HP0-A100^{Q&As}

HP ArcSight Security Solutions

Pass HP HP0-A100 Exam with 100% Guarantee

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

https://www.pass2lead.com/hp0-a100.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 correct?

A. ArcSight Logger event schema is different from the ESM event schema

B. ArcSight Logger receives events from Connectors rather than from raw events

C. ArcSight Logger cannot compress data.

D. ArcSight Logger must be used together with an ArcSight ESM

Correct Answer: B

QUESTION 2

Which statement describes a CIP?

A. A collection of packages to interface ArcSight products with ticket management systems

B. A suite of ArcSight resources focusing on system performance issues

C. A product that scales easily to manage extreme machine data across IT

D. A collection of ArcSight resources to monitor IT assets, based on regulatory requirements

Correct Answer: D

QUESTION 3

What is the output of the Data Collection and Event Processing phase?

A. Correlation events

B. Base events

C. Filtered events

D. Raw events

Correct Answer: A

QUESTION 4

What is the major benefit of ArcSight Logger?

A. Correlation of raw events

B. Long-term storage of events

C. Storage of connectors

D. Real-time threat detection

Correct Answer: D

QUESTION 5

Which database management system technology is utilized by the Arc Sight ESM 6.5c?

A. DB2

B. CORR-Engine

C. SQL Server Express Edition

D. Oracle 10g

Correct Answer: B

HP0-A100 Study Guide   HP0-A100 Exam Questions   HP0-A100 Braindumps