Questions 1. What must be done first to restore the database from an online backup?   
  
A. run the Oracle restore wizard   
B. ensure that the archived redo logs are located in the archive log destination   
C. bring the affected tablespaces online   
D. reinstall the Oracle installation   
Answer: A  
  
Questions 2. What happens when a Connector upgrade that was initiated from within the ArcSight Console fails?   
  
A. The Connector automatically rolls back to the previously working version.   
B. The Connector does not respond to the failed upgrade.   
C. The Connector reports to the Manager that the upgrade failed and then died.   
D. The Connector automatically attempts the upgrade again.   
Answer: A  
  
Questions 3. With regard to SmartConnectors, what is roll back?   
  
A. collecting cached data after a communication failure   
B. uninstallation of a package in the event of failure   
C. a way to revert to the previous version of a Connector when a Connector upgrade fails   
D. a way to gather data that has moved beyond the archive window   
Answer: C  
  
Questions 4. Which statement is true about starting and stopping ArcSight SmartConnector services?   
  
A. They are started and stopped independently of the other ArcSight component services.   
B. The order in which they are started and stopped is based on event flow.   
C. How they are started and stopped depends on whether or not the ArcSight Manager is running.   
D. They are started and stopped in conjunction with the Oracle database services.   
Answer: A  
  
Questions 5. What is a trust store (sometimes called a key store)?   
  
A. the preferred source for obtaining signed certificates   
B. a list of trusted Certificate Authorities   
C. the location of a system's private keys   
D. the set of backup files containing SSL information   
Answer: B  
  
Questions 6. Which key pair types are valid selections when using the Manager Setup Wizard to create an SSL key pair? (Select two.)   
  
A. non-expiring SSL key pair   
B. self-signed key pair   
C. demo key pair   
D. random generator key pair   
Answer: B  
  
Questions 7. During Connector install, which statement is true about the ArcSight Manager's host name or IP address?   
  
A. It must match the host name or IP address in the ArcSight Manager's SSL certificate.   
B. The host name or IP address is used as an encryption key.   
C. It can be any legitimate host name or IP address.   
D. It must contain a combination of alpha-numeric characters.   
Answer: A  
  
Questions 8. What are ArcSight Foundations?   
  
A. user groups organized to explore and share ideas for extending ArcSight ESM capabilities   
B. coordinated resources that provide monitoring, analysis, and reporting capabilities   
C. categories of resources used for monitoring ArcSight system health and status   
D. packages that are installed but cannot be modified   
Answer: B  
   
Questions 9. Which ArcSight Foundation should you use to identify traffic and bandwidth usage?   
  
A. Configuration Monitoring   
B. Intrusion Monitoring   
C. ArcSight Administration   
D. Network Monitoring   
Answer: D  
   
Questions 10. Which ArcSight Foundation should you use to identify and analyze unexpected modifications to systems, devices, or applications?   
A. Configuration Monitoring   
B. Intrusion Monitoring   
C. ArcSight Administration   
D. Network Monitoring   
Answer: A

Questions 11. There are three types of ArcSight SmartConnectors. Which type is used primarily to execute commands on a device to retrieve, modify, or analyze its configuration?   
  
A. Event Connectors   
B. Scanner Connectors   
C. CounterACT Connectors   
D. SNMP Connectors   
Answer: C  
   
Questions 12. Which file types MUST be included in an Oracle backup? (Select two.)   
  
A. table files   
B. data files   
C. program files   
D. configuration files   
Answer: B  
   
Questions 13. How can you restore a new ArcSight Web installation to a previous configuration?   
  
A. copy the old ArcSight Web installation's config directory and cacerts file into the new installation   
B. copy the ArcSight Manager's config directory into the new installation   
C. manually reconfigure the new installation   
D. connect to the Manager and download the saved configuration   
Answer: A  
   
Questions 14. In Network Modeling, what is closest to being a subnet?   
A. zone   
B. network   
C. Asset Range   
D. Network Range   
Answer: A  
   
Questions 15. Which components does a Network Model include? (Select two.)   
A. assets   
B. data monitors   
C. dashboards   
D. zones   
Answer: A,D  
   
Questions 16. In Network Modeling, what are SmartConnectors bound to? (Select two.)   
  
A. zones   
B. networks   
C. devices   
D. customers   
Answer: D  
   
Questions 17. What is a Network Model?   
  
A. a representation of the nodes on a network and certain characteristics of the network itself   
B. a preconfigured resource used to set up ArcSight zones and communication paths   
C. a dashboard containing data monitors for network, zone, asset, and customer monitoring   
D. a diagram of network interface points and vulnerabilities   
Answer: A  
   
Questions 18. Package bundles are exported with which file extension?   
  
