Free Questions for C1000-162

Shared by Benson on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two (2) options are at the top level when an analyst right-clicks on the Source IP or Destination IP that is associated with an offense at the Offense Summary?

Options:

A- Information

B- DNS Lookup

C- Navigate

D- WHOIS Lookup

E- Asset Summary page

Answer:

B, D

Explanation:

When an analyst right-clicks on the Source IP or Destination IP that is associated with an offense at the Offense Summary in QRadar, two of the top-level options areDNS LookupandWHOIS Lookup1.These options provide additional information about the IP address, such as its domain name (DNS Lookup) and registration information (WHOIS Lookup)1.

Question 2

Question Type: MultipleChoice

What does an analyst need to do before configuring the QRadar Use Case Manager app?

Options:

A- Create a privileged user.

B- Run a QRadar health check.

C- Check the license agreement.

D- Create an authorized service token.

Answer:

D

Explanation:

Before configuring the QRadar Use Case Manager app, it is essential to ensure that the app has the necessary permissions to function correctly. This typically involves creating an authorized service token which provides the app with the permissions to access and manage the QRadar environment.

Question 3

Question Type: MultipleChoice

On the Reports tab in QRadar. what does the message "Queued (position in the queue)" indicate when generating a report?

Options:

A- The report is scheduled to run, and the message is a count-down timer that specifies when the report will run next.

B- The report is ready to be viewed in the Generated Reports column.

C- The report is generating.

D- The report is queued for generation and the message indicates the position of the report in the queue.

Answer:

D

Explanation:

In the Reports tab of QRadar, the message 'Queued (position in the queue)' indicates that the report is queued for generation. The message provides the position of the report within the generation queue, which helps users understand the report's status and expected generation time

Question 4

Question Type: MultipleChoice

How long does QRadar store payload indexes by default?

Options:

A- 7 days

B- 30 days

C- 14 days

D- 90 days

Answer:

B

Explanation:

By default, QRadar stores payload indexes for a duration of 30 days. This retention period is configurable, allowing administrators to adjust how long specific data is retained based on their requirements.

Question 5

Question Type: MultipleChoice

Which two (2) values are valid for the Offense Type field when a search is performed in the My Offenses or All Offenses tabs?

Options:

A- QID

B- Any

C- Risk Score

D- DDoS

E- Source IP

Answer:

B, E

Explanation:

In QRadar, when performing a search in the My Offenses or All Offenses tabs, valid values for the Offense Type field include 'Any' and 'Source IP'. 'Any' searches all offense sources, while 'Source IP' allows for searching offenses with a specific source IP address.

Question 6

Question Type: MultipleChoice

The Pulse app contains which two (2) widget chart types?

Options:

A- Small number chart

B- Hexadecimal chart

C- Binary chart

D- Scatter chart

E- Big number chart

Answer:

D, E

Explanation:

Widget chart types - IBM Documentation

Question 7

Question Type: MultipleChoice

Which of these statements regarding the deletion of a generated content report is true?

Options:

A- Only specific reports that were not generated from the report template as well as the report template are deleted.

B- All reports that were generated from the report template are deleted, but the report template is retained.

C- All reports that were generated from the report template as well as the report template are deleted.

D- Only specific reports that were not generated from the report template are deleted, but the report template is retained.

Answer:

B

Explanation:

When deleting a generated content report in QRadar, all reports that were generated from the report template are deleted, but the report template itself is retained. This ensures that the structure for generating future reports remains intact, while only the instances of reports generated from that template are removed.

Question 8

Question Type: MultipleChoice

A QRadar analyst wants to limit the time period for which an AOL query is evaluated. Which functions and clauses could be used for this?

Options:

A- START, BETWEEN. LAST. NOW. PARSEDATETIME

B- START, STOP. LAST, NOW, PARSEDATETIME

C- START. STOP. BETWEEN, FIRST

D- START, STOP. BETWEEN, LAST

Answer:

B

Explanation:

In QRadar, to limit the time period for which an AQL (Ariel Query Language) query is evaluated, the functions and clauses that can be used include START, STOP, LAST, NOW, and PARSEDATETIME. Specifically, the LAST function is used to define a relative time range

for the query, such as 'LAST 2 DAYS'.

Question 9

Question Type: MultipleChoice

Which two (2) aggregation types ate available for the pie chart in the Pulse app?

Options:

A- Last

B- Total

C- Average

D- First

E- Middle

Answer:

B, C

Explanation:

For pie charts in the Pulse app of QRadar, the available aggregation types include 'Total' and 'Average.' These aggregation types allow for the representation of data in a manner that summarizes the total sum of the data points or their average value, respectively, providing insightful and concise visualizations of the data within the Pulse app dashboards. This information is implied from the general capabilities of dashboard items in QRadar, as detailed in the provided documentation, which typically includes such aggregation options for data visualization.

Question 10

Question Type: MultipleChoice

Which statement regarding saved event search criteria is true?

Options:

A- Saved search criteria expires

B- Saved search criteria does not expire

C- Saved search criteria cannot be reused

D- You cannot define the name of the saved search criteria

Answer:

B

Explanation:

In QRadar, when you save search criteria, especially on the Offenses tab, the configured search criteria are retained for future use and do not expire. This permanence ensures that users can quickly access and reuse their preferred search configurations, thereby streamlining the process of monitoring and investigating offenses over time.

Question 11

Question Type: MultipleChoice

What happens when you select "False Positive" from the right-click menu in the Log Activity tab?

Options:

A- You can tune out events that are known to be false positives.

B- You can investigate an IP address or a user name.

C- Items are filtered that match or do not match the selection.

D- The selected event is filtered based on the selected parameter in the event.

Answer:

A

Explanation:

Selecting 'False Positive' from the right-click menu in the Log Activity tab opens a window that enables users to tune out events that are known to be false positives, preventing them from generating offenses. This feature is crucial for minimizing noise and focusing on genuine threats, thereby enhancing the efficiency of threat detection and response processes within QRadar.

Question 12

Question Type: MultipleChoice

What type of custom property should be used when an analyst wants to combine extraction-based URLs, virus names, and secondary user names into a single property?

Options:

A- AOL-based property

B- Absolution-based property

C- Extraction-based property

D- Calculation-based property

Answer:

A

Explanation:

When an analyst wants to combine multiple extraction and calculation-based properties into a single property, such as URLs, virus names, and secondary user names, an AQL-based property should be used. AQL (Ariel Query Language)-based properties allow for the aggregation of diverse data types into a unified custom property, facilitating more flexible and comprehensive data analysis within QRadar.