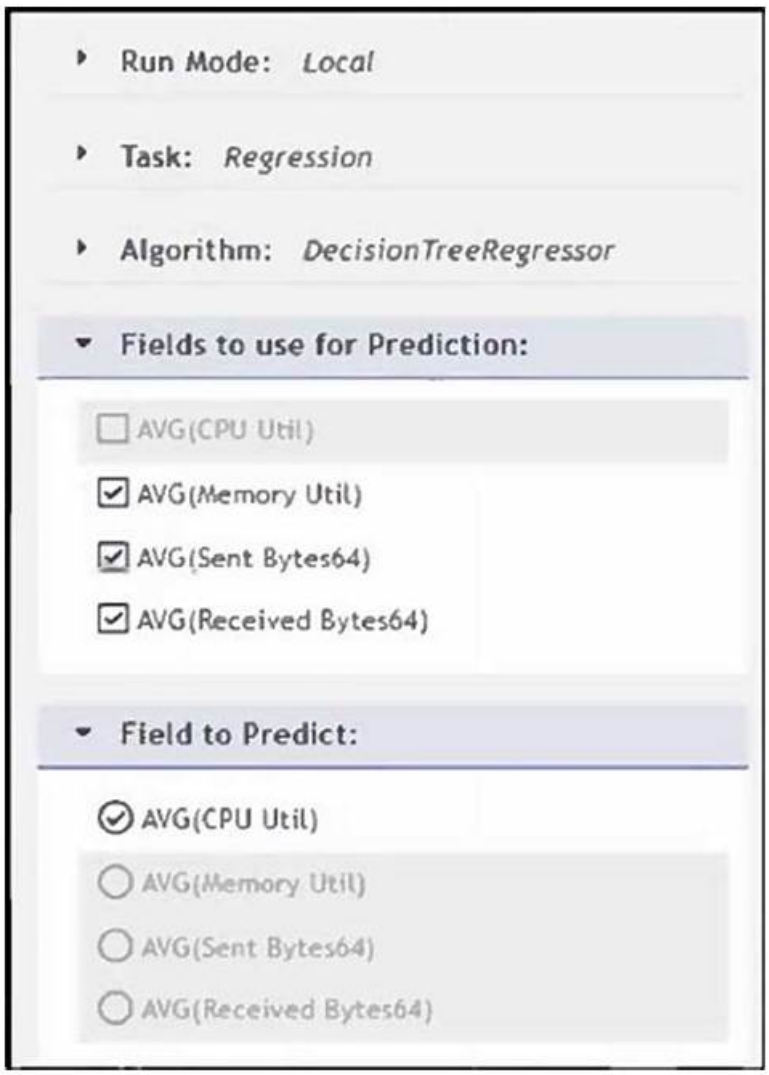
FCP_FSM_AN-7.2 Accurate Test | FCP_FSM_AN-7.2 Valid Exam Online



Our FCP_FSM_AN-7.2 test questions provide free trial services for all customers so that you can better understand our products. You can experience the effects of outside products in advance by downloading clue versions of our FCP_FSM_AN-7.2 exam torrent. In addition, it has simple procedure to buy our learning materials. After your payment is successful, you will receive an e-mail from our company within 10 minutes. After you click on the link and log in, you can start learning using our FCP_FSM_AN-7.2 test material. You can download our FCP_FSM_AN-7.2 test questions at any time.

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

Topic	Details
Topic 1	• Incidents, notifications, and remediation: This section of the exam measures the skills of Incident Responders and encompasses the entire incident management lifecycle. This includes the skills required to manage and prioritize security incidents, configure policies for alert notifications, and set up automated remediation actions to contain and resolve threats.