A. .xml file   
B. .exe file   
C. .msc file   
D. .arb file   
Answer: D  
   
Questions 19. Which command is used to modify retention periods?   
  
A. Arcsight archive install   
B. Arcsight database create   
C. Arcsight retention create   
D. Arcsight database pc   
Answer: D  
   
Questions 20. What is an offline partition?   
  
A. a partition that resides within the database   
B. a partition that exceeds the online retention threshold and is therefore archived   
C. a partition reserved for a future date   
D. data that is no longer needed by ESM   
Answer: C  
  
Questions 21. Which statements are true about retention areas? (Select two.)   
  
A. Retention policies cannot be changed once they are set.   
B. Retention areas can be configured using the Partition Management Wizard.   
C. If the size of a retention area is reduced, the data outside of the retention area is automatically backed up.   
D. Archived partitions outside the offline archive period become invalid.   
Answer: B,D  
   
Questions 22. When configuring the ArcSight Database, what is the result of setting the offline archive period (Days) to Zero?   
  
A. Partition Archiving is enabled.   
B. Partition Archiving is disabled.   
C. Online retention is enabled.   
D. Online reserved period is enabled.   
Answer: B  
   
Questions 23. What does Partition Archiving allow you to specify?   
  
A. the number of partitions to keep offline   
B. the number of partitions that remain online   
C. the compression ratio to be used in partitioning   
D. the amount of data to store in a partition   
Answer: A  
   
Questions 24. What is the Reserve Period?   
  
A. the amount of time to allow before compressing event data for storage   
B. the number of future partitions to be maintained   
C. the amount of time to wait before determining that a device is not operating   
D. the maximum length of time archived partitions will be stored   
Answer: B  
   
Questions 25. What is stored in a database partition?   
  
A. as much data as it can hold   
B. a user-configurable number of events   
C. events from a one week time period   
D. events from a 24-hour time period   
Answer: B  
   
Questions 26. When can the online partition compression task fail? (Select two.)   
  
A. when the partition being compressed is too old   
B. when events are inserted into the partition that is being compressed   
C. when the compression task takes more than two hours to complete   
D. when the partition compressor does not have the necessary file permissions   
Answer: B,C  
   
Questions 27. You are unable to see events from a specific device in the Console. The Active Channel filters are not the cause. Which component should you examine next in order to troubleshoot this issue?   
  
A. Database   
B. SmartConnector   
C. Console   
D. Device   
Answer: B  
   
Questions 28. Which statements are true about SmartConnectors and batching? (Select two.)   
  
A. Batches can be sent when they reach a certain size.   
B. Batches can be sent on command.   
C. Batches can be sent in priority order by severity.   
D. Batches can be sent by Connector type.   
Answer: A,C  
   
Questions 29. Preserve Raw Events, Turbo Mode, and Limit Event Processing Rate are all examples of which type of Connector options?   
  
A. Processing options   
B. Aggregation options   
C. Filter conditions   
D. Preservation options   
Answer: A  
   
Questions 30. Which document provides the most detailed instructions for applying an Oracle CPU?   
  
A. Oracle CPU release notes   
B. ArcSight ESM Administrator's Guide   
C. Opatch Readme file   
D. ArcSight ESM Installation Guide   
Answer: D  
  
Questions 31. What is a bundle?   
  
A. a set of resources that makes up a package   
B. a data transmission containing SSL information   
C. a set of raw log events before they are parsed   
D. a container for one or more packages   
Answer: D  
   
Questions 32. Which method is used to back up an Oracle database without shutting down the database?   
  
A. sequential backup   
B. standalone backup   
C. online backup   
D. offline backup   
Answer: C  
   
Questions 33. Which command should you use to configure notification acknowledgements after the initial configuration of ArcSight ESM?   
  
A. arcsight managersetup   
B. arcsight notifysetup   
C. arcsight notifyconfig   
D. arcsight setupnotify   
Answer: A  
   
Questions 34. What are capabilities of the ArcSight Manager? (Select two.)   
  
A. receives event data from SmartConnectors   
B. normalizes events from devices   
C. performs advanced event correlation and analysis   
D. allows users to perform security monitoring through a built-in web interface   
Answer: A,C  
   
Questions 35. Which statement is true about the ArcSight Web Server?   
  
A. It is not required.   
B. It is required if users will be accessing ESM through a web browser.   
C. It should always be installed on the same server as the ArcSight Manager.   
D. It can be used to create rules and view reports.   
Answer: B  
   
Questions 36. Which command is used to add a secondary destination to a Connector's configuration?   
  
A. arcsight destinations -n   
B. arcsight connectorsetup -w   
C. arcsight connectionwizard   
D. arcsight connector -d   
Answer: B  
   
Questions 37. Using SSL technology, information can be communicated over an encrypted channel. What is SSL?   
  
