

# PDFVCE



Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarantee in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

<http://www.pdfvce.com>

Highly Efficiently Exam Tool and Effective Exam Practice Materials

**Exam :** HP0-M54

**Title :** ArcSight ESM Security Analyst

**Vendors :** HP

**Version :** DEMO

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

NO.2 Which Event Schema group contains data fields, which describe the connector reporting an event?

- A. Event
- B. Device
- C. Source
- D. Agent

Answer: D

NO.3 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

Answer: A

NO.4 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

NO.5 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

NO.6 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

NO.7 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

NO.8 What does a Network Model include? (Select two.)

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

Answer: A,C

NO.9 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

NO.10 Which user role is responsible for building content within ESM?

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

Answer: C

