HP0-A116^{Q&As}

HP0-A116$^{Q\&As}$

HP ArcSight ESM 6.5 Security Administrator and Analyst

Pass HP HP0-A116 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/hp0-a116.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

What can ArcSight ESM Dashboards display?

A. multiple Data Monitors

B. multiple Cases

C. multiple Stages

D. multiple Reports

Correct Answer: A

QUESTION 2

What do the start and end times associated with a notification destination indicate?

A. the period of time the system will wait for a notification response

B. the period of time during which the destination is expected to respond

C. the period of time during which the notification can be sent

D. the period of time during which the notification can be received

Correct Answer: C

QUESTION 3

What does the Priority Formula calculation run on?

A. FlexConnectors

B. SmartConnectors only

C. the Manager only

D. both SmartConnectors and the Manager

Correct Answer: C

QUESTION 4

What is the default port used by the ArcSight ESM Console to connect to the ArcSight Manager?

A. TCP 8443

B. UDP 8443

C. TCP 9443

D. UDP 9443

Correct Answer: A

QUESTION 5

In ESM, what allows contextual information to be added to an individual event or group of events in support of workflow or operational metrics?

A. Knowledge Base

B. Templates

C. Annotations

D. Rules

Correct Answer: C

QUESTION 6

The Packages view in the ArcSight Console Navigator provides access to all discrete resources that are part of a package in a single view. The dependency view toggle in the Package tree header shows required packages, which are packages on which other packages depend. What is the visual indicator of this dependency?

A. The package name is underlined.

B. The package name is shown in hold font.

C. The package icon contains a red asterisk.

D. The package icon is highlighted in yellow.

Correct Answer: A

QUESTION 7

Which component determines how a report looks when it is generated?

A. Query

B. Layout

C. Form

D. Template

Correct Answer: A

QUESTION 8

What does the ArcSight Manager use to automatically establish identity, ownership, and criticality of the assets installed on a network?

A. Asset Types

B. Asset Groups

C. Asset Categories

D. Asset Ranges

Correct Answer: C

QUESTION 9

Which functions does a non-event based Data Monitor perform?

A. evaluates the event stream and creates Correlation events when anomalies are discovered

B. monitors and displays rule and filter data flow thresholds and latencies

C. summarizes and displays event-based Data Monitor statistics

D. monitors and displays ArcSight ESM system and platform status

Correct Answer: D

QUESTION 10

Which statements are true about SmartConnectors and batching? (Select two.)

A. Batches can be sent when they reach a certain size.

B. Batches can be sent on command.

C. Batches can be sent in priority order by severity.

D. Batches can be sent by Connector type.

Correct Answer: AC

QUESTION 11

Which processes occur in the first phase of the event lifecycle? (Select two.)

A. evaluating event data

B. applying event categories

C. applying hashing to event data

D. correlating event data

E. normalizing event data

Correct Answer: BE

QUESTION 12

Asset categories can be assigned to zones as well as assets. What happens to the assets that belong to a zone with a category of "Critical"?

A. All assets in the zone inherit the zone\\'s category.

B. Nothing happens. Assets in the zone maintain their own individual category identities.

C. Assets with a category that matches the zone category are grouped into a "Critical" asset group.

D. Assets in the zone inherit the zone\\'s category and are grouped into a "Critical" asset group.

Correct Answer: B

QUESTION 13

What are functions of Query Viewers? (Select two.)

A. present detailed comparisons of report elements, not possible with the reporting tool

B. provide a baseline analysis of events against which future queries can be compared

C. determine which devices are off-line at any given point in time by querying their status

D. display the Boolean logic behind filters and rules

E. provide a quick way to run SQL queries and identify trends without running reports

Correct Answer: BE

QUESTION 14

If a username and password are used for authenticating a remote peer, when would you need to use those credentials a second time?

A. if credential caching expires and the auto-refresh option is not enabled

B. only if the peer relationship is broken and you need to authenticate the peer again

C. only for a content management subscriber manual synchronization

D. every time a distributed search is run and results are exported to the remote peer

Correct Answer: D

QUESTION 15

What is a good way for an operator or analyst to quickly determine which events must be addressed first?

A. check the priority rating in a Dashboard or Active Channel

B. run a report of High Priority Threats

C. ask more senior analysts or architects

D. view the Event Grid and Correlation categories

Correct Answer: A

Latest HP0-A116 Dumps   HP0-A116 Exam Questions   HP0-A116 Braindumps