



**Vendor:** HP

**Exam Code:** HP0-M54

**Exam Name:** ArcSight ESM Security Analyst

**Version:** DEMO

#### QUESTION 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 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 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 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:** AB

#### QUESTION 5

Which user role is responsible for building content within ESM?

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

**Answer: C**

**QUESTION 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 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 8**

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

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

**Answer: AC**

## 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>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC²  
where information lives®

**10% Discount Coupon Code: ASTR14**