A. Secure Sockets Layer   
B. Security Standards Layer   
C. Smart Stealth Layer   
D. Standard Security Layer   
Answer: A  
   
Questions 38. Which are clients of the ArcSight Manager? (Select two.)   
  
A. ArcSight Correlation Engine   
B. ArcSight Web   
C. ArcSight SmartConnectors   
D. ArcSight Database   
Answer: B,C  
   
Questions 39. One of the benefits of SSL technology is authentication. What does authentication do?   
  
A. validates client logins using advanced identity detection technology   
B. encrypts information sent between clients and servers   
C. adds a hashing algorithm to prevent data modification between client and server   
D. ensures that clients send information to the actual intended server, not a machine pretending to be that server   
Answer: D  
   
Questions 40. What is the default port used when connecting to the ArcSight Web interface?   
  
A. TCP 9443   
B. UDP 9443   
C. TCP 8443   
D. UDP 8443   
Answer: A  
Questions 41. What is the default port used by the ArcSight ESM Console to connect to the ArcSight Manager?   
  
A. TCP 8443   
B. UDP 8443   
C. TCP 9443   
D. UDP 9443   
Answer: A  
  
Questions 42. What is the default port used to connect the ArcSight Manager to the ArcSight ESM Database (Oracle)?   
  
A. 443   
B. 1443   
C. 1521   
D. 8443   
Answer: C  
   
Questions 43. The ArcSight Web release version must be the same version as what?   
  
A. ArcSight Manager   
B. ArcSight Database   
C. ArcSight SmartConnectors   
D. ArcSight Console   
Answer: A  
   
Questions 44. What must you do prior to applying a patch to the ArcSight Manager?   
  
A. stop the ArcSight Manager service   
B. shut down all ArcSight SmartConnectors   
C. delete all files in the tmp directory   
D. disconnect the network cable   
Answer: A  
   
Questions 45. What do the start and end times associated with a notification destination indicate?   
  
A. the period of time the system will wait for a notification response   
B. the period of time during which the destination is expected to respond   
C. the period of time during which the notification can be sent   
D. the period of time during which the notification can be received   
Answer: C  
   
Questions 46. Which actions might the whine daemon initiate? (Select two.)   
  
A. sending a message to the admin consoles   
B. sending SNMP traps to a monitoring station   
C. sending syslog messages to a syslog server   
D. writing an event to the server.log file   
Answer: A,D  
   
Questions 47. What are potential ways of acknowledging notifications? (Select two.)   
  
A. by replying to notification email   
B. by calling in to the notification response hotline   
C. by sending email to SysAdmin   
D. by using the Notifications Manager in the ArcSight Console   
Answer: A,D  
   
Questions 48. Which statement is true about ArcSight SmartConnectors acting in "passive" mode?   
  
A. They receive events forwarded from originating devices.   
B. They pull events from originating devices.   
C. They do not process events from devices.   
D. They process events for performance testing but then discard them.   
Answer: A  
   
Questions 49. Which statement is true about Connectors that are in a Paused state?   
  
A. Paused Connectors are responding to the Manager but not sending or caching events.   
B. Paused Connectors are responding to the Manager but events are being cached.   
C. Paused Connectors are responding to the Manager and sending events.   
D. Paused Connectors are not responding to the Manager.   
Answer: B  
   
Questions 50. ArcSight SmartConnectors send event data directly to what?   
  
A. ArcSight Manager   
B. ArcSight Console   
C. ArcSight Web Server   
D. ArcSight Database   
Answer: A

Questions 51. Which command is used to check the status of the TNS Listener?   
  
A. lsnrctl status   
B. listener status   
C. tnsstat   
D. oralistener status   
Answer: A  
   
  
Questions 52. Which ArcSight Manager directory should be backed up in order to preserve the server.properties file?   
  
A. user directory   
B. config directory   
C. properties directory   
D. jre directory   
Answer: B  
   
  
Questions 53. What is the name of the resource you can use to override the default ArcSight mapping IP addresses to geographic regions?   
  
A. zones   
B. destinations   
C. locations   
D. categories   
Answer: C  
   
  
Questions 54. What does the ArcSight Manager use to automatically establish identity, ownership, and criticality of the assets installed on a network?   
  
A. Asset Types   
B. Asset Groups   
C. Asset Categories   
D. Asset Ranges   
Answer: C  
   
  
Questions 55. Which three attributes are used to describe an Asset Model?   
  
A. vulnerabilities, locations, and asset categories   
B. locations, asset categories, and threats   
C. asset types, asset categories, and locations   
D. vulnerabilities, addresses, and threats   
Answer: A  
   
  
Questions 56. Which statements are true about user groups? (Select two.)   
  
