Free Questions for C1000-162

Shared by Fitzgerald on 16-04-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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 2

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 3

Question Type: MultipleChoice

Which type of rule should you use to test events or (lows for activities that are greater than or less than a specified range?

Options:

A- Behavioral rules
B- Anomaly rules
C- Custom rules
D- Threshold rules

Answer:

D

Explanation:

Threshold rules in QRadar are designed to test events or flows for activities that are greater than or less than a specified range. These rules are particularly useful for detecting significant changes such as bandwidth usage variations, failed services, changes in the number of connected users, and large outbound data transfers. By setting acceptable limits within threshold rules, administrators can effectively monitor for and respond to abnormal activities within the network.

Question 4

Question Type: MultipleChoice

Offense chaining is based on which field that is specified in the rule?

Options:

A- Rule action field
B- Offense response field
C- Rule response field
D- Offense index field

Answer:

D

Explanation:

Offense chaining in IBM Security QRadar SIEM V7.5 is based on the offense index field specified in the rule. This means that if a rule is configured to use a specific field, such as the source IP address, as the offense index field, there will only be one offense for that specific source IP address while the offense is active. This mechanism is crucial for tracking and managing offenses efficiently within the system.

Question 5

Question Type: MultipleChoice

A Security Analyst was asked to search for an offense on a specific day. The requester was not sore of the time frame, but had Source Host information to use as well as networks involved, Destination IP and username.

Which fitters can the Security Analyst use to search for the information requested?

Options:

A- Offense ID, Source IP, Username

B- Magnitude, Source IP, Destination IP
C- Description, Destination IP. Host Name
D- Specific Interval, Username, Destination IP

Answer:

D

P2P exams