Activity: Apply more filters in SQL

Scenario

In this scenario, you're investigating a recent security incident.

You need to gather information about login attempts for certain dates and times. This will help in resolving a security incident.

Here's how you'll do this task: **First**, you'll retrieve login events made after a certain date. **Second**, you'll narrow the focus of the search to filter logins in a date range. **Third**, you'll investigate logins that were made at certain times. **Finally**, you'll filter login attempts based on their event IDs.

Task 1. Retrieve login attempts after a certain date

1. Complete the SQL query to retrieve data for login attempts made **after** '2022-05-09':

```
MariaDB [organization]> SELECT * FROM
    ->
    -> log_in_attempts
    ->
    -> WHERE login_date > '2022-05-09';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168.3.24    |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1 |
|        9 | yappiah  | 2022-05-11 | 13:47:29   | MEX     | 192.168.59.136  |       1 |
```

2. Complete the SQL query to retrieve data for login attempts that were made **on or after** '2022-05-09'.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_date >= '2022-05-09';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168.3.24    |       0 |
```

Task 2. Retrieve logins in a date range

In this task, you need to narrow the focus of the search. Login attempts made after 2022-05-11 shouldn't be included. Use the **BETWEEN and AND** operators to return results between '2022-05-09' and '2022-05-11'.

- Run the query to retrieve the required records.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_date BETWEEN '2022-05-09' AND '2022-05-11';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1 |
```

Task 3. Investigate logins at certain times

1. Write a SQL query to retrieve data for login attempts made **before** '07:00:00'.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_time < '07:00:00';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1 |
```

2. Modify the query to return logins **between** '06:00:00' **and** '07:00:00'.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_time BETWEEN '06:00:00' AND '07:00:00';
+----------+----------+------------+------------+---------+----------------+---------+
| event_id | username | login_date | login_time | country | ip_address     | success |
+----------+----------+------------+------------+---------+----------------+---------+
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.189 |       1 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |       1 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.148 |       0 |
|       71 | mcouliba | 2022-05-09 | 06:57:42   | CAN     | 192.168.55.169  |       0 |
|       98 | gesparza | 2022-05-11 | 06:30:14   | CANADA  | 192.168.148.80  |       0 |
|      106 | tmitchel | 2022-05-12 | 06:15:41   | MEXICO  | 192.168.3.252   |       1 |
|      134 | iuduike  | 2022-05-09 | 06:46:40   | USA     | 192.168.22.115  |       1 |
|      136 | mabadi   | 2022-05-10 | 06:56:44   | US      | 192.168.214.234 |       1 |
|      142 | gesparza | 2022-05-11 | 06:31:14   | CANADA  | 192.168.117.56  |       1 |
|      147 | yappiah  | 2022-05-08 | 06:04:34   | MEX     | 192.168.65.245  |       0 |
|      148 | daquino  | 2022-05-08 | 06:15:55   | CANADA  | 192.168.135.6   |       1 |
|      182 | lyamamot | 2022-05-10 | 06:01:31   | USA     | 192.168.106.52  |       0 |
|      191 | cjackson | 2022-05-08 | 06:46:07   | CANADA  | 192.168.7.187   |       0 |
|      195 | alevitsk | 2022-05-11 | 06:59:13   | CANADA  | 192.168.236.78  |       1 |
+----------+----------+------------+------------+---------+----------------+---------+
15 rows in set (0.001 sec)
```

Task 4. Investigate logins by event ID

1. Write a query to return login attempts with **event_id greater than or equal to** 100.

With this query, you want to **return only the event_id, username, and login_date fields** from the log_in_attempts table.

```
MariaDB [organization]> SELECT event_id, username, login_date
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE event_id >= 100;
+----------+----------+------------+
| event_id | username | login_date |
+----------+----------+------------+
|      100 | tmitchel | 2022-05-12 |
|      101 | sbaelish | 2022-05-08 |
|      102 | jreckley | 2022-05-09 |
|      103 | jhill    | 2022-05-11 |
|      104 | asundara | 2022-05-11 |
```

2. Modify the query to return only login attempts with event_id **between** 100 **and** 150.

```
MariaDB [organization]> SELECT event_id, username, login_date
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE event_id BETWEEN 100 AND 150;
+----------+----------+------------+
| event_id | username | login_date |
+----------+----------+------------+
|      100 | tmitchel | 2022-05-12 |
|      101 | sbaelish | 2022-05-08 |
|      102 | jreckley | 2022-05-09 |
|      103 | jhill    | 2022-05-11 |
|      104 | asundara | 2022-05-11 |
```