSE6_FSM_AN-7.4 Unterlage □ NSE6_FSM_AN-7.4 Online Prüfungen □ URL kopieren ▹ de.fast2test.com ◃ Öffnen und suchen Sie ▸ NSE6_FSM_AN-7.4 ◂ Kostenloser Download □NSE6_FSM_AN-7.4 Testing Engine
- www.stes.tyc.edu.tw, www.slideshare.net, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.zazzle.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.grunnboek.nl, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, scalar.usc.edu, Disposable vapes