Apply filters to SQL queries

Project description

As the security analyst of my organization, I recently discovered a potential security incident that occurred after business hours. To further investigate this issue, I decided to query the `log_in_attempts` table using SQL to review after-hours login activity. Additionally, I queried the `employees` table to update employee computers as required.

Retrieve after hours failed login attempts

I used this query to filter out failed login attempts from `log_in_attempts` that were made after business hours (after 18:00).

```
SELECT * FROM log_in_attempts WHERE login_time > '18:00' AND success = 'FALSE';
```

```
MariaDB [organization]> SELECT * FROM log_in_attempts WHERE login_time
 > '18:00' AND success = 'FALSE';
+----------+----------+------------+------------+---------+-----------
------+---------+
| event_id | username | login_date | login_time | country | ip_address
     | success |
+----------+----------+------------+------------+---------+-----------
------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.20
5.12  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66
.142  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.10
9.50  |       0 |
```

Retrieve login attempts on specific dates

I used this query to find login attempts that were made on 2022-05-09 or on 2022-05-08 since a suspicious event happened on 2022-05-09.

```
SELECT * FROM log_in_attempts WHERE login_date = '2022-05-09' OR login_date = '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     | 192.168.24
3.140 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.15
1.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.17
8.71  |       0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.11
```

Retrieve login attempts outside of Mexico

All login attempts that occurred outside of Mexico need to be investigated.

I used this query to find the login attempts where the country is not Mexico.

```
SELECT * FROM log_in_attempts WHERE NOT country LIKE 'MEX%';
```

```
MariaDB [organization]> SELECT * FROM log_in_attempts WHERE NOT countr
y LIKE 'MEX%';
+----------+----------+------------+------------+---------+-----------
------+---------+
| event_id | username | login_date | login_time | country | ip_address
     | success |
+----------+----------+------------+------------+---------+-----------
------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.24
3.140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.20
5.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.15
1.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.17
8.71  |       0 |
```

Retrieve employees in Marketing

My company wants to update the computers for employees in the Marketing department.

I used this query to filter out employees who is in marketing department and their office is in East building.

```
SELECT * FROM employees WHERE department = 'Marketing' AND office LIKE 'East%';
```

```
MariaDB [organization]> SELECT * FROM employees WHERE department = 'Marketing' AND office LIKE 'East%';
+-------------+--------------+----------+------------+----------+
| employee_id | device_id    | username | department | office   |
+-------------+--------------+----------+------------+----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
|        1088 | k8651965m233 | rgosh    | Marketing  | East-157 |
|        1103 | NULL         | randerss | Marketing  | East-460 |
|        1156 | a184b775c707 | dellery  | Marketing  | East-417 |
|        1163 | h679i515j339 | cwilliam | Marketing  | East-216 |
+-------------+--------------+----------+------------+----------+
```

Retrieve employees in Finance or Sales

Computers for employees in the Finance and Sales departments also need to be updated.
I used this query to find employees who is in the Finance department or in the Sales department.

```
SELECT * FROM employees WHERE department = 'Finance' OR department = 'Sales';
```

```
MariaDB [organization]> SELECT * FROM employees WHERE department = 'Finance' OR department = 'Sales';
+-------------+--------------+----------+------------+-------------+
| employee_id | device_id    | username | department | office      |
+-------------+--------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
|        1009 | NULL         | lrodriqu | Sales      | South-134   |
|        1010 | k2421212m542 | jlansky  | Finance    | South-109   |
```

Retrieve all employees not in IT

My company needs to make a security update on employees who are not in the IT department.
I used this query to find employees who is not in the IT department.

```
SELECT * FROM employees WHERE NOT department = 'Information Technology';
```

```
MariaDB [organization]> SELECT * FROM employees WHERE NOT department =
 'Information Technology';
+-------------+-------------+----------+----------------+-----------
--+
| employee_id | device_id    | username | department      | office
  |
+-------------+-------------+----------+----------------+-----------
--+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170
  |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-27
6 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-434
  |
|        1003 | d394e816f943 | sgilmore | Finance         | South-153
  |
|        1004 | e218f877g788 | eraab    | Human Resources | South-127
  |
|        1005 | f551g340h864 | gesparza | Human Resources | South-366
  |
|        1007 | h174i497j413 | wjaffrey | Finance         | North-406
```

Summary

Using SQL to query data is a very efficient way to filter out the information we need, whether it's for investigating a security incident or gathering employee information to update their computers. In this project, I used the operators `AND`, `OR`, and `NOT` to filter the necessary information for each task. I also used `LIKE` and the wildcard `%` to filter for patterns.