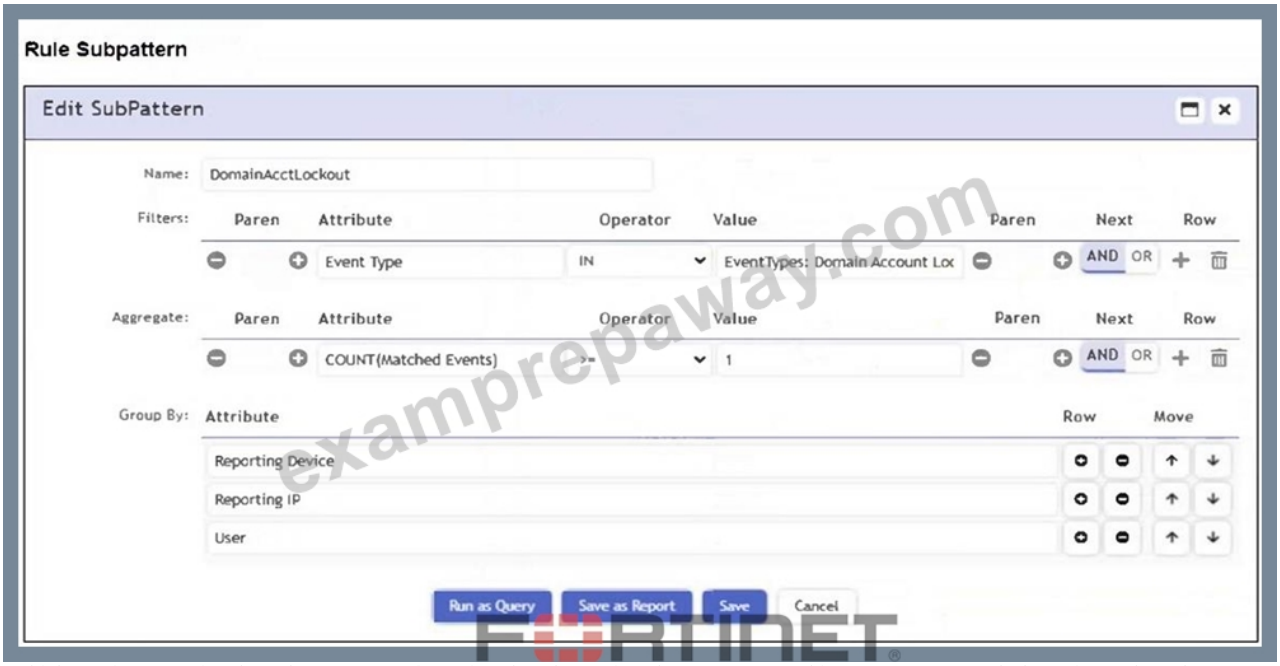
Topic 2	• Machine learning, UEBA, and ZTNA: This section of the exam measures the skills of Advanced Security Architects and covers the integration of modern security technologies. It involves performing configuration tasks for machine learning models, incorporating UEBA (User and Entity Behavior Analytics) data into rules and dashboards for enhanced threat detection, and understanding how to integrate ZTNA (Zero Trust Network Access) principles into security operations.
Topic 3	• Rules and subpatterns: This section of the exam measures the skills of SOC Engineers and focuses on the construction and implementation of analytics rules. It involves identifying the different components that make up a rule, utilizing advanced features like subpatterns and aggregation, and practically configuring these rules within the FortiSIEM platform to detect security events.
Topic 4	• Analytics: This section of the exam measures the skills of Security Analysts and covers the foundational techniques for building and refining queries. It focuses on creating searches from events, applying grouping and aggregation methods, and performing various lookup operations, including CMDB and nested queries to effectively analyze and correlate data.

2025 FCP_FSM_AN-7.2 Accurate Test | High Pass-Rate FCP_FSM_AN-7.2: FCP - FortiSIEM 7.2 Analyst 100% Pass

ExamPrepAway also offers simple and easy-to-use FCP - FortiSIEM 7.2 Analyst (FCP_FSM_AN-7.2) Dumps PDF files of real Fortinet FCP_FSM_AN-7.2 exam questions. It is easy to download and use on smart devices. Since it is a portable format, it can be used on a smartphone, tablet, or any other smart device. This FCP - FortiSIEM 7.2 Analyst (FCP_FSM_AN-7.2) PDF file contains the most probable actual FCP - FortiSIEM 7.2 Analyst (FCP_FSM_AN-7.2) exam questions.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q32-Q37):

NEW QUESTION # 32
Refer to the exhibit.



