# HP0-A100<sup>Q&As</sup>

HP ArcSight Security Solutions

## Pass HP HP0-A100 Exam with 100% Guarantee

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

**https://www.geekcert.com/hp0-a100.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

Which function is performed by the ArcSight ESM Manager?

A. Aggregates events

B. Normalizes event data into CEF fields

C. Receives raw events from devices spread throughout the network

D. Prioritizes events

Correct Answer: B

**QUESTION 2**

What is the main purpose of using Identity View within an ESM environment?

A. To correlate identity information maintained by the Identity Management System with events generated m the network

B. To model network architecture within the ESM environment to perform advanced correlation on Asset and User events

C. To extract user and asset information from events in a logger environment to perform correlation analysis on them

D. To forward LDAP and active directory events to ESM Server

Correct Answer: B

**QUESTION 3**

Which component performs the data collection and normalization?

A. Data monitors

B. FSM manager

C. Smart Connectors

D. Correlation engine

Correct Answer: C

**QUESTION 4**

Which event lifecycle phase discovers the relationships between events, infers the significance of those relationships, prioritizes them, and provides a framework to take action?

A. Correlation evaluation

B. Priority evaluation and network model lookup

C. Workflow

D. Data collection and event processing

Correct Answer: C

---

QUESTION 5

What are the features that allow you to use Arc Sight Logger throughout your network?

A. Logger has pre-packaged content with forensics on-the-fly capability.

B. Logger allows you to deploy a single solution to manage all log data across your enterprise.

C. Logger uses a pattern matching and anomaly detection system to find very subtle and sophisticated threats.

D. Logger has two deployment options with a detached database.

Correct Answer: A

Latest HP0-A100 Dumps          HP0-A100 Practice Test          HP0-A100 Study Guide