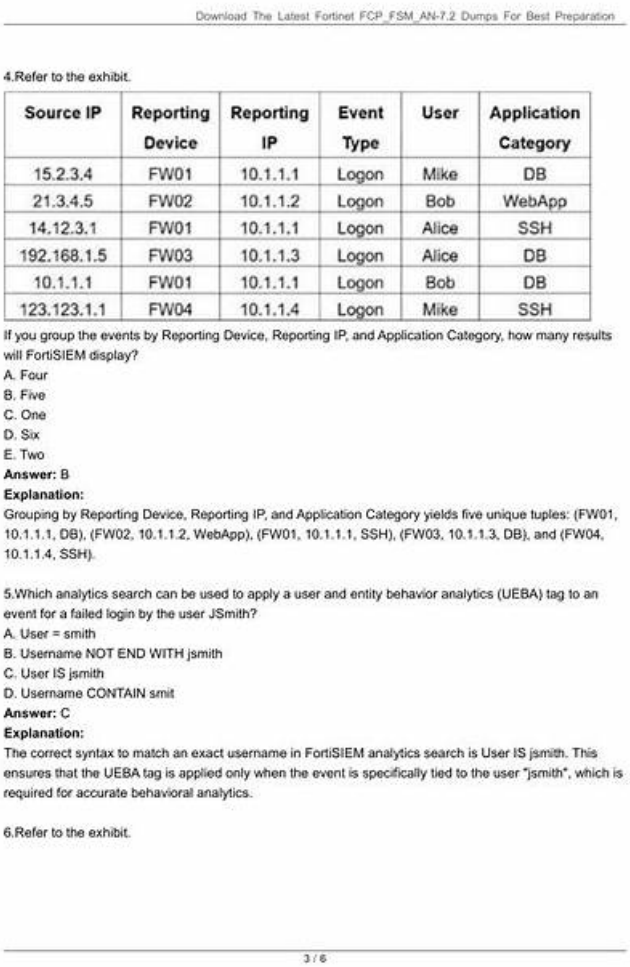
Free PDF 2026 FCP_FSM_AN-7.2: FCP - FortiSIEM 7.2 Analyst–Valid Reliable Dumps Ppt



4.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. Five
C. One
D. Six
E. Two
Answer: B
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).

5.Which analytics search can be used to apply a user and entity behavior analytics (UEBA) tag to an event for a failed login by the user JSmith?
A. User = smith
B. Username NOT END WITH jsmith
C. User IS jsmith
D. Username CONTAIN smit
Answer: C
Explanation:
The correct syntax to match an exact username in FortiSIEM analytics search is User IS jsmith. This ensures that the UEBA tag is applied only when the event is specifically tied to the user "jsmith", which is required for accurate behavioral analytics.

6.Refer to the exhibit.

2026 Latest PassSureExam FCP_FSM_AN-7.2 PDF Dumps and FCP_FSM_AN-7.2 Exam Engine Free Share: https://drive.google.com/open?id=13YwPJon_En5CJTNI6JyFUdLQQUk-zs4P

Our company pays high attentions to the innovation of our FCP_FSM_AN-7.2 study dump. We constantly increase the investment on the innovation and build an incentive system for the members of the research expert team. Our experts group specializes in the research and innovation of our FCP_FSM_AN-7.2 exam practice guide and supplements the latest innovation and research results into the FCP_FSM_AN-7.2 Quiz prep timely. Our experts group collects the latest academic and scientific research results and traces the newest industry progress in the update of the FCP_FSM_AN-7.2 study materials.

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.

