HP

Exam HP0-M54

ArcSight ESM Security Analyst

Version: 6.0

[Total Questions: 59]

Question No : 1

Which statement is true about inline filters?

A. An inline filter applies only to its current Active Channel.
B. An inline filter applies only as long as the Active Channel is open, and cannot be saved.
C. An inline filter cannot use AND or OR conditions.
D. An inline filter is created using Boolean logic in the Inspect/Edit panel.

Answer: A

Question No : 2

What stores information about logons, user actions, and the resulting events in the most concise way?

A. Event annotations
B. Session Lists
C. Active Lists
D. Cases

Answer: B

Question No : 3

Which statement is true about the ArcSight Web interface?

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

Answer: A

Question No : 4

What are valid actions for a rule to take? (Select two.)

A. send notification
B. execute command
C. generate report
D. add to filter

Answer: A,B

Question No : 5

Which user role is responsible for building content within ESM?

A. Administrator
B. Analyst
C. Author
D. Operator

Answer: C

Question No : 6

There are 17 event field groups defined in the ArcSight Event Schema. In which group would you look for data fields describing an event's importance as assessed by ArcSight ESM?

A. Category
B. Threat
C. Attacker
D. Event

Answer: B

Question No : 7

Which Event Schema group contains data fields, which describe the connector reporting an event?

A. Event

B. Device
C. Source
D. Agent

Answer: D

Question No : 8

What does a Network Model include? (Select two.)

A. assets
B. destinations
C. zones
D. file resources

Answer: A,C

Question No : 9

Which tools are used to view events in ArcSight ESM? (Select two.)

A. Active Channel
B. Knowledge Base article
C. Dashboard
D. Annotations

Answer: A,C

Question No : 10

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