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.passapply.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 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 2

What is the purpose of the ArcSight ESM?

A. Enables a security bus that allows devices to communicate

B. Enables situational awareness and visibility of the security risks across an organization

C. Enables security device management using a common browser-based Management Console

D. Enables security integration between disparate devices

Correct Answer: B

QUESTION 3

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 4

Which component performs event aggregation?

A. ESM Database

B. ESM Manager

C. CORR-Engine

D. Smart Connectors

Correct Answer: D

QUESTION 5

What are three resources used in the Correlation phase of the event lifecycle?

A. Rules, active channels, trends

B. Dashboards, queries, filters

C. Query viewers, active channels, data monitors

D. Filters, rules, data monitors

Correct Answer: D

QUESTION 6

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 7

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 8

Which ESM component does the Event Priority Evaluation and Asset Model look up?

A. ESM console

B. CORR engine

C. Smart Connectors

D. ESM manager

Correct Answer: C

QUESTION 9

What is an ArcSight Logger architecture component?

A. Oracle Database

B. Receivers

C. Pattern Discovery

D. Correlation Engine

Correct Answer: D

QUESTION 10

Which type of ESM resources are imported from an external Identity Management System by using IdentityView?

A. Actors

B. Asset Categories

C. Users

D. Customers

Correct Answer: C