HP0-A100$^{\text{Q\&As}}$

HP ArcSight Security Solutions

Pass HP HP0-A100 Exam with 100% Guarantee

QUESTION 1

What is a reporting enhancement in ArcSight Express release 4.0?

A. Ability to include more than one chart type in a report

B. Ability to define non ESM users as recipients, and create a report once and distribute it to multiple recipients

C. Ability to generate reports of list members

D. Ability to generate reports of trend data

Correct Answer: B

QUESTION 2

Which resource used in the Workflow phase in the event lifecycle, .tracks either individual events or multiple related events?

A. Reports

B. Stages

C. Query viewers

D. Cases

Correct Answer: B

QUESTION 3

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

QUESTION 4

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 5

What is CIP an acronym for?

A. Collector Intrusion Package

B. Compliance Insight Package

C. Correlation Incursion Package

D. Component Instruction Package

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

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

What is the main purpose of the ArcSight ESM Query Viewer resource?

A. To view both SQL queries and reports in a dashboard

B. To view quick, high-level summaries of security events

C. To get low-level detailed event activities

D. To view and edit the underlying SOL queries

Correct Answer: B

QUESTION 9

What is the extension used to deliver and install CIPs?

A. aup

B. cab

C. cip

D. arb

Correct Answer: A

QUESTION 10

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