

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

How does a CIP help an organization? (Select two.)

- A. Reduces deployment times of ArcSight components in the organization
- B. Contributes to establishing a strong IT governance program and reducing costs
- C. Shares, uploads, or downloads connectors within your Arc Sight community
- D. Helps to meet regulatory compliance requirements
- E. Helps to define high availability scenarios for ArcSight components

Correct Answer: BD

QUESTION 2

What are functions of a Smart Connector? (Select two)

- A. Collecting data from a source device
- B. Parking and normalizing events
- C. Long-term storage repository for events
- D. Performing correlation evaluation
- E. Discovering day-zero attacks

Correct Answer: AB

QUESTION 3

What is the main purpose of the ArcSight ESM?

- A. To archive raw event data
- B. To correlate events and provide real-time threat detection
- C. To centrally manage Smart Connector configuration
- D. To manage multiple retention policies

Correct Answer: B

QUESTION 4

In the Workflow phase, what are Annotations?

- A. Annotations are a field in the ESM event schema that enables you to flag events far follow up
- B. Annotations are pointers to an internal or external web page where a user can find more information about vulnerable
- C. Annotations are a monitoring tool used by Security Operation Centers
- D. Annotations are an ESM resource to export event data to third-party products, such as BMC Remedy

Correct Answer: C

QUESTION 5

Which task is performed by the manager during the Priority Evaluation and Network Model Lookup phase?

- A. Batching
- B. Parsing
- C. Asset model lookup
- D. Raw events processing

Correct Answer: D

[Latest HP0-A100 Dumps](#)

[HP0-A100 Practice Test](#)

[HP0-A100 Exam Questions](#)