Vendor: HP

Exam Code: HP0-A116

Exam Name: HP ArcSight ESM 6.5 Security Administrator and Analyst

Version: DEMO

QUESTION 1
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

Answer: BE

QUESTION 2
What do the start and end times associated with a notification destination indicate?

A. the period of time that the system waits for a notification response
B. the period of time during which the notification can be received
C. the period of time during which the destination is expected to respond
D. the period of time during which the notification can be sent to the destination

Answer: D

QUESTION 3
Which functions are on the right-click menu for an event in the ConsoleViewer panel? (Select two.)

A. Correlate Events
B. Show Event Details
C. Show Event Chart
D. Annotate Events
E. Prioritize Events

Answer: CE

QUESTION 4
Which statement best describes how baselines are established and used in Query Viewers?

A. Baselines are created using query results, which are fed into the Image Editor for filtering and display in the related Data Monitor.
B. Baselines are created using rules. After the rule is triggered, the resulting action establishes a baseline against which future rules are evaluated in the Query Viewer.
C. Baselines are created using query results. When a query has one or more baselines available, you can compare the current results with a baseline.
D. Baselines are created using query results. The baseline from the query is used to create a new field set definition that can be run against future events.

Answer: B

QUESTION 5
From where are the local ArcSight Console Preference Settings accessed?

A. File Menu
B. Edit Menu
C. Tools Menu
D. View Menu

Answer: C

QUESTION 6
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

Answer: D

QUESTION 7
Which statement is true about the ArcSight Web interface?

A. Inline filters cannot be used from the ArcSight Web interface.
B. Data Monitors cannot be added to a Dashboard from the ArcSightWebinterface.
C. Reports cannot be formatted from the ArcSight Web interface.
D. Cases cannot be modified from the ArcSight Web interface.

Answer: B

QUESTION 8
Where are the resource settings located that determine ArcSight ESM User Password Policy?

A. in the User E2 80 99s Access Control List
B. in the server.defaults.properties file
C. in the server.properties file
D. in either ArcSight Console or Command Center

Answer: B

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**