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 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 2

The normalization process occurs at which event lifecycle phase?

A. Reporting and incident analysis

B. Monitoring and investigation

C. Priority evaluation and network model lookup

D. Data collection and event processing

Correct Answer: C

QUESTION 3

In which ESM event schema group can the Priority field with a value from 0 to 10 (calculated using ArcSight proprietary Threat Level Formula) be found?

A. Flex

B. Threat

C. Attacker

D. Root

Correct Answer: B

QUESTION 4

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 5

Which security product features are offered in ArcSight Express? (Select two)

A. SRL authentication support

B. Connector management

C. First I tool Wizard

D. Support for FIPS

E. Connector appliance functionality

Correct Answer: BD

QUESTION 6

Which component performs event aggregation?

A. ESM Database

B. ESM Manager

C. CORR-Engine

D. Smart Connectors

Correct Answer: D

QUESTION 7

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

![Pass2Lead](https://Pass2Lead.com)
QUESTION 8

Which statement is true about Arc Sight Identity View?

A. It uses the Arc Sight Actor Model Import Connector to populate and maintain the model in sync with your identity Management System (IDMS)

B. It is one core component of ArcSight ESM system without separate licensing.

C. It uses the Arc Sight Network Model Import Connector to populate and maintain the model in sync with your Identity Management System (IDMS)

D. It uses the Arc Sight Asset Model import Connector to populate and maintain the model in sync with your Identity Management System (IDMS)

Correct Answer: D

QUESTION 9

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 10

How many ESM event schema groups are there?

A. 5

B. 17

C. 300

D. 400

Correct Answer: B

Latest HP0-A100 Dumps   HP0-A100 VCE Dumps   HP0-A100 Study Guide