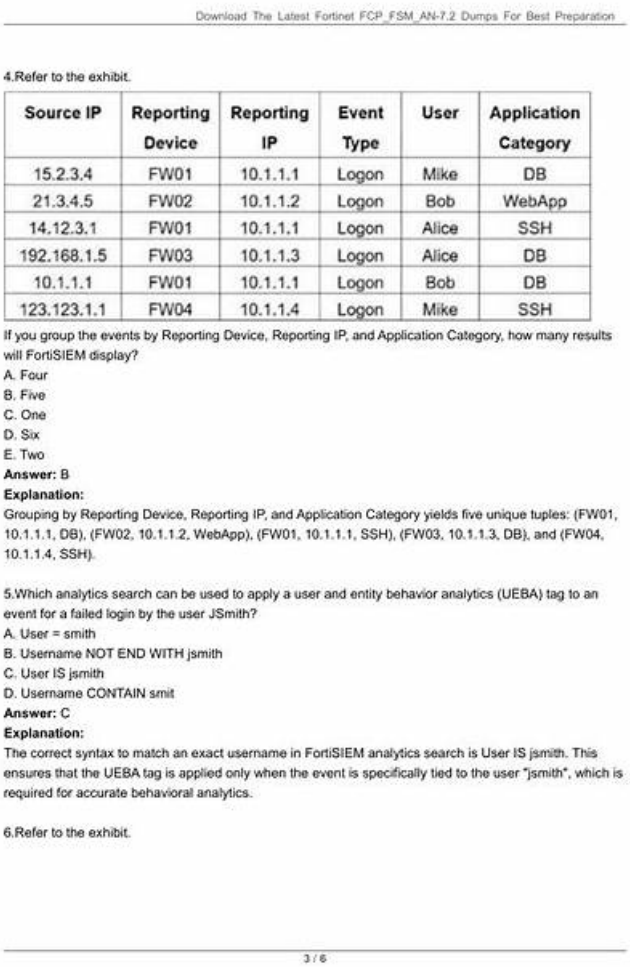
Cost Effective FCP_FSM_AN-7.2 Dumps & Certification FCP_FSM_AN-7.2 Exam Infor


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 TorrentValid: https://drive.google.com/open?id=1kXHpcpy73Bqua8Q2ztPqoA0hhdtPfOsg

It is known to us that getting the FCP_FSM_AN-7.2 certification is not easy for a lot of people, but we are glad to tell you good news. The study materials from our company can help you get the FCP_FSM_AN-7.2 certification in a short time. Now we are willing to introduce our FCP_FSM_AN-7.2 practice questions to you in detail, we hope that you can spare your valuable time to have a look to our FCP_FSM_AN-7.2 Exam questoins. Please believe that we will not let you down. You can just free download the demo of our FCP_FSM_AN-7.2 training guide on the web to know the excellent quality.

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	• 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	• 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.

Certification FCP_FSM_AN-7.2 Exam Infor, Key FCP_FSM_AN-7.2 Concepts

As is known to us, getting the newest information is very important for all people to pass the exam and get the certification in the shortest time. In order to help all customers gain the newest information about the FCP_FSM_AN-7.2 exam, the experts and professors from our company designed the best FCP_FSM_AN-7.2 test guide. The experts will update the system every day. If there is new information about the exam, you will receive an email about the newest information about the FCP_FSM_AN-7.2 Learning Materials. We can promise that you will never miss the important information about the FCP_FSM_AN-7.2 exam.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q29-Q34):

NEW QUESTION # 29
Refer to the exhibit.

The analyst is troubleshooting the analytics query shown in the exhibit.
Why is this search not producing any results?

- A. The Time Range is set incorrectly.
- B. The Boolean operator is wrong between the attributes.
- C. The inner and outer nested query attribute types do not match.
- D. You cannot reference User and Event Type attributes in the same search.

Answer: C

Explanation:
The issue is that the "User" attribute is incorrectly assigned a Device IP group value, which is a mismatch of attribute types. "User" expects a user name or identity, not a device IP group. This mismatch between the attribute type and the provided value causes the search to return no results.

NEW QUESTION # 30
What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?

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

Answer: A

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 # 31
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. Two
- B. One
- C. Five
- D. Three
- E. Six

Answer: C

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

NEW QUESTION # 32
When configuring anomaly detection machine learning, in which step must you select the fields to analyze?

- A. Prepare Data
- B. Train
- C. Design
- D. Schedule

Answer: A

Explanation:

In the Prepare Data step of configuring anomaly detection in FortiSIEM, you must select the fields to analyze. This step defines the input features that the machine learning model will evaluate during training and detection.

NEW QUESTION # 33
Which items are used to define a subpattern?

- A. Filters, Threshold, Time Window definitions
- B. Filters, Aggregate, Time Window definitions
- C. Filters, Aggregate, Group By definitions
- D. Filters, Group By, Threshold 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 # 34
.....

You will have good command knowledge with the help of our FCP_FSM_AN-7.2 study materials. The certificate is of great value in the job market. Our FCP_FSM_AN-7.2 learning prep can exactly match your requirements and help you pass FCP_FSM_AN-7.2 exams and obtain certificates. As you can see, our products are very popular in the market. Time and tides wait for no people. Take your satisfied FCP_FSM_AN-7.2 Actual Test guide and start your new learning journey. After learning our FCP_FSM_AN-7.2 learning materials, you will benefit a lot. Being brave to try new things, you will gain meaningful knowledge.

Simply search for ✔ FCP_FSM_AN-7.2 □✔□ for free download on ▸ www.exam4labs.com ◂ □FCP_FSM_AN-7.2 Testdump

- study.stcs.edu.np, 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, 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.stes.tyc.edu.tw, alkalamacademy.com, behindvlsi.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, tinnitusheal.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, Disposable vapes

BTW, DOWNLOAD part of TorrentValid FCP_FSM_AN-7.2 dumps from Cloud Storage: https://drive.google.com/open?id=1kXHpcpy73Bqua8Q2ztPqoA0hhdtPfOsg