HP HP0-M54

ArcSight ESM Security Analyst

Version: 4.0

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

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
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

event?

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:

QUESTION NO: 28

What is a function of the Variable GetSessionData?

A. retrieves data fields from a Session List
B. sends session details to the ArcSight Manager
C. populates a Session List
D. investigates session details in the audit log

Answer: A
Explanation:

QUESTION NO: 29

Which string function is used to join two data fields?

A. Correlate
B. Concatenate
C. Substring
D. Find

Answer: B
Explanation:

QUESTION NO: 30

What are functions of Query Viewers? (Select two.)

A. present detailed comparisons of report elements, not possible with the reporting tool
B. provide a baseline analysis of events against which future queries can be compared
C. determine which devices are off-line at any given point in time by querying their status
D. display the Boolean logic behind filters and rules
E. provide a quick way to run SQL queries and identify trends without running reports

Answer: B,E
Explanation:

QUESTION NO: 31

How are baselines established and used in Query Viewers?

A. Baselines are created using rules. After the rule is triggered, the resulting action establishes a

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

Answer: C
Explanation:

QUESTION NO: 32

In network modeling, what is a set of nodes with similar characteristics that have IPs enumerated one after the other?

A. IP group
B. asset group
C. asset range
D. IP range

Answer: C
Explanation:

QUESTION NO: 33

Which statements are true about assets? (Select two.)

A. Assets can be grouped in folders called asset ranges.
B. Assets require a MAC address to be categorized properly.
C. Assets can include bridges, routers, web servers, or anything with an IP or MAC address.
D. An asset is any endpoint considered significant enough to characterize with details to help with correlation and reporting.

Answer: C,D
Explanation:

QUESTION NO: 34

In network modeling, which resource is used by MSSP or by users with different cost centers?

A. networks
B. zones
C. customers
D. asset groups

Answer: C
Explanation:

QUESTION NO: 35

What is the name of the resource you can use to override the default ArcSight mapping of IP addresses to geographic regions?

A. zones
B. destinations
C. locations
D. categories

Answer: C
Explanation:

QUESTION NO: 36

What do you use to establish identity, ownership, and criticality of the assets you have installed on your network?

A. asset types
B. asset groups
C. asset categories
D. asset ranges

Answer: C
Explanation:

QUESTION NO: 37

Asset categories can be assigned to zones as well as assets. What happens to the assets that belong to a zone with a category of "Critical"?

A. All assets in the zone inherit the zone's category.
B. Nothing happens. Assets in the zone maintain their own individual category identities.
C. Assets with a category that matches the zone category are grouped into a "Critical" asset group.
D. Assets in the zone inherit the zone's category and are grouped into a "Critical" asset group.

Answer: B

Explanation:

QUESTION NO: 38

Which statements are true about event lifecycle data collection and the event processing phase? (Select two.)

A. Model confidence is determined, based on details provided by the event source.
B. Each line of incoming log data is processed as a separate event.
C. Event severity is determined, based on an Active List of recent severity factors.
D. Values are normalized and entered into the ArcSight Event Schema.

Answer: B,D

Explanation:

QUESTION NO: 39

Which process uncovers the relationship between events, infers the significance of those relationships, prioritizes them, and then provides a framework for taking action?

A. categorization
B. aggregation
C. correlation
D. filtration

Answer: C

Explanation:

QUESTION NO: 40

How do asset categorization and event categorization relate to each other?

A. Asset categorization and event categorization are the same.
B. Asset categorization and event categorization use the same field set to apply categories to assets and events.
C. Asset categorization requires custom FlexConnectors; event categorization uses standard SmartConnectors.
D. Asset categorization is the fingerprint of an asset; event categorization is a set of criteria that describes an event.

Answer: D
Explanation:

QUESTION NO: 41

What does the Priority Formula calculation run on?

A. FlexConnectors
B. SmartConnectors only
C. the Manager only
D. both SmartConnectors and the Manager

Answer: C
Explanation:

QUESTION NO: 42

What is a criteria factor within the ArcSight Priority Formula?

