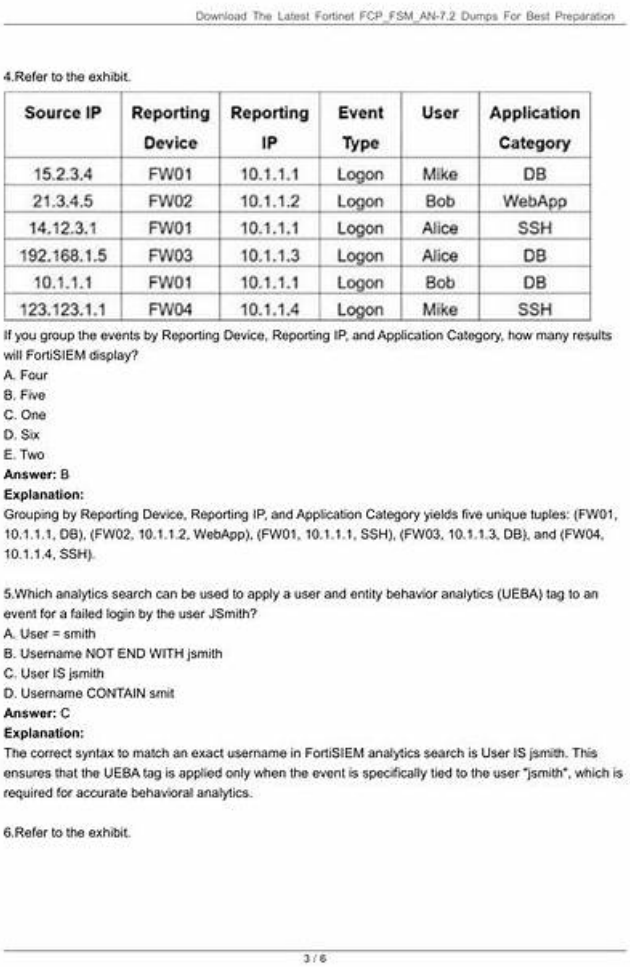
New FCP_FSM_AN-7.2 Dumps Ppt & Reliable FCP_FSM_AN-7.2 Exam Online



Download The Latest Fortinet FCP_FSM_AN-7.2 Dumps For Best Preparation

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.

3 / 6

P.S. Free 2026 Fortinet FCP_FSM_AN-7.2 dumps are available on Google Drive shared by Pass4SureQuiz: https://drive.google.com/open?id=1GVIR_9-JyQEkPvd3o_naw4UBF-qU36E0

In order to meet the demands of all the customers, we can promise that we will provide all customers with three different versions of the FCP_FSM_AN-7.2 study materials. In addition, we can make sure that we are going to offer high quality practice study materials with reasonable prices but various benefits for all customers. It is our sincere hope to help you Pass FCP_FSM_AN-7.2 Exam by the help of our FCP_FSM_AN-7.2 study materials.

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	• 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 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.

Reliable FCP_FSM_AN-7.2 Exam Online | Reliable FCP_FSM_AN-7.2 Test Cram

More and more people look forward to getting the FCP_FSM_AN-7.2 certification by taking an exam. However, the exam is very difficult for a lot of people. Especially if you do not choose the correct study materials and find a suitable way, it will be more difficult for you to pass the exam and get the Fortinet related certification. If you want to get the related certification in an efficient method, please choose the FCP_FSM_AN-7.2 learning dumps from our company. We can guarantee that the study materials from our company will help you pass the exam and get the certification in a relaxed and efficient method.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q21-Q26):

NEW QUESTION # 21
Which items are used to define a subpattern?

- A. Filters, Aggregate, Time Window definitions
- B. Filters, Group By, Threshold definitions
- C. Filters, Aggregate, Group By definitions
- D. Filters, Threshold, Time Window definitions

Answer: C

Explanation:
A subpattern in FortiSIEM is defined using Filters to match specific events, Aggregate conditions to apply statistical thresholds (e.g., COUNT), and Group By attributes to segment data for evaluation. These three components collectively determine how the subpattern functions.

NEW QUESTION # 22
How can you query the configuration management database (CMDB) in an analytics search?

