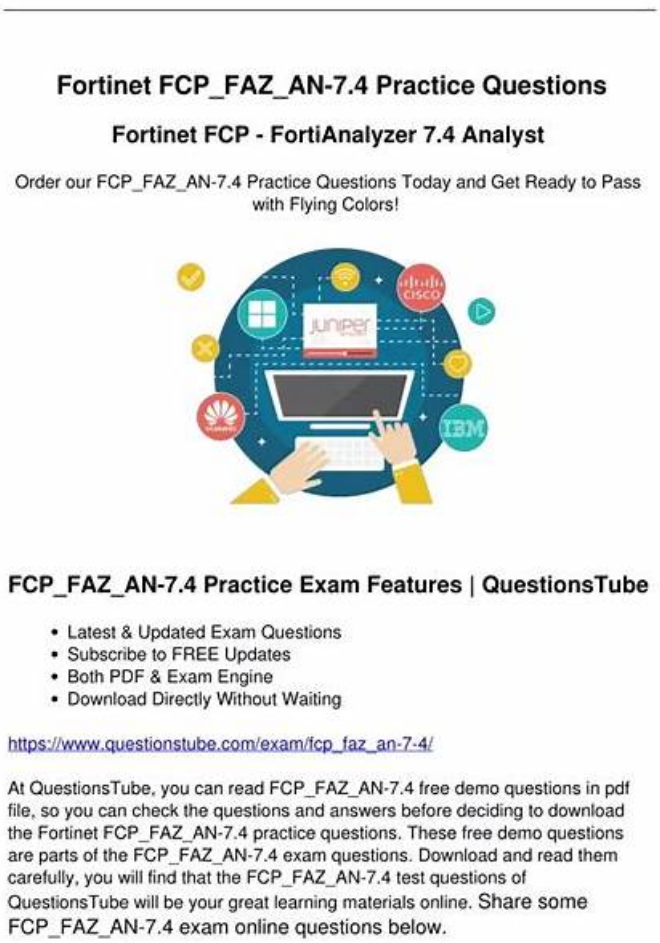
The Key to Success: Proper Planning and the Right Fortinet FCP_FSM_AN-7.2 Exam Questions



BONUS!!! Download part of TestPassKing FCP_FSM_AN-7.2 dumps for free: https://drive.google.com/open?id=1KMkAZ6ncb4cHzt409wbfb6aT8VNXd8BW

If you visit our website TestPassKing, then you will find that our Fortinet FCP_FSM_AN-7.2 practice questions are written in three different versions: PDF version, Soft version and APP version. All types of FCP_FSM_AN-7.2 Training Questions are priced favorably on your wishes. Obtaining our Fortinet FCP_FSM_AN-7.2 study guide in the palm of your hand, you can achieve a higher rate of success.

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.

Topic 2	• 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 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	• 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.

Valid Dumps FCP_FSM_AN-7.2 Files | Test FCP_FSM_AN-7.2 Sample Online

In the past ten years, our company has never stopped improving the FCP_FSM_AN-7.2 exam cram. For a long time, we have invested much money to perfect our products. At the same time, we have introduced the most advanced technology and researchers to perfect our FCP_FSM_AN-7.2 exam questions. At present, the overall strength of our company is much stronger than before. We are the leader in the market and master the most advanced technology. In fact, our FCP_FSM_AN-7.2 Test Guide has occupied large market shares because of our consistent renovating. We have built a powerful research center and owned a strong team. Up to now, we have got a lot of patents about the FCP_FSM_AN-7.2 test guide. In the future, we will continuously invest more money on researching.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q22-Q27):

NEW QUESTION # 22
Which two settings must you configure to allow FortiSIEM to apply tags to devices in FortiClient EMS? (Choose two.)

- A. FortiSIEM API credentials defined on FortiEMS\
- B. ZTNA tags defined on FortiSIEM
- C. FortiEMS API credentials defined on FortiSIEM
- D. Remediation script configured

Answer: A,C

Explanation:
To allow FortiSIEM to apply tags to devices in FortiClient EMS, FortiEMS API credentials must be defined on FortiSIEM to enable communication with EMS, and FortiSIEM API credentials must be defined on FortiEMS to allow EMS to accept tagging instructions from FortiSIEM. This bidirectional API trust is essential for tag application.

NEW QUESTION # 23
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 each time the rule triggers, and updates the First Seen and Last Seen timestamps.
- D. FortiSIEM generates a new incident based on the Rule Frequency value, and updates the First Seen and Last Seen timestamps.

Answer: B

Explanation:
When a performance rule triggers repeatedly, FortiSIEM updates the existing incident by incrementing the Incident Count and refreshing the Last Seen timestamp. This avoids flooding the incident table with duplicates while still tracking repeated occurrences.

NEW QUESTION # 24
What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?

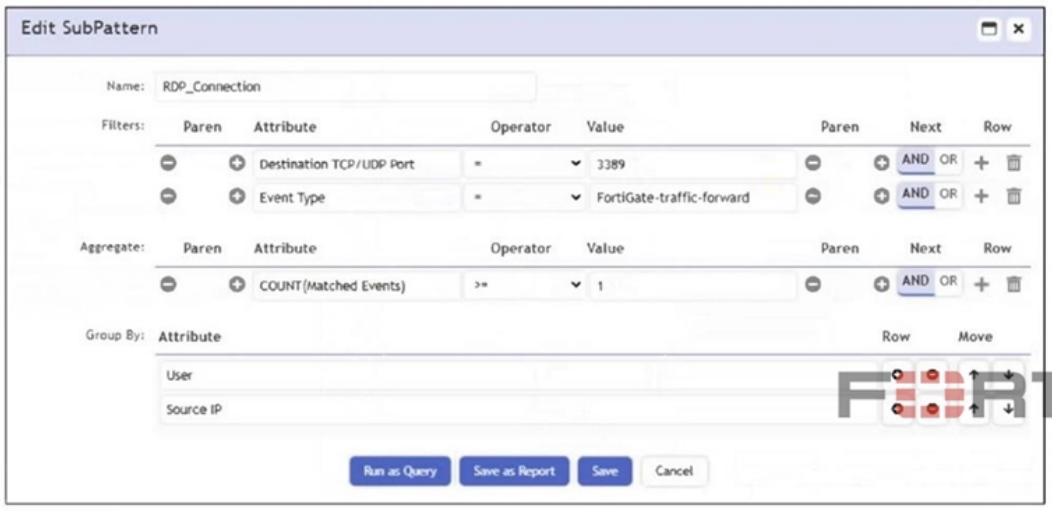
- A. SNMP
- B. SSH
- C. FortiSIEM worker
- D. FortiSIEM agent

Answer: D

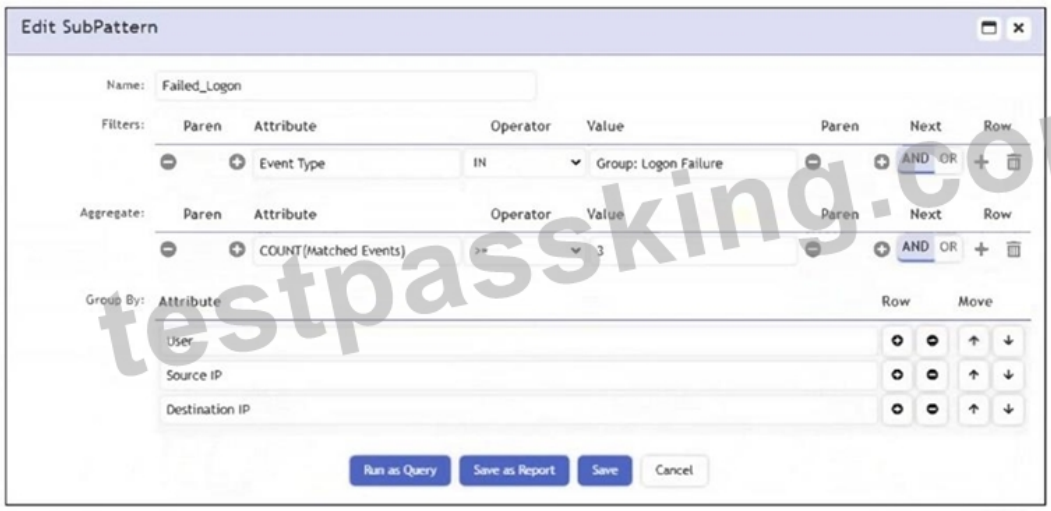
Explanation:
The FortiSIEM agent can be used to send detailed endpoint data such as user activity and process behavior to FortiSIEM, which is essential for performing User and Entity Behavior Analytics (UEBA).

NEW QUESTION # 25
Refer to the exhibit.