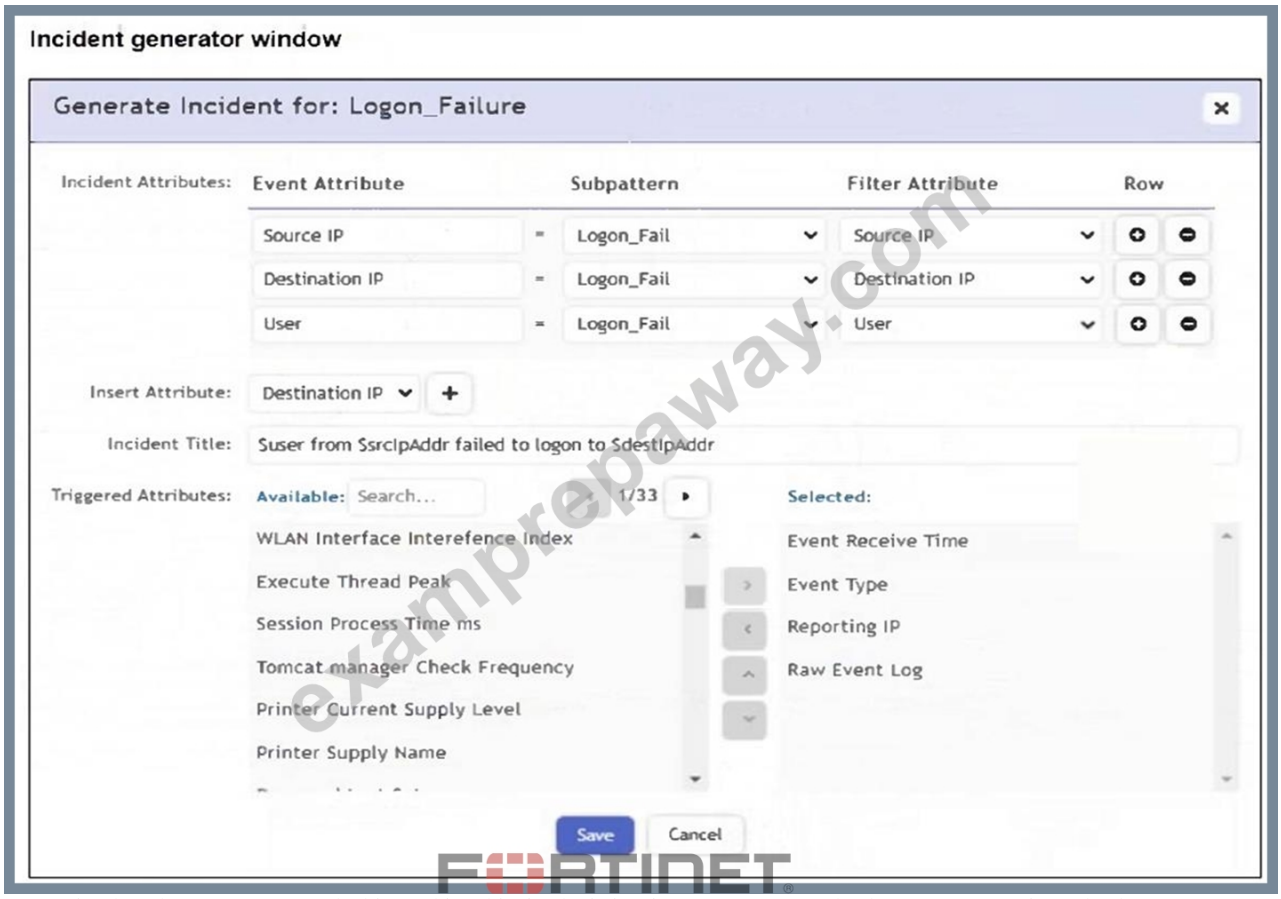
Which section contains the subpattern configuration that determines how many matching events are needed to trigger the rule?

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

Answer: B

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.

NEW QUESTION # 33
Refer to the exhibit.



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

Answer: D

Explanation:
For an attribute like Destination Host Name to be used in the incident title, it must first be included in the Triggered Attributes list. Only attributes listed there are available for substitution in the title template (e.g., $destIpAddr, $srcIpAddr).

NEW QUESTION # 34
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. Six
- C. Two
- D. Five
- E. One

