Filtering dates and times in SQL

Introduction

As a security analyst I had to filter through dates to see what devices needed the latest updates, to increase security. Also, I had to check login attempt counts, to determine whether there's been malicious activity in the system.

Objectives

1) Filter for login attempts made after a certain date
2) Filter for login attempts made in a certain date range
3) Filter for login attempts made at a certain time
4) Filter for login attempts by ID

Filter for login attempts made after a certain date

In this task I had to filter login attempts before 7am in response to a recent security event.

```
MariaDB [organization]> SELECT * FROM log_in_attempts  WHERE login_time < '07:00:00' ORDER BY login_time;
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|      110 | mabadi   | 2022-05-09 | 00:01:54   | USA     | 192.168.90.124  |       1 |
|      177 | wjaffrey | 2022-05-11 | 00:15:55   | USA     | 192.168.144.165 |       0 |
|      175 | jhill    | 2022-05-10 | 00:17:09   | USA     | 192.168.130.218 |       0 |
|      117 | bsand    | 2022-05-08 | 00:19:11   | USA     | 192.168.197.187 |       0 |
|      143 | jhill    | 2022-05-11 | 00:30:22   | USA     | 192.168.189.19  |       0 |
|       92 | pwashing | 2022-05-08 | 00:36:12   | US      | 192.168.247.219 |       0 |
|      187 | arusso   | 2022-05-09 | 00:36:26   | MEX     | 192.168.77.137  |       0 |
```

Filter for login attempts made in a certain date range

Expanding on my query above I decided to narrow my search down to logs between 6am and 7am.

```
MariaDB [organization]> SELECT * FROM log_in_attempts
    -> WHERE login_time BETWEEN '06:00:00' AND '07:00:00' ORDER BY login_time;
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|      182 | lyamamot | 2022-05-10 | 06:01:31   | USA     | 192.168.106.52  |       0 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.148 |       0 |
|      147 | yappiah  | 2022-05-08 | 06:04:34   | MEX     | 192.168.65.245  |       0 |
|      106 | tmitchel | 2022-05-12 | 06:15:41   | MEXICO  | 192.168.3.252   |       1 |
|      148 | daquino  | 2022-05-08 | 06:15:55   | CANADA  | 192.168.135.6   |       1 |
|       98 | qesparza | 2022-05-11 | 06:30:14   | CANADA  | 192.168.148.80  |       0 |
```

Filter for login attempts made at a certain time

In this query I looked at logs made at a specific time.

```
MariaDB [organization]> SELECT * FROM log_in_attempts  WHERE login_time < '07:00:00' ORDER BY login_time;
+----------+----------+------------+------------+---------+----------------+---------+
| event_id | username | login_date | login_time | country | ip_address     | success |
+----------+----------+------------+------------+---------+----------------+---------+
|      110 | mabadi   | 2022-05-09 | 00:01:54   | USA     | 192.168.90.124 |       1 |
|      177 | wjaffrey | 2022-05-11 | 00:15:55   | USA     | 192.168.144.165 |       0 |
|      175 | jhill    | 2022-05-10 | 00:17:09   | USA     | 192.168.130.218 |       0 |
|      117 | bsand    | 2022-05-08 | 00:19:11   | USA     | 192.168.197.187 |       0 |
|      143 | jhill    | 2022-05-11 | 00:30:22   | USA     | 192.168.189.19  |       0 |
|       92 | pwashing | 2022-05-08 | 00:36:12   | US      | 192.168.247.219 |       0 |
|      187 | arusso   | 2022-05-09 | 00:36:26   | MEX     | 192.168.77.137  |       0 |
```

Filter for login attempts by ID

Lastly, I decided to check the event IDs to gain a clearer understanding on users making these login attempts before normal working hours.

```
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 |
|      105 | cjackson | 2022-05-12 |
```