# Time Based Filters in SQL

## Project description

This simulation project puts the performer, **Maheswar Reddy Avula**, into the position of a system administrator for an organization. Responsibilities include investigating a recent security incident by gathering information about login attempts for certain dates and times.

(For readability and simplicity, the outputs have been limited to 5 table entries out of 200)

## Retrieve login attempts after a certain date

**Direction:** The administrator must investigate a recent security incident by gathering information about login attempts made after **2022-05-09**. Then expand the search range to include **2022-05-09** as well.

Using the **where** clause with the **> (greater than)** operator the following query was run to display the required result:

```
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
 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1
 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |       0
 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |       1
 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.137  |       1
```

Replacing the **>** operator with the **>=(greater than or equal to)** operator, the following query is run to get desired outcome:

```
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
 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |       1
```

## Retrieve logins in a date range

**Direction:** The administrator must narrow the focus of the search by excluding the login attempts made after **2022-05-11.**

Using the **where** clause with the **between** operator on dates **‘2022-05-09’** and ’2022-05-11’, the following query was run to display the required result:

```
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
```

## Investigating logins at certain times

**Direction:** The admin must investigate logins made before **7:00:00** in the aforementioned date range. Then narrow down the search results to the time

range between **06:00:00** to **07:00:00**. The required results were displayed using **< (less than)** operator to specify time before **07:00:00** as follows:

```
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
 |
```

The required results were displayed using **between** and **and** operators specified from **06:00:00** to **07:00:00** as follows:

```
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
```

## Investigating logins by event ID

**Direction:** The admin must now investigate login attempts based on **event_id** numbers greater than or equal to **100**. The search space must then be expanded to the range **100** to **150.**

Using the **where** clause with the **>= (greater than or equal to)** operator the following query was run to display the required result:

```
MariaDB [organization]> select event_id, username, login_date from log_in_attempts wh
ere 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 |
|      105 | cjackson | 2022-05-12 |
```

To include the **100** to **150** range, the >= operator was replaced with the **between** operator to display result as follows:

```
MariaDB [organization]> select event_id, username, login_date from log_in_attempts wh
ere event_id between 100 and 200;
+----------+----------+------------+
| 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 |
|      105 | cjackson | 2022-05-12 |
|      106 | tmitchel | 2022-05-12 |
```

## Summary

The investigatory data was retrieved and provided to the organization. All tasks were successfully completed in accordance with the directions given by the organization.