HP0-A116 Q&As

HP ArcSight ESM 6.5 Security Administrator and Analyst

Pass HP HP0-A116 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/hp0-a116.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

What is an example of an event-based Data Monitor?

A. rules partial match

B. last n events

C. session reconciliation

D. moving average

Correct Answer: B

QUESTION 2

Which statement best describes how baselines are established and used in Query Viewers?

A. Baselines are created using query results, which are fed into the Image Editor for filtering and display in the related Data Monitor.

B. Baselines are created using rules. After the rule is triggered, the resulting action establishes a baseline against which future rules are evaluated in the Query Viewer.

C. Baselines are created using query results. When a query has one or more baselines available, you can compare the current results with a baseline.

D. Baselines are created using query results. The baseline from the query is used to create a new field set definition that can be run against future events.

Correct Answer: B

QUESTION 3

In ESM, what allows contextual information to be added to an individual event or group of events in support of workflow or operational metrics?

A. Knowledge Base

B. Templates

C. Annotations

D. Rules

Correct Answer: C

QUESTION 4

Which are operators in the ArcSight Common Conditions Editor (CCE)? (Select two.)

A. ELSE

B. AND

C. OR

D. IF

Correct Answer: BC

QUESTION 5

Which type of event is displayed in an Active Channel with the following Inline Filter applied?

Category Behavior = /Authentication/Verify

Category Outcome = /Failure

A. Logout events

B. Login Success events

C. Login Failure events

D. Account Locked events

Correct Answer: C