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.geekcert.com/hp0-a116.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which statement is true about how filters are applied by the Connector or by the Manager?

A. When filters are applied by either the Connector or the Manager, events that match the filter conditions are selected and forwarded for further processing.

B. When filters are applied by either the Connector or the Manager, events that match the filter conditions are excluded and are not forwarded for further processing.

C. Events that match the Connector filter are excluded and not forwarded further; events that match the Manager filter are selected for further analysis.

D. Events that match the Connector filter are included and forwarded to the Manager; events that match the Manager filter are excluded.

Correct Answer: C

QUESTION 2

What is stored in a database partition?

A. as much data as it can hold

B. a user-configurable number of events

C. events from a one week time period

D. events from a 24-hour time period

Correct Answer: D

QUESTION 3

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 4

When is it useful to schedule rules rather than have them run in real time?

A. when a network device is down

B. when events are occurring less frequently than usual

C. when you anticipate a worm or virus attack

D. when you need to minimize impact on system performance

Correct Answer: C

QUESTION 5

Which statements are true about event lifecycle data collection and the event processing phase? (Select two.)

A. Model confidence is determined, based on details provided by the event source.

B. Each line of incoming log data is processed as a separate event.

C. Event severity is determined, based on an Active List of recent severity factors.

D. Values are normalized and entered into the ArcSight Event Schema.

Correct Answer: BD