# Sample Simple SQL Queries

Stephen Langford
2/18/25

## Project description

You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines.

Your task is to examine the organization's data in their employees and log_in_attempts tables. You'll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

## Retrieve after hours failed login attempts

You recently discovered a potential security incident that occurred after business hours. To investigate this, you need to query the log_in_attempts table and review after hours login activity. Use filters in SQL to create a query that identifies all failed login attempts that occurred after 18:00. (The time of the login attempt is found in the login_time column. The success column contains a value of 0 when a login attempt failed; you can use either a value of 0 or FALSE in your query to identify failed login attempts.)

```
MariaDB [organization]> SELECT * FROM log_in_attempts WHERE login_time > '
18:00' AND success = 0 ORDER BY username, login_date, login_time;
+----------+----------+------------+------------+---------+--------------
--+---------+
| event_id | username | login_date | login_time | country | ip_address
  | success |
+----------+----------+------------+------------+---------+--------------
--+---------+
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122
  |       0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX     | 192.168.234.49
  |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57
  |       0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.168.76.27
  |       0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.168.132.15
3 |       0 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12
  |       0 |
```

## Retrieve login attempts on specific dates

Your team is investigating a suspicious event that occurred on `'2022-05-09'`. You want to retrieve all login attempts that occurred on this day and the day before (`'2022-05-08'`).

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
+----------+----------+------------+------------+---------+---------------
--+---------+
| event_id | username | login_date | login_time | country | ip_address
  | success |
+----------+----------+------------+------------+---------+---------------
--+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.14
0 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.16
2 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71
  |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.17
3 |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.15
8 |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51
  |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.19
2 |       1 |
```

## Retrieve login attempts outside of Mexico

There's been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. Now, you need to investigate login attempts that occurred outside of Mexico. Use filters in SQL to create a query that identifies all login attempts that occurred outside of Mexico.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+---------------
--+---------+
| event_id | username | login_date | login_time | country | ip_address
  | success |
+----------+----------+------------+------------+---------+---------------
--+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.14
0 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12
  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.16
2 |       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     | 192.168.170.24
3 |       1 |
```

## Retrieve employees in Marketing

Your team is updating employee machines, and you need to obtain the information about employees in the `'Marketing'` department who are located in all offices in the East building (such as `'East-170'` or `'East-320'`).

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE office = 'East-170' OR office = 'East-320';
+-------------+-------------+----------+-----------------------+---------
-+
| employee_id | device_id    | username | department             | office
 |
+-------------+-------------+----------+-----------------------+---------
-+
|        1000 | a320b137c219 | elarson  | Marketing              | East-170
 |
|        1006 | g329h357i597 | alevitsk | Information Technology | East-320
 |
+-------------+-------------+----------+-----------------------+---------
-+
2 rows in set (0.001 sec)
```