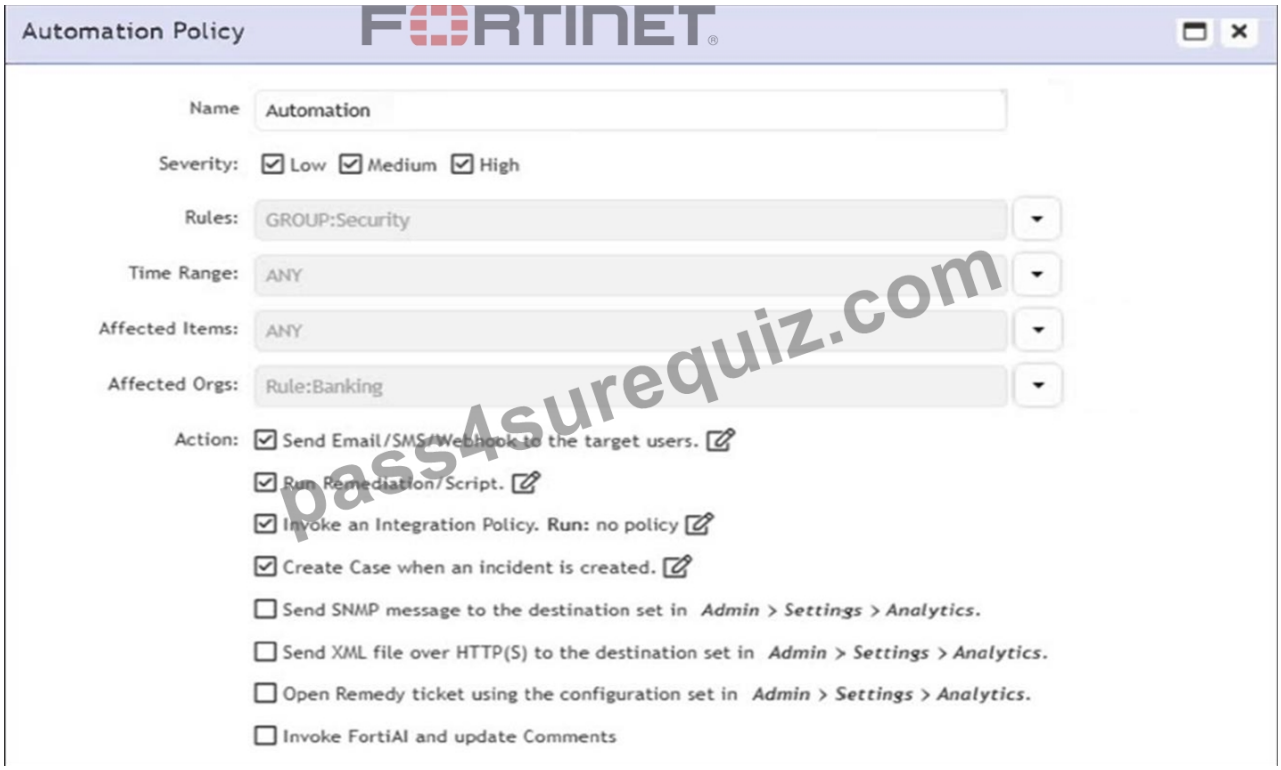
- A. On the Admin tab, click CMDB Search.
- B. Click Value > Select from CMDB.
- C. Click Attribute > Select from CMDB.
- D. On the CMDB tab, select an entry, and then click Create Search.

Answer: B

Explanation:
In an analytics search, you can query the CMDB by clicking Value > Select from CMDB, which allows you to choose values

directly from CMDB entries for the selected attribute, enabling precise filtering based on asset data.

NEW QUESTION # 23
Refer to the exhibit.



According to the automation policy configuration shown in the exhibit, what happens if an associated rule triggers?

- A. FortiSIEM fails to the integration policy, because no policy is defined.
- B. FortiSIEM runs the remediation script, because that takes precedence over all other options.
- C. FortiSIEM sends an email, because that is first on the list.
- D. FortiSIEM performs all selected actions.

Answer: D

Explanation:
When an associated rule triggers, FortiSIEM performs all selected actions in the automation policy. In this case, it will send an email/SMS/webhook, run the remediation script, invoke the integration policy (even if none is currently defined), and create a case. All checked actions are executed.

NEW QUESTION # 24
What are two required components of a rule? (Choose two.)

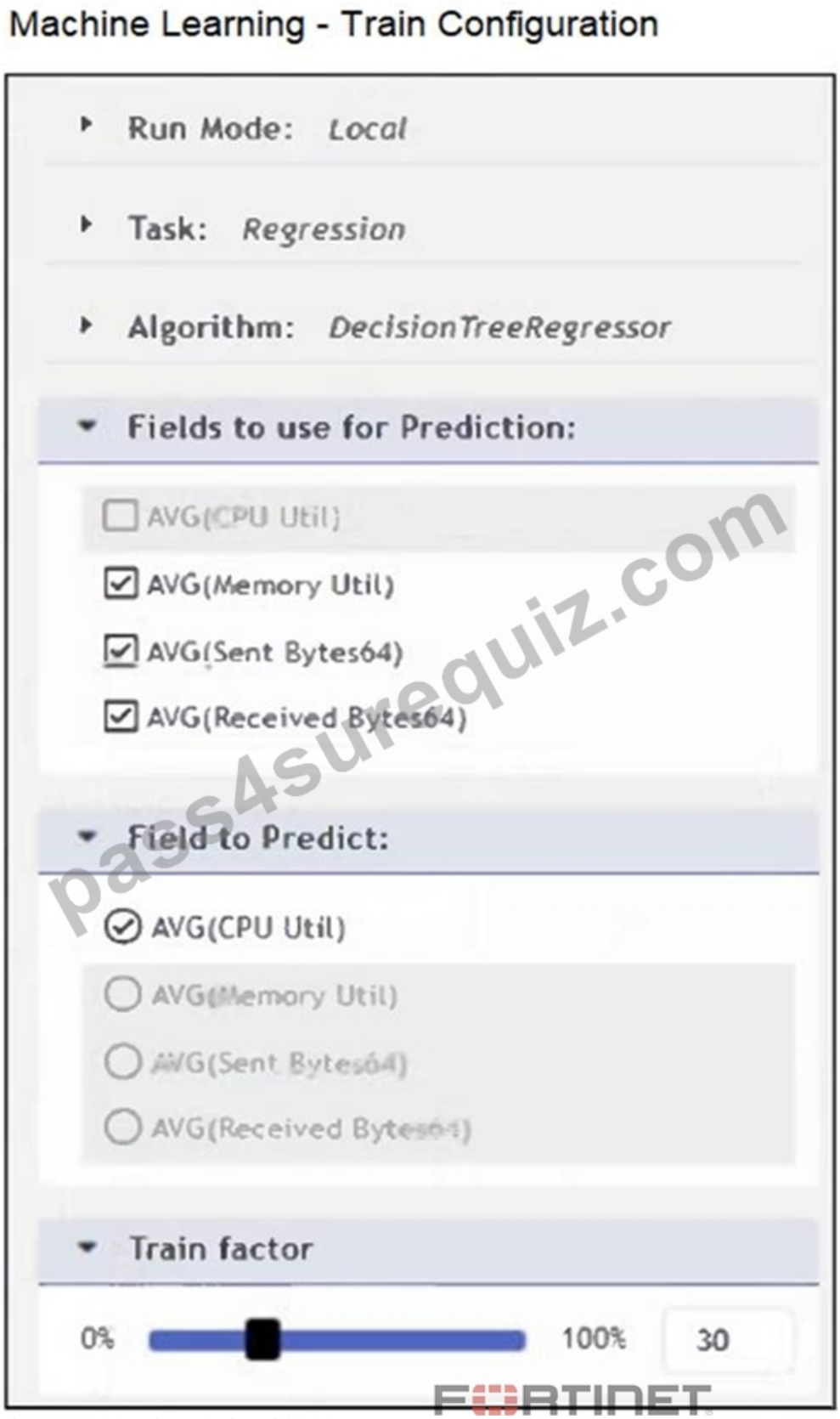
- A. Detection Technology
- B. Clear policy
- C. Subpattern
- D. Exception policy

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 # 25

Refer to the exhibit.



The configuration shown in the exhibit is incorrect.
What must you change to allow this configuration to be successfully applied to FortiSIEM?

- A. Only one AVG type field must be selected under Fields to use for Prediction.
- B. The Train factor must be 70% or greater.
- C. The selection in Fields to use for Prediction and Field to Predict must match.
- D. Run Mode must be set to ML.

Answer: D

Explanation:
The Run Mode is set to Local, which is not valid for training machine learning models in FortiSIEM. To apply this configuration correctly, the Run Mode must be set to ML, which enables proper model training and prediction using selected fields.

NEW QUESTION # 26
.....

Having a FCP_FSM_AN-7.2 certificate is a task that every newcomer rookie dreams about. With it, you can not only become the elite in the workplace in the eyes of leaders, but also get a quick promotion and a raise, and maybe you have the opportunity to move to a better business. Whether you are a student or an office worker, you can be satisfied here, and you will never regret if you choose FCP_FSM_AN-7.2 Exam Torrent. For we have successfully help tens of thousands of candidates achieve their aims. We believe you won't be the exception to pass the FCP_FSM_AN-7.2 exam and get the dreaming FCP_FSM_AN-7.2 certification.