HP

Exam HP0-A116

HP ArcSight ESM 6.5 Security Administrator and Analyst

Version: 6.0

[Total Questions: 179]

Question No : 1

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

Question No : 2

What is a criteria factor within the ArcSight Priority Formula?

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

Answer: D

Question No : 3

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

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

Answer: C,E

Question No : 4

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

A. Common Conditions Editor
B. Case Editor
C. Notifications Editor
D. Event Annotations

Answer: B

Question No : 5

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

Question No : 6

Which four basic Event Search elements affect what is displayed in the Search results?

A. filter, constraints, time range, and field set
B. filter, constraints, time range, and row limit
C. filter, time range, variables, and field set
D. filter, time range, time zone, and field set

Answer: A

Question No : 7

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

Question No : 8

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

Question No : 9

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

Question No : 10

The Packages view in the ArcSight Console Navigator provides access to all discrete resources that are part of a package in a single view. The dependency view toggle in the Package tree header shows required packages, which are packages on which other packages depend. What is the visual indicator of this dependency?

A. The package name is underlined.
B. The package name is shown in hold font.

C. The package icon contains a red asterisk.
D. The package icon is highlighted in yellow.

Answer: A

Question No : 11

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

Question No : 12

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

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

Answer: D

Question No : 13

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

Question No : 14

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: B

Question No : 15

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

Question No : 16

Which statement is true about the ArcSight Web interface?

A. Inline filters cannot be used from the ArcSight Web interface.
B. Data Monitors cannot be added to a Dashboard from the ArcSightWebinterface.
C. Reports cannot be formatted from the ArcSight Web interface.
D. Cases cannot be modified from the ArcSight Web interface.

Answer: B

Question No : 17

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

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

Answer: D

Question No : 18

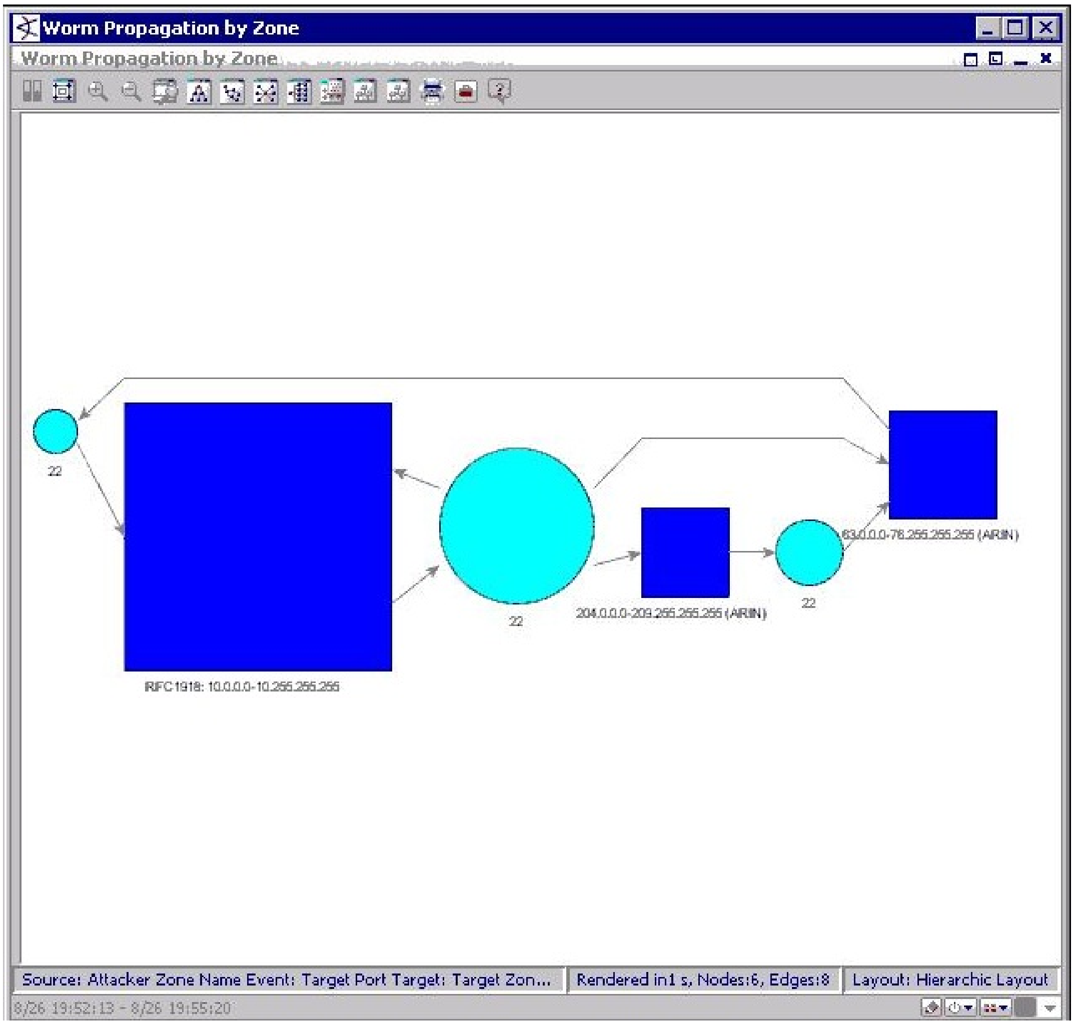
Which three attributes are used to describe an Asset Model?

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

Question No : 19

Click the Exhibit button.



Worm Propagation by Zone

Source: Attacker Zone Name Event: Target Port Target: Target Zon... | Rendered in1 s, Nodes:6, Edges:8 | Layout: Hierarchic Layout

8/26 19:52:13 - 8/26 19:55:20

22
RFC1918: 10.0.0.0-10.255.255.255
22
204.0.0.0-209.255.255.255 (ARIN)
22
63.0.0.0-76.255.255.255 (ARIN)

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

Question No : 20

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

Question No : 21

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

Question No : 22

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

Question No : 23

How are ESM Global Variables created?

A. from within the Manager's server.properties file by using the System Global Variable link
B. from the Fields and Global Variable tab in the Field SetResource or by promoting a Local Variable
C. from the System Tools menu by using the Create System Global Variable option
D. from the Local Variables tab of the Filter Resource and only by promoting a Local Variable

Answer: D

Question No : 24

What can ArcSight ESM Dashboards display?

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

Answer: A

Question No : 25

ESM components fail to consistently restart after a system reboot and require individual intervention with repeated arcsight_services component restart commands. Which log file offers troubleshooting information that will help resolve this issue?

A. monit.log
B. server.log
C. arcsight_services.log
D. server.status.log

Answer: A

Question No : 26

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

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