Subpattern 1



Subpattern 2



Rule Conditions

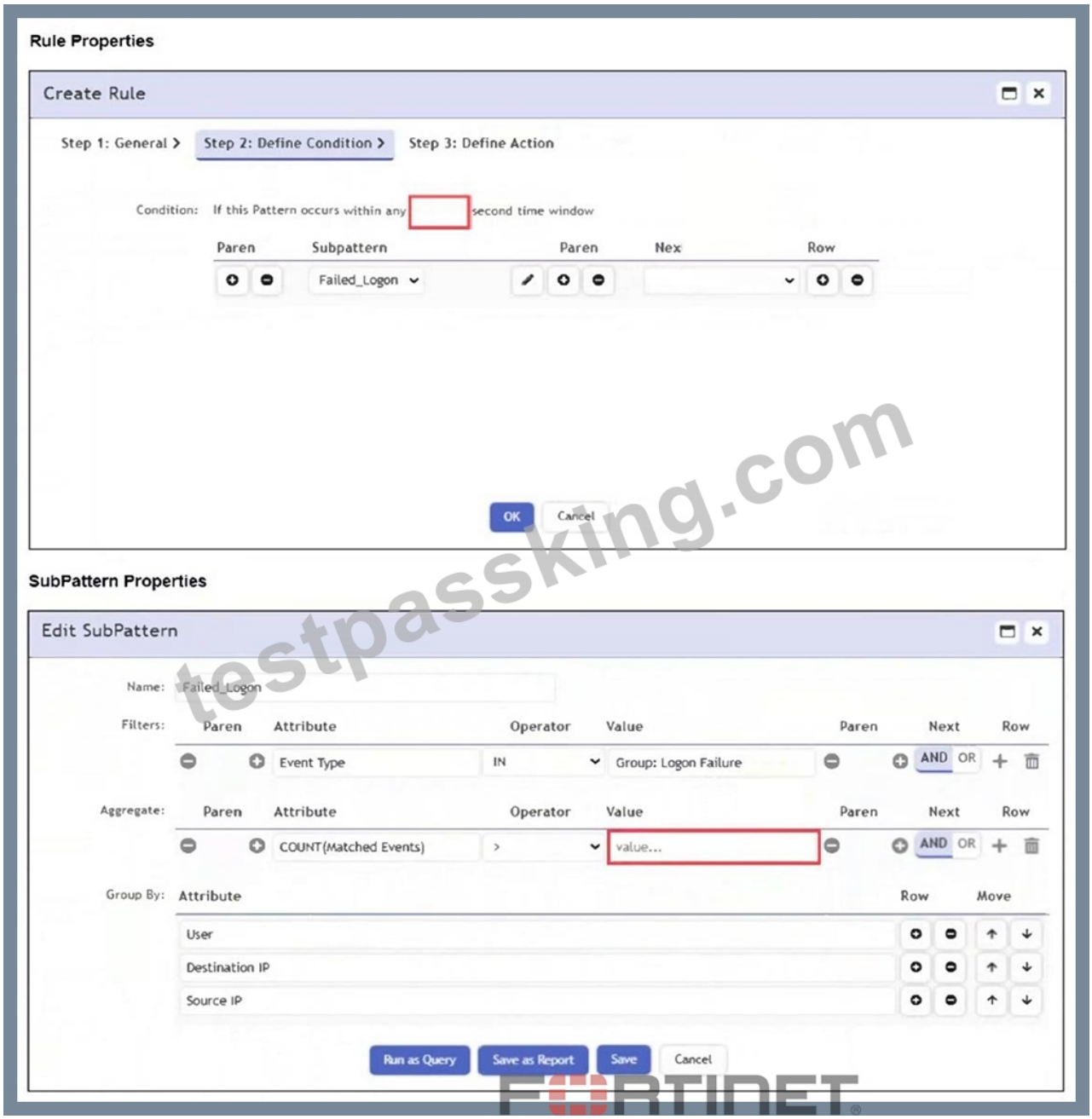
Which two conditions will match this rule and subpatterns? (Choose two.)

- A. A user fails twice to log in when connecting through RDP.
- B. A user runs a brute force password cracker against an RDP server.
- C. A user connects to the wrong IP address for an RDP session five times.
- D. A user using RDP over SSL VPN fails to log in to an application five times.

Answer: B,D

Explanation:
The user initiates an RDP session (Subpattern 1) and then fails to log in multiple times (Subpattern 2 with COUNT(Matched Events) >= 3) - both from the same Source IP and User within 300 seconds.
The brute force attempts typically involve a successful RDP connection followed by multiple failed logins, satisfying the sequence and grouping conditions in the rule.

NEW QUESTION # 26
Refer to the exhibit.



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

NEW QUESTION # 27

......

You can take the Fortinet FCP_FSM_AN-7.2 desktop practice exam on Windows computers. TestPassKing has come up with this new style format in which you can easily track the records of your previous progress. So, you will understand how much you have improved or how much you need improvement for passing exam. The FCP - FortiSIEM 7.2 Analyst (FCP_FSM_AN-7.2) practice exam will also boost your time management skills.