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.pass4itsure.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

What is a purpose of Smart Connectors?

A. To parse raw data

B. To calculate priority value

C. To generate reports

D. To perform correlation

Correct Answer: A

QUESTION 2

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 3

What is an example of a CIP package used for compliance?

A. DOD

B. NSA

C. PCI

D. MOD

Correct Answer: C

QUESTION 4

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 5

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 6

Which database management system technology is utilized by the Arc Sight ESM 6.5c?

A. DB2

B. CORR-Engine

C. SQL Server Express Edition

D. Oracle 10g

Correct Answer: B

QUESTION 7

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 8

Which statement is correct?

A. Smart Connectors cannot execute commands.

B. Smart Connect or installers are operating system independent

C. Smart Connectors use the Event Category Model to describe normalized events

D. Smart Connectors correlate events from raw data.

Correct Answer: C

QUESTION 9

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 10

What is IAM an acronym for?

A. Intrusion and Access Management

B. Identity and Access Management

C. Incident Account Management

D. Identity Account Management

Correct Answer: B