A. Assurance
B. Asset Priority
C. Seriousness
D. Model Confidence

Answer: D
Explanation:

QUESTION NO: 43

What can ArcSight ESM Dashboards display?

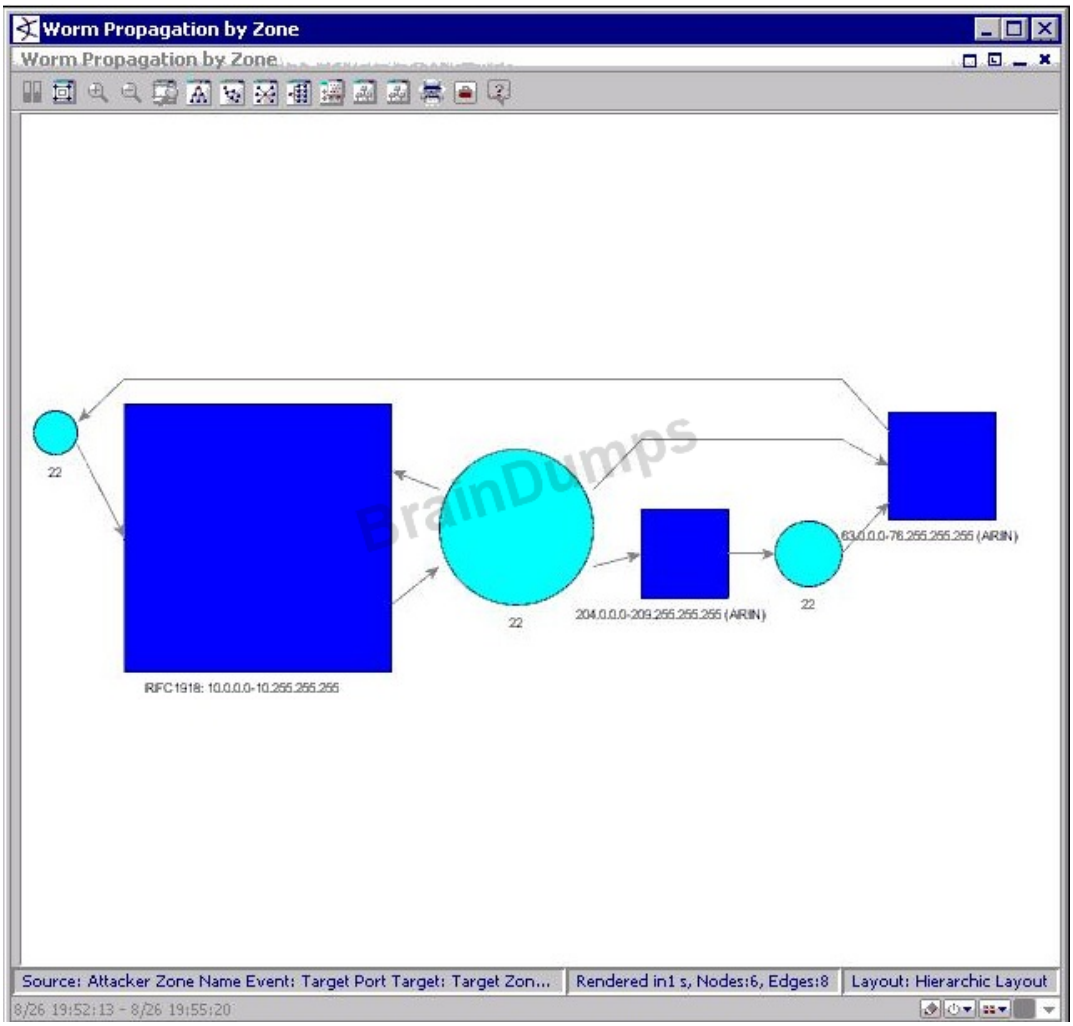
A. multiple Data Monitors
B. multiple Cases
C. multiple Stages
D. multiple Reports

Answer: A

Explanation:

QUESTION NO: 44

Click the Exhibit button.



Which type of diagram is shown in the exhibit?

A. a geographic hierarchy map

B. an event graph
C. an image viewer map
D. a query topology

Answer: B
Explanation:

QUESTION NO: 45

What are the three types of Data Monitors?