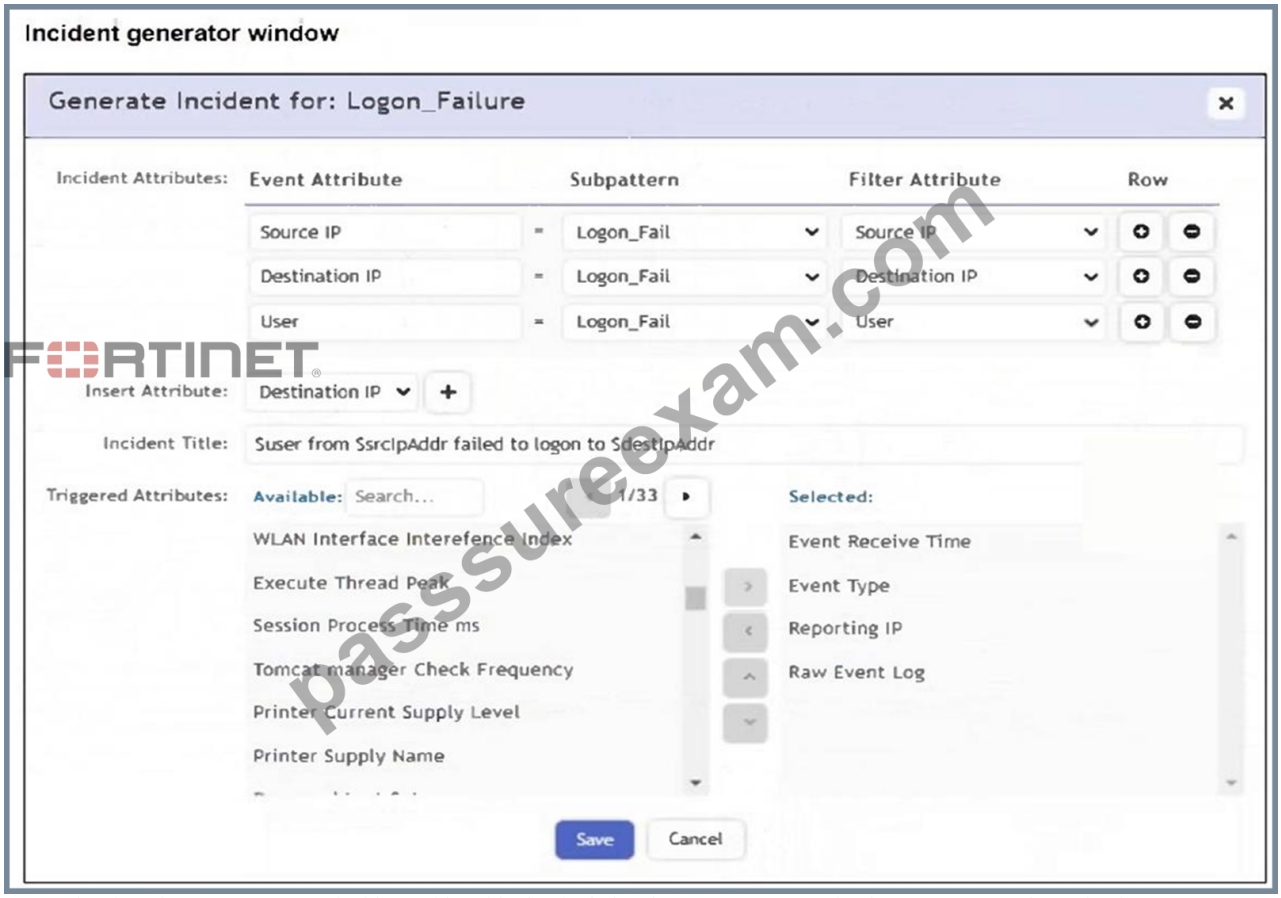
Topic 2	• Incidents, notifications, and remediation: This section of the exam measures the skills of Incident Responders and encompasses the entire incident management lifecycle. This includes the skills required to manage and prioritize security incidents, configure policies for alert notifications, 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	• 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.

Complete coverage FCP_FSM_AN-7.2 Online Learning Environment

All contents of FCP_FSM_AN-7.2 training prep are made by elites in this area rather than being fudged by laymen. Let along the reasonable prices of our FCP_FSM_AN-7.2 exam materials which attracted tens of thousands of exam candidates mesmerized by their efficiency by proficient helpers of our company. Any difficult posers will be solved by our FCP_FSM_AN-7.2 Quiz guide. And we have free demos of our FCP_FSM_AN-7.2 study braindumps for you to try before purchase.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q17-Q22):

NEW QUESTION # 17
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 Host Name must be selected as a Triggered Attribute.
- D. The Destination IP Event Attribute must be removed.

Answer: C

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 # 18
What are two required components of a rule? (Choose two.)

- A. Subpattern
- B. Clear policy
- C. Detection Technology
- D. Exception policy

Answer: A,C

Explanation:
A Subpattern defines the specific conditions or event patterns the rule is designed to detect, and the Detection Technology specifies the type of detection logic (e.g., real-time, historical). Both are essential for a rule to function in FortiSIEM.

NEW QUESTION # 19
How does FortiSIEM update the incident table if a performance rule triggers repeatedly?

- A. FortiSIEM generates a new incident each time the rule triggers, and updates the First Seen and Last Seen timestamps.
- B. FortiSIEM updates the Incident Count value and Last Seen timestamp.
- C. FortiSIEM generates a new incident based on the Rule Frequency value, and updates the First Seen and Last Seen timestamps.
- D. FortiSIEM changes the incident status to Repeated, and updates the Last Seen timestamp.

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 # 20
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

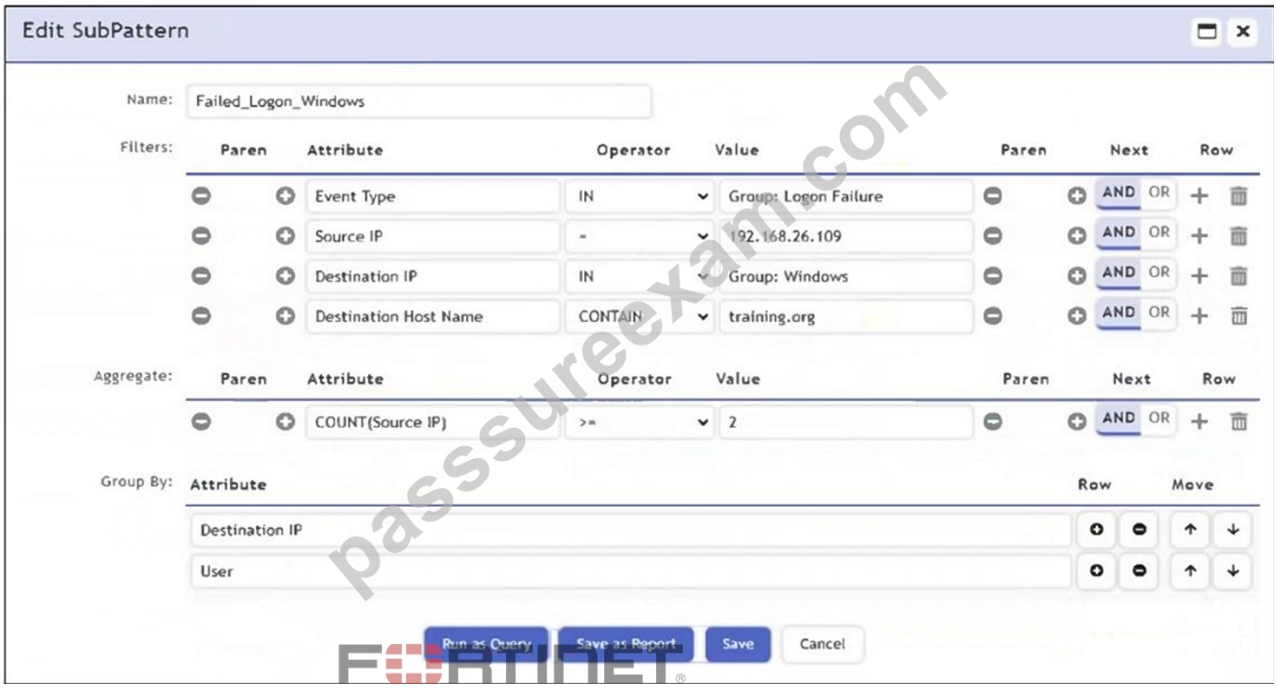
If you group the events by User and Count attributes, how many results will FortiSIEM display?

- A. One
- B. Three
- C. Five
- D. Six
- E. Two

Answer: C

Explanation:
Grouping by User and Count yields five unique pairs: (Mike,4), (Bob,3), (Alice,2), (Bob,6), (Mike,5).

NEW QUESTION # 21
Refer to the exhibit.
SubPattern edit window



An analyst is troubleshooting the rule shown in the exhibit. It is not generating any incidents, but the filter parameters are generating events on the Analytics tab.
What is wrong with the rule conditions?

- A. The Aggregate attribute is too restrictive.
- B. The Group By attributes restricts which events are counted.
- C. The Destination Host Name value is not fully qualified.
- D. The Event Type refers to a CMDB lookup and should be an Event lookup.

Answer: B

Explanation:
The Group By attributes - Destination IP and User - cause the aggregation (COUNT(Source IP) >= 2) to apply within each unique combination of those groupings. This restricts the count calculation and can prevent the rule from triggering incidents, even if matching events exist in the Analytics tab.

NEW QUESTION # 22
.....

It is known to us that time is money, and all people hope that they can spend less time on the pass. We are happy to tell you that The FCP_FSM_AN-7.2 study materials from our company will help you save time. With meticulous care design, our study materials will help all customers pass their exam in a shortest time. If you buy the FCP_FSM_AN-7.2 Study Materials from our company, you just need to spend less than 30 hours on preparing for your exam, and then you can start to take the exam.

P.S. Free 2026 Fortinet FCP_FSM_AN-7.2 dumps are available on Google Drive shared by PassSureExam: https://drive.google.com/open?id=13YwPJon_En5CJTNI6JyFUdLQQUk-zs4P