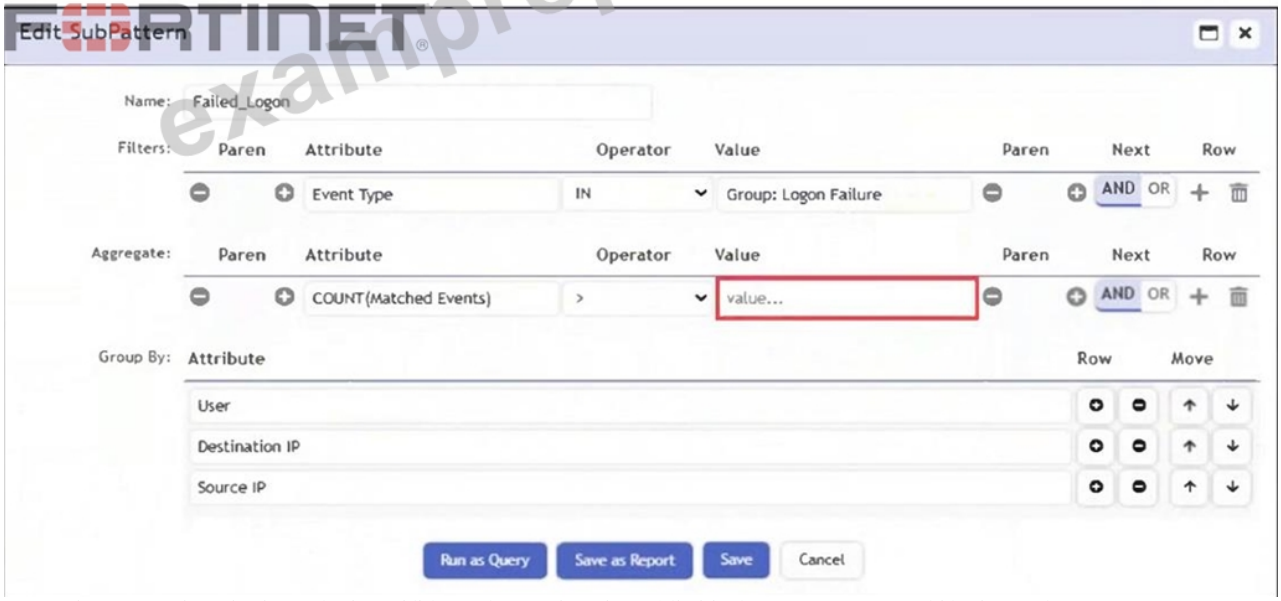
Answer: D

Explanation:
Grouping by Reporting Device, Reporting IP, and Application Category yields five unique tuples: (FW01, 10.1.1.1, DB), (FW02, 10.1.1.2, WebApp), (FW01, 10.1.1.1, SSH), (FW03, 10.1.1.3, DB), and (FW04, 10.1.1.4, SSH).

NEW QUESTION # 35
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?

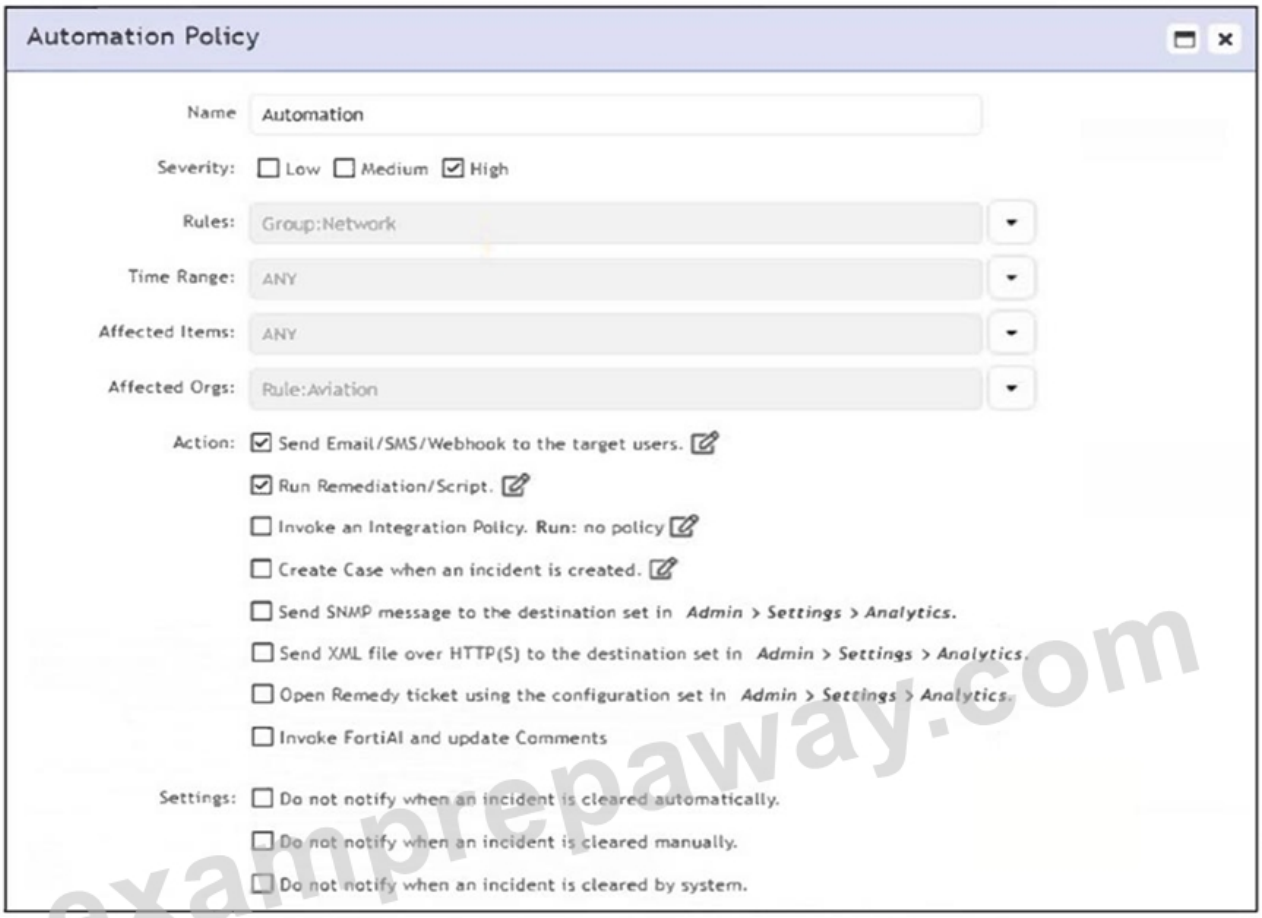
- A. Time window 90 seconds, aggregate count 2
- B. Time window 90 seconds, aggregate count 3
- C. Time window 180 seconds, aggregate count 2
- D. Time window 180 seconds, aggregate count 3

