1. Which tools are used to view events in ArcSight ESM?

Active Channel

Dashboard

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

Session Lists

3. Which statement is true about inline filters?

An inline filter applies only to its current Active Channel.

4. Which statement is true about the ArcSight Web interface?

Data Monitors cannot be added to a Dashboard in the ArcSight Web interface.

5. What are valid actions for a rule to take?

send notification

execute command

6.Which user role is responsible for building content within ESM?

Author

7. which group would you look for data fields describing an event’s importance as assessed by ArcSight ESM?

Threat

8. which describe the connector reporting an event?

Agent

9.What does a Network Model include?

assets

zones

10. What is a good way for an operator or analyst to quickly determine which events must be addressed first?

check the priority rating in a Dashboard or Active Channel

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

The notification is escalated to the next level of notification.

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

Stages

13. Why would you lock a Case?

to prevent others from modifying the Case while you edit or attach something to the Case

14. What is the primary function of the ArcSight Manager?

It writes incoming events to the database while simultaneously processing events through the Correlation engine.

15. Which ESM components collect event data?

SmartConnectors

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

Case Editor

17. What is the "focus" of a Focus report?

a subset of a larger (e.g., monthly or quarterly) report

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

Category Behavior = /Authentication/Verify

Category Outcome = /Failure

Login Failure events

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

template

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

It must be promoted to a Global Variable.

21. Which functions are on the right-click menu for an event?

Show Event Details

Annotate Events

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

The rule can be replayed against historical events in the Active Channel.

23. Which output formats are available when running a report?

HTML

PDF

24. how many networks?

1

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

customers

networks

26. 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?

->which data fields to select; how the data should be ordered; how the data should be grouped

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

report parameters

28. What is a function of the Variable GetSessionData?

retrieves data fields from a Session List

29. Which string function is used to join two data fields?

Concatenate

30. What are functions of Query Viewers?

provide a baseline analysis of events against which future queries can be compared

provide a quick way to run SQL queries and identify trends without running reports

31. How are baselines established and used in Query Viewers?

Baselines are created using query results. When a query has one or more baselines available,

you can compare the current results with thebaseline.

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

Asset range

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

Assets can include bridges, routers, web servers, or anything with an IP or MAC address.

An asset is any endpoint considered significant enough to characterize with details to help with correlation and reporting.

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

Customers

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

locations

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

asset categories

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”?

Nothing happens. Assets in the zone maintain their own individual category identities.

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

Each line of incoming log data is processed as a separate event.

Values are normalized and entered into the ArcSight Event Schema.

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

action?

correlation

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

Asset categorization is the fingerprint of an asset; event categorization is a set of criteria that describes an event.

41. What does the Priority Formula calculation run on?

the Manager only

42. What is a criteria factor within the ArcSight Priority Formula?

Model Confidence

43. What can ArcSight ESM Dashboards display?

multiple Data Monitors

44. Which type of diagram is shown in the exhibit?

an event graph

45.What are the three types of Data Monitors?

event-based, correlation, and non-event based

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

correlation

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

last n events

48. Which command is a valid investigate command?

Add [Attribute=Value] to Filter

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

Events that match the Connector filter are excluded and not forwarded further; events that match the Manager filter are selected for furtheranalysis.

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

AND

OR

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

Reports and Dashboards

Cases, Notifications, and Active Channels

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

What is TTL?

Time To Live

53. What do field sets correspond to?

columns in an Active Channel Grid view

54. Which statement is true about a join rule?

It recognizes patterns that involve more than one type of event.

55. Which statement is true about join rules and chained rules?

Chained rules may or may not be join rules that also use Active Lists or rely on Correlation events generated by other rules.

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

Secure Sockets Layer

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?

Continuously Evaluate

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

Active Channels

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

Resource views

Results views