



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.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

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





QUESTION 1

What does the ArcSight ESM prioritize?

- A. Every event
- B. Correlated events only
- C. Forwarded events only
- D. Every event exclusive of audit and monitor events

Correct Answer: B

QUESTION 2

How are CIPs licensed?

- A. CIPs are included as standard in Logger
- B. CIPs are additional, paid for components.
- C. CIPs are included as standard in Connector Appliance
- D. CIPs are included as standard in ESM

Correct Answer: A

QUESTION 3

How many ESM event schema groups are there?

- A. 5
- B. 17
- C. 300
- D. 400

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 for 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

For its correlation and automated event analysis capabilities, which ESM component is considered the brain of the HP ArcSight SIEM platform?

A. web server

B. ESM manager

C. ESM console

D. CORR-E database

Correct Answer: B

[HP0-A100 PDF Dumps](#)

[HP0-A100 VCE Dumps](#)

[HP0-A100 Practice Test](#)