Answer: D

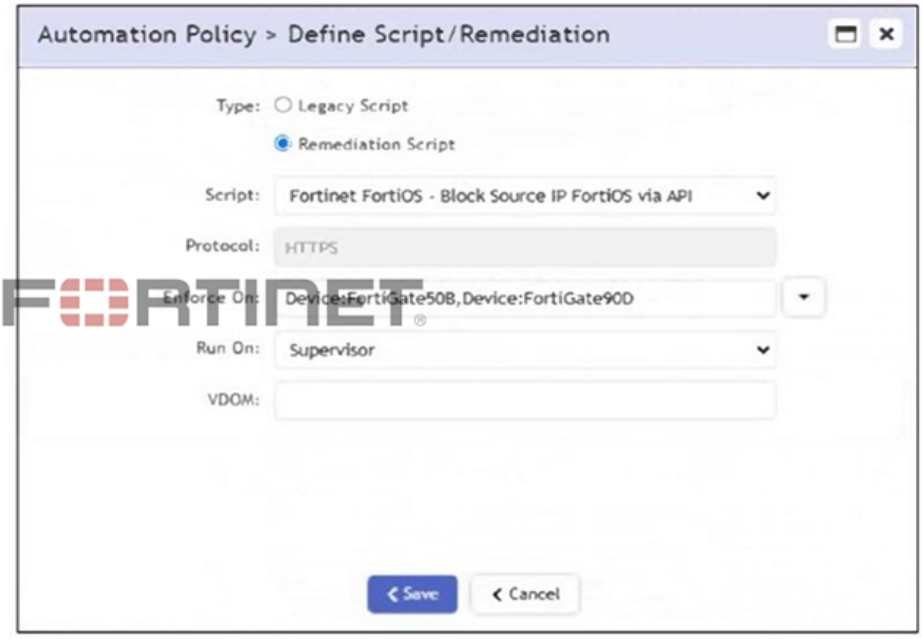
Explanation:
To detect three failed login attempts within three minutes, you must set the aggregate count to 3 in the subpattern and the time window to 180 seconds in the rule condition. This ensures the rule triggers only if three or more failed logins occur in that timeframe.

NEW QUESTION # 36
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 all FortiGate firewalls.
- B. Associated source IP addresses will be blocked on devices in the Aviation organization.
- C. Associated source IP addresses will be blocked on two FortiGate firewalls.
- D. Associated source IP addresses will be blocked on devices in the Network CMDB group.

Answer: C

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 # 37
.....

We can understand your apprehension before you buy it, but we want to told you that you don't worry about it anymore, because we have provided a free trial, you can download a free trial version of the FCP_FSM_AN-7.2 latest dumps from our website, there are many free services and training for you. In this way, you can consider that whether our FCP_FSM_AN-7.2 latest dumps are suitable for you. Before you decide to get the FCP_FSM_AN-7.2 Exam Certification, you may be attracted by many exam materials, but we believe not every material is suitable for you. Therefore, you can try to download the demo of FCP_FSM_AN-7.2 latest dumps that you can know if it is what you want. What's more, we provide it free of charge. How rare a chance is. If you want to pass FCP_FSM_AN-7.2 exam at first attempt, FCP_FSM_AN-7.2 exam dumps is your best choice.