Vendor: HP

Exam Code: HP0-M54

Exam Name: ArcSight ESM Security Analyst

Version: Demo

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
Explanation:

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
Explanation:

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
Explanation:

QUESTION NO: 4

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

Answer: A,B
Explanation:

QUESTION NO: 5

Which user role is responsible for building content within ESM?

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

Answer: C
Explanation:

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
Explanation:

QUESTION NO: 7

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

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

Answer: D
Explanation:

QUESTION NO: 8

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

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

Answer: A,C
Explanation:

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
Explanation:

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

Answer: A
Explanation:

QUESTION NO: 11

What happens if a notification requiring a response within 24 hours is not acknowledged within that time?

A. The notification is escalated to the next level of notification.
B. The notification is added to the Session List.
C. An error message appears on the ArcSight Console.
D. The condition generating the notification is escalated to a higher priority.

Answer: A
Explanation:

QUESTION NO: 12

What represents the current status in the investigation of a Case?

A. Notifications
B. Cases
C. Annotations
D. Stages

Answer: D
Explanation:

QUESTION NO: 13

Why would you lock a Case?

A. to close and archive a Case

B. to prevent others from modifying the Case while you edit or attach something to the Case
C. to prevent the Case from being seen in the Resource List
D. to preserve the state of the Case

Answer: B
Explanation:

QUESTION NO: 14

What is the primary function of the ArcSight Manager?

A. It accepts correlated, prioritized events from SmartConnectors with instructions from the ArcSight Console, and writes events to the database.
B. It manages bottlenecks between the connectors, the ArcSight Console, and the ESM Database.
C. It writes incoming events to the database while simultaneously processing events through the Correlation engine.
D. It restores the rule definitions that drive the functioning of ArcSight ESM.

Answer: C
Explanation:

QUESTION NO: 15

Which ESM components collect event data?

A. SmartConnectors
B. events
C. resources
D. nodes

Answer: A
Explanation:

QUESTION NO: 16

What can you use to change the stage of a Case?

A. Event annotations

B. Case Editor
C. Query Viewer
D. Common Conditions Editor

Answer: B
Explanation:

QUESTION NO: 17

What is the "focus" of a Focus report?

A. the differences between two similar reports
B. a subset of a larger (e.g., monthly or quarterly) report
C. events that have been missed
D. high priority Correlation events only

Answer: B
Explanation:

QUESTION NO: 18

Which type of event is displayed in an Active Channel with the following Inline Filter applied?

Category Behavior = /Authentication/Verify

Category Outcome = /Failure

A. Logout events
B. Login Success events
C. Login Failure events
D. Account Locked events

Answer: C
Explanation:

QUESTION NO: 19

Which resource defines what a report will look like when generated?

A. layout
B. query
C. template
D. form

Answer: C
Explanation:

QUESTION NO: 20

What must be done to a local Variable before it can be used with multiple resources?

A. It must be renamed.
B. It must be copied.
C. It must be moved it to a new resource.
D. It must be promoted to a Global Variable.

Answer: D
Explanation:

QUESTION NO: 21

Which functions are on the right-click menu for an event? (Select two.)

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

Answer: B,C
Explanation:

QUESTION NO: 22

Which role does the Active Channel play in testing a rule?

A. The rule can be replayed and verified against real-time events in the Active Channel.
B. The rule can be replayed against historical events in the Active Channel.

C. The rule cannot be tested with the Active Channel because it will create additional invalid Correlation events.
D. The rule can only be tested with an Active Channel by an administrator.

Answer: B
Explanation:

QUESTION NO: 23

Which output formats are available when running a report? (Select two.)

A. XML
B. HTML
C. PDF
D. JPEG

Answer: B,C
Explanation:

QUESTION NO: 24

At most, a zone can belong to how many networks?

A. 0 (Zones do not belong to networks, zones contain networks.)
B. 1
C. 2
D. as many as needed based on the Network Model

Answer: B
Explanation:

QUESTION NO: 25

In network modeling, what are SmartConnectors bound to? (Select two.)

A. zones
B. assets
C. devices

D. customers
E. networks

Answer: D,E
Explanation:

QUESTION NO: 26

Report run start time, output format for report results, email distribution for report results, and report filters are all examples of what?

A. report parameters
B. report formats
C. report data sources
D. report attributes

Answer: A
Explanation:

QUESTION NO: 27

When using the Query Editor, three sub-tabs provide the options you need to properly set up the query. What information do these sub-tabs require?

A. when the query should be run; which format the query output should take; how many data elements should be included
B. when the query should be run; what the query should be called; how long the data should be archived
C. which data fields to select; how the data should be displayed; how long the data should be archived
D. which data fields to select; how the data should be ordered; how the data should be grouped

Answer: D
Explanation:

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

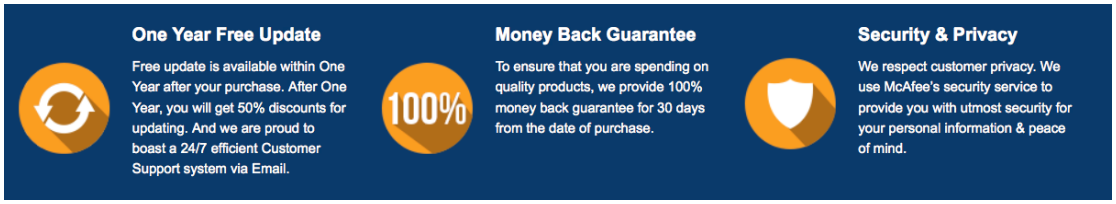
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions