ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Fortinet

Code: FCP_FSM_AN-7.2

Exam: FCP - FortiSIEM 7.2 Analyst

https://www.examsnest.com/exam/fcp_fsm_an-72/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Question: 1

Which statement about thresholds is true?

A. FortiSIEM uses fixed, hardcoded global and device thresholds for all performance metrics.
B. FortiSIEM uses only device thresholds for security metrics.
C. FortiSIEM uses global and per device thresholds for performance metrics.
D. FortiSIEM uses only global thresholds for performance metrics.

Answer: C

Explanation:
FortiSIEM evaluates performance metrics against both global thresholds, which apply system-wide, and per-device thresholds, which can be customized for individual devices. This dual approach allows flexibility in monitoring while ensuring consistent baseline alerting.

Question: 2

Which running mode takes the most time to perform machine learning tasks?

A. Local auto
B. Local
C. Forecasting
D. Regression

Answer: B

Explanation:
In Local mode, FortiSIEM performs machine learning tasks using the full dataset without optimization shortcuts, making it the most time-consuming mode compared to Local Auto, Forecasting, or Regression.

Question: 3

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

Answer: B

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.

Question: 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).

Question: 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.

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Fortinet

Code: FCP_FSM_AN-7.2

Exam: FCP - FortiSIEM 7.2 Analyst

https://www.examsnest.com/exam/fcp_fsm_an-72/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation