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.leads4pass.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

Which appliance provides advanced event correlation, event analysis and investigation, options for remediation and even, storage?

A. ArcSight Connector Appliance

B. ArcSight Network Configuration Manager/Threat Response Manager

C. ArcSight Logger Appliance

D. ArcSight Express

Correct Answer: C

QUESTION 2

How does the ArcSight ESM Manager display statistical views of the data on your network?

A. Active channels

B. Rules

C. Cases

D. Dashboards

Correct Answer: B

QUESTION 3

Which feature of Arc Sight Smart Connectors reduces the quantity of events sent to the ESM Manager?

A. Normalization

B. Host name lookup

C. Categorization

D. Aggregation

Correct Answer: D

QUESTION 4

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 5

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 6

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

QUESTION 7

In which phase are functions from the ESM Console (such as NS lookup, Ping, Port info, Trace route and who is) performed?

A. Workflow

B. Analysis

C. Trending

D. Correlation

Correct Answer: B

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

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 10

The ArcSight ESM collects, normalizes, aggregates, and filters millions of what?

A. Intrusions

B. Transactions

C. Packets

D. Log events

Correct Answer: D