Knowledge check

3 minutes

1. When using KQL to build a query where you want to filter the table to a subset of rows that satisfy the predicate, what function would you use?

- ○ `summarize`
- ◉ `where`

  ✔ **That's right! When you are building a query, it is important to limit the rows you are working with to a specific subset. The `where` command will let you do that.**

- ○ `limit`

2. When constructing queries, you can use a built-in schema reference to obtain information about the contents of the schema. Which built-in schema would you use to obtain the type of data contained in a table and the source of the data?

- ◉ Table description

  ✔ **Correct! This built-in schema provides information on the type of data contain in the table.**

- ○ Columns
- ○ Action types

3. When using a custom detection rule, what is the quota limit applied to every query result set?

- ○ 1,000 rows
- ◉ 10,000 rows

  ✔ **Each query can return up to 10,000 records.**

- ○ 100,000 rows

Next unit: Summary

Continue