A. event type, matching conditions, and non-event
B. event-based, correlation, and non-event based
C. event type, correlation, and aggregation matching
D. event-based, event graph, and non-event based

Answer: B
Explanation:

QUESTION NO: 46

Event correlation, event reconciliation, moving average, session reconciliation, and statistics are all examples of which type of Data Monitors?

A. event-based
B. non-event-based
C. correlation
D. system status

Answer: C
Explanation:

QUESTION NO: 47

What is an example of an event-based Data Monitor?

A. moving average
B. rules partial match

C. last n events
D. session reconciliation

Answer: C
Explanation:

QUESTION NO: 48

Which command is a valid investigate command?

A. Add [Attribute=Value] to Filter
B. Create [Filter=Value]
C. Add [Value!=Condition] to Filter
D. Add to Filter [List of Related Conditions]

Answer: A
Explanation:

QUESTION NO: 49

Which statement is true about how filters are applied by the Connector or by the Manager?

A. When filters are applied by either the Connector or the Manager, events that match the filter conditions are selected and forwarded forfurther processing.
B. When filters are applied by either the Connector or the Manager, events that match the filter conditions are excluded and are not forwardedfor further processing.
C. Events that match the Connector filter are excluded and not forwarded further; events that match the Manager filter are selected for furtheranalysis.
D. Events that match the Connector filter are included and forwarded to the Manager; events that match the Manager filter are excluded.

Answer: C
Explanation:

QUESTION NO: 50

Which are operators in the ArcSight Common Conditions Editor (CCE)? (Select two.)

A. ELSE
B. AND
C. OR
D. IF

Answer: B,C
Explanation:

QUESTION NO: 51

Which resources can be displayed in the ArcSight Web interface? (Select two.)

A. Reports and Dashboards
B. Queries and Partitions
C. Cases, Notifications, and Active Channels
D. Knowledge Base articles and Templates

Answer: A,C
Explanation:

QUESTION NO: 52

When specifying the attributes of a new Active List, you can set TTL days, hours, and minutes. What is TTL?

A. Total Time Lag
B. Time Threshold Lag
C. Time To Live
D. Total Time Left

Answer: C
Explanation:

QUESTION NO: 53

What do field sets correspond to?

A. Variables in a rule configuration

B. components in a Network Model
C. attributes in a Query Viewer
D. columns in an Active Channel Grid view

Answer: D
Explanation:

QUESTION NO: 54

Which statement is true about a join rule?

A. It is triggered by events that match a single set of conditions.
B. It matches the output of more than one simple rule to an Active List.
C. It recognizes patterns that involve more than one type of event.
D. It rejects partial matches but can be set for aggregation.

Answer: C
Explanation:

QUESTION NO: 55

Which statement is true about join rules and chained rules?

A. Join rules link simple rules together; chained rules link join rules.
B. Join rules use Session Lists; chained rules use Active Lists.
C. Chained rules may or may not be join rules that also use Active Lists or rely on Correlation events generated by other rules.
D. Chained rules result in detailed chains; join rules result in simple chains.

Answer: C
Explanation:

QUESTION NO: 56

Using SSL technology, information can be communicated over an encrypted channel. What is SSL?

A. Standard Security Layer

B. Smart Stealth Layer
C. Secure Sockets Layer
D. Security Standards Layer

Answer: C
Explanation:

QUESTION NO: 57

You want your Active Channel to automatically display new events as they arrive at ESM. Which time parameter should you use to accomplish this?

A. Evaluate Once at Attach Time
B. Evaluate $NOW-1h
C. Continuously Evaluate
D. Evaluate Continuously from Attach Time

Answer: C
Explanation:

QUESTION NO: 58

Which ArcSight ESM Resource enables you to perform live monitoring of events?

A. Cases
B. Active Channels
C. Stages
D. Knowledge Base

Answer: B
Explanation:

QUESTION NO: 59

Active Channel views and Dashboard views are examples of Viewer Panel views. Which other views are associated with the Viewer Panel? (Select two.)

A. Asset views

B. Resource views
C. Combined views
D. Simple views
E. Results views

Answer: B,E

Explanation: