Valid FCP_FSM_AN-7.2 Exam Syllabus | FCP_FSM_AN-7.2 Braindump Free

BTW, DOWNLOAD part of Exam4PDF FCP_FSM_AN-7.2 dumps from Cloud Storage: https://drive.google.com/open?id=1X6YkiJaBXV7N7dJZ9CD8gW_Qwr4bJsZF

In fact, sticking to a resolution will boost your sense of self-esteem and self-control. So our FCP_FSM_AN-7.2 exam materials can become your new aim. Our FCP_FSM_AN-7.2 study materials could make a difference to your employment prospects. Getting rewards need to create your own value to your company. However, your capacity for work directly proves your value. As long as you get your FCP_FSM_AN-7.2 Certification with our FCP_FSM_AN-7.2 practice braindumps, you will have a better career for sure.

Fortinet FCP_FSM_AN-7.2 Exam Overview:

Certification Vendor:	Fortinet
Exam Name:	FCP - FortiSIEM 7.2 Analyst
Exam Number:	FCP_FSM_AN-7.2
Passing Score:	60%
Exam Duration:	120 minutes
Available Languages:	English
Certificate Validity Period:	2 years
Exam Price:	USD 400
Real Exam Qty:	35
Related Certifications:	FCP - FortiSIEM
Exam Format:	Multiple Select, Multiple Choice
Sample Questions:	Fortinet FCP_FSM_AN-7.2 Sample Questions
Exam Way:	Online proctored or at Pearson VUE testing center
Pre Condition:	Recommended: FortiSAE, FortiSIEM training courses or equivalent practical experience
Official Syllabus URL:	https://www.fortinet.com/training/certification

>> Valid FCP_FSM_AN-7.2 Exam Syllabus <<

FCP_FSM_AN-7.2 Braindump Free - FCP_FSM_AN-7.2 New Learning Materials

The contents of FCP_FSM_AN-7.2 exam torrent was all compiled by experts through the refined off textbooks. Hundreds of experts simplified the contents of the textbooks, making the lengthy and complex contents easier and more understandable. With FCP_FSM_AN-7.2 study tool, you only need 20-30 hours of study before the exam. FCP_FSM_AN-7.2 guide torrent provides you with a brand-new learning method. In the course of doing questions, you can memorize knowledge points. You no longer need to look at the complicated expressions in the textbook. Especially for those students who are headaches when reading a book, FCP_FSM_AN-7.2 Study Tool is their gospel. Because doing exercises will make it easier for one person to concentrate, and at the same time, in the process of conducting a mock examination to test yourself, seeing the improvement of yourself will makes you feel very fulfilled and have a stronger interest in learning. FCP_FSM_AN-7.2 guide torrent makes your learning process not boring at all.

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.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q36-Q41):

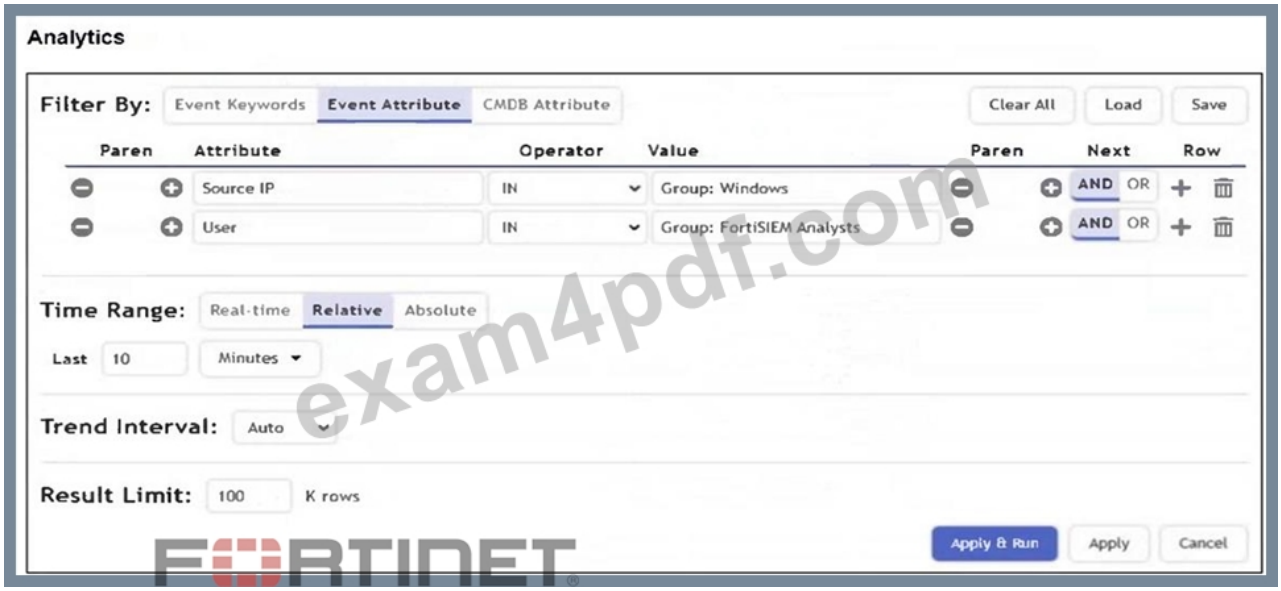
NEW QUESTION # 36
What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?

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

Answer: C

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 # 37
Refer to the exhibit.



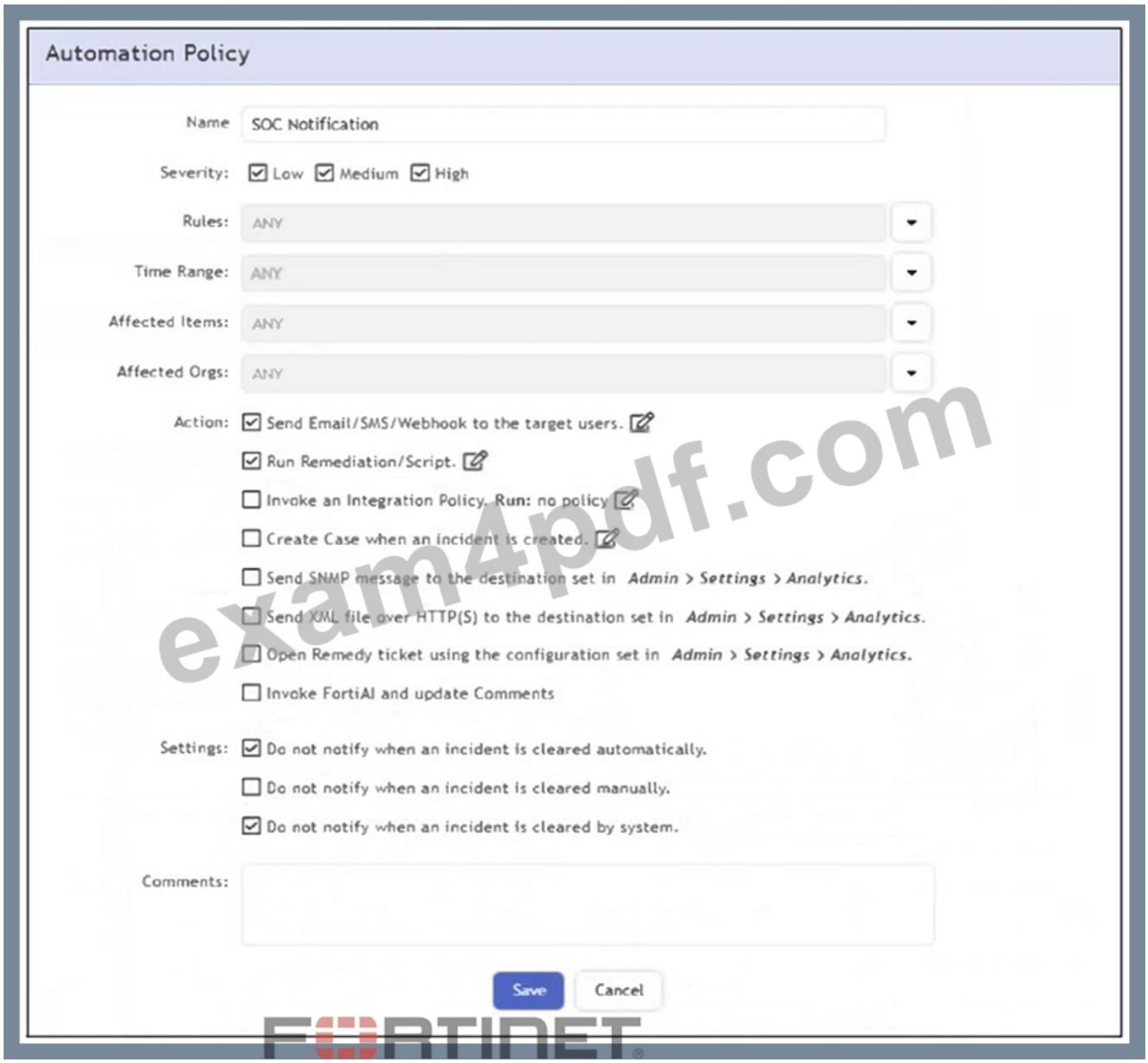
What is the Group: FortiSIEM Analysts value referring to?

- A. Windows Active Directory user group
- B. CMDB user group
- C. FortiSIEM organization group
- D. LDAP user group

Answer: B

Explanation:
In FortiSIEM, the value Group: FortiSIEM Analysts under the User attribute refers to a CMDB user group. These groups are defined within FortiSIEM's CMDB and used to logically organize users for analytics, correlation rules, and reporting.

NEW QUESTION # 38
Refer to the exhibit.



What happens when an analyst clears an incident generated by a rule containing the automation policy shown in the exhibit?

- A. No notification is sent.
- B. A notification is sent to the SOC manager dashboard.
- C. The remediation script is run.
- D. An email is sent to the SOC manager.

Answer: A

Explanation:
The automation policy has the option "Do not notify when an incident is cleared manually" enabled. Therefore, when an analyst manually clears an incident, no notification or automation action is triggered.

NEW QUESTION # 39
An analyst wants to create a rule from a newly created analytics search. What is the quickest method?

- A. On the Analytics tab, click the New button next to the Filter By box.
- B. Create a new rule under Resources > Rules and fill in the search details.
- C. On the upper menu bar on any tab, click the pencil icon.
- D. On the Analytics tab, click Actions > Create Rule.

Answer: D

Explanation:

The quickest way to create a rule from an existing analytics search in FortiSIEM is to go to the Analytics tab and select Actions > Create Rule. This automatically converts the current search filters and parameters into a correlation rule template, saving time compared to manually re- entering all the search criteria.

NEW QUESTION # 40
How can you query the configuration management database (CMDB) in an analytics search?

- A. Click Attribute > Select from CMDB.
- B. Click Value > Select from CMDB.
- C. On the Admin tab, click CMDB Search.
- 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 # 41
.....

P.S. Free 2026 Fortinet FCP_FSM_AN-7.2 dumps are available on Google Drive shared by Exam4PDF: https://drive.google.com/open?id=1X6YkiJaBXV7N7dJZ9CD8gW_Qwr4bJsZF