A. They can be based on departments, permission levels, or roles.   
B. They control which users are allowed to log in to the Console.   
C. They can be nested within other user groups.   
D. They are enabled or disabled using Access Control Lists.   
Answer: A,C  
   
  
Questions 57. Which statements are true about user groups and resources? (Select two.)   
  
A. Resources are only visible to a user if the user's group has "Read" permissions for the resource.   
B. A group with "inspect" permission enabled allows all users in that group to edit resources.   
C. To change a user's permission to access a resource group, you either change the permissions of the user's group or put the user in a new group with different permissions.   
D. A resource can only be accessed by a user if the user's group has "viewer" permissions for the resource.   
Answer: A,C  
   
  
Questions 58. Which tablespace is used by ArcSight to store resources?   
  
A. ARC\_EVENT\_DATA   
B. ARC\_SYSTEM\_INDEX   
C. ARC\_SYSTEM\_DATA   
D. ARC\_EVENT\_INDEX   
Answer: C  
   
  
Questions 59. Which statement is true about ArcSight Database structures?   
  
A. Data tablespaces typically use more disk space than indices.   
B. Indices typically use more disk space than data tablespaces.   
C. There is no appreciable difference between index and data tablespaces.   
D. The system data tablespace is always much larger than the event data tablespace.   
Answer: B  
   
  
Questions 60. Which statement is true about SmartConnectors and FlexConnectors?   
  
A. FlexConnectors allow creation of SmartConnectors that are tailored to individualized custom situations and specific security event data.   
B. FlexConnectors are plug-and-play, self-programming SmartConnectors.   
C. SmartConnectors do not include tools for customizing FlexConnectors.   
D. SmartConnectors are vendor-specific and must be purchased through the individual device vendors.   
Answer: A

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.

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

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

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

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

A. Administrator

B. Analyst

**C. Author**

D. Operator

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

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

event?

A. Event

B. Device

C. Source

**D. Agent**

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

**A. assets**

B. destinations

**C. zones**

D. file resources

9. Which tools are used to view events in ArcSight ESM? (Select two.)

**A. Active Channel**

B. Knowledge Base article

**C. Dashboard**

D. Annotations

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

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.

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

A. Notifications

B. Cases

C. Annotations

**D. Stages**

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

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.

15. Which ESM components collect event data?

**A. SmartConnectors**

B. events

C. resources

D. nodes

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

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

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

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

A. layout

B. query

**C. template**

D. form

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**

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

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.

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

A. XML

**B. HTML**

**C. PDF**

D. JPEG

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

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

A. zones

B. assets

C. devices

**D. customers**

**E. networks**

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

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**

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

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

A. Correlate

**B. Concatenate**

C. Substring

D. Find

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**

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.

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

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.**

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

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

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

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.

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**.

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

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.**

41. What does the Priority Formula calculation run on?

A. FlexConnectors

B. SmartConnectors only

**C. the Manager only**

D. both SmartConnectors and the Manager

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

A. Assurance

B. Asset Priority

C. Seriousness

**D. Model Confidence**

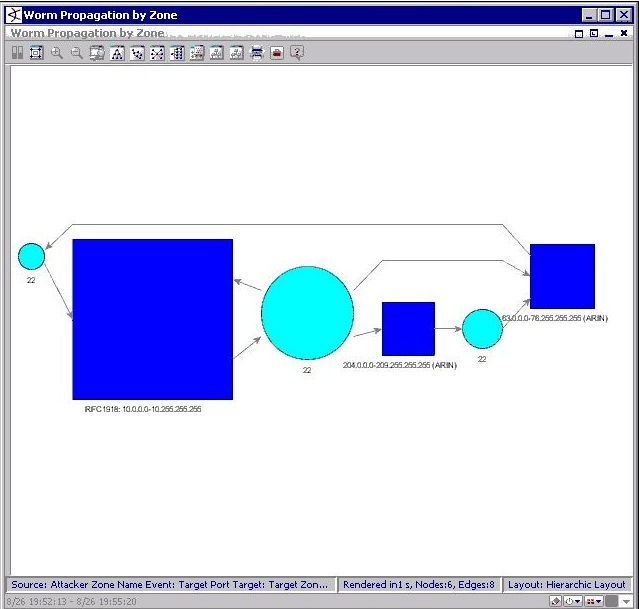
43. What can ArcSight ESM Dashboards display?

**A. multiple Data Monitors**

B. multiple Cases

C. multiple Stages

D. multiple Reports

44. Refer to the Exhibit.  


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

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

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

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

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]

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.

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

A.ELSE

**B. AND**

**C. OR**

D. IF

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

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

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**

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.

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.

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

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

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

A. Cases

**B. Active Channels**

C. Stages

D. Knowledge Base

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**