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 processes occur in the first phase of the event lifecycle? (Select two.)

A. evaluating event data

B. applying event categories

C. applying hashing to event data

D. correlating event data

E. normalizing event data

Correct Answer: BE

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

During Connector install, which statement is true about the ArcSight Manager\\'s host name or IP address?

A. It must match the host name or IP address in the ArcSight Manager\\'s SSL certificate.

B. The host name or IP address is used as an encryption key.

C. It can be any legitimate host name or IP address.

D. It must contain a combination of alpha-numeric characters.

Correct Answer: A

QUESTION 4

What is the "focus" of a Focus report?

A. the differences between two similar reports

B. a subset of a larger (e.g., monthly or quarterly) report

C. events that have been missed

D. high priority Correlation events only

Correct Answer: B

QUESTION 5

Which statement is true about SmartConnectors and FlexConnectors?

A. FlexConnectors allow creation of SmartConnectors that are tailored to individualized custom situations and specific security event data.

B. FlexConnectors are plug-and-play, self-programming SmartConnectors.

C. SmartConnectors do not include tools for customizing FlexConnectors.

D. SmartConnectors are vendor-specific and must be purchased through the individual device vendors.

Correct Answer: A

Latest HP0-A116 Dumps   HP0-A116 VCE Dumps   HP0-A116 Exam Questions