Apply filters to SQL queries

Project description

My organisation wants to make our security stronger. It is my duty to investigate any potential security and make sure that the systems of all employees are safe and uptodate.
This document summarizes how SQL can be used to perform security related tasks.

Retrieve after hours failed login attempts

Recently a potential security incident occurred where several login attempts were made after the office working hours(18:00).
All the failed login attempts made after 18:00 need to be investigated.
Following are the SQL queries I used to make filter all failed login attempts made after office working hours:

```
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     | 192.168.205.12  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |       0 |
```

The first part in the image is the query i made to retrieve relevant login attempts and the second part shows the output of the query.
The query I made filters all the login attempts from the `log_in_attemps` table where the `login_time` was greater(after) `18:00` that failed as indicated by the second condition `success = FALSE` indicated by `0` in the output.

Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09 so all the login attempts made on that day or the day before need to be investigated.
The following image shows the SQL query I created to filter out the date based on specific dates:

```
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     | 192.168.243.140 |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       0 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
```

The first part shows the query I made and the second part shows the output of the query. The query starts by selecting all data from the `log_in_attempts` table, Then made conditions with the `WHERE` clause here i used the `OR` operator with the two conditions I made OR make sure that one of the given condition is TRUE so here it will filter data with `login_date = 2022-05-08` which filters for logins on '2022-05-08' `OR login_date = 2022-05-09` which filters for login attempts on '2022-05-08'.

Retrieve login attempts outside of Mexico

After investigating the organization data on login attempts i believe the issue is with login attempts outside Mexico. These login attempts should be investigated.
The following image shows the query i made to filter all the login attempts made outside 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     | 192.168.243.140 |       0 |
|        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 |       0 |
```

The first part of the screenshots shows the query I made and the second part shows the output of the query with all the login attempts outside Mexico. First I selected all the data from the `log_in_attempts` table . Then I used the `WHERE` clause with the `NOT` operator which returns data excluding the given condition which in this case I combined it with the `LIKE` operator with `'MEX%'` to filter the data set representing Mexico as 'MEX' and 'MEXICO'. The `%` acts as a wildcard (unspecified) character when used with the LIKE operator.

Retrieve employees in Marketing

My team wants to perform security updates on specific employees in the Marketing department. For this i have to get information of the employees that work in the Marketing department.
The following image shows how i created the SQL query to get fitter data to get information on the employees that are working in Marketing department from the east building:

```
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 |
```

The first part of the screenshot shows the query I made and the second part shows the output of the query.
First i selected all the data from the `employees` table then I applied the `WHERE` clause it has two conditions first it will filter based on the department where `department = 'Marketing'` , and the second condition joined by the AND operator I combined it with the `LIKE` operator with office value `LIKE 'East%'` which will filter and give all the employees that work in the east building.

Retrieve employees in Finance or Sales

Now my team wants to update the machines of all the employees in the Sales and Finance department.For this I have to get the information of all the employees that work in these specific departments with the help of SQL queries.
The following image shows how i created the SQL query to get filter data to get information on the employees that are working in Sales and Finance department:

```
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   |
```

The first part of the screenshot shows the query I made and the second part shows the output of my query.
First I started by selecting all the data from the employees table. Then I used the WHERE clause with the OR operator to select only those employees who are in the Sales and Finance department. I used OR operator instead of AND operator as I wanted employees who work in either department so it should return even if one of the conditions is not met. The first condition department = 'Finance' filter for employees that work in the finance department. The second condition department = 'Sales' filter for employees that work in the sales department.

Retrieve all employees not in IT

My team needs to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it. For that i first need to get information of these employees.
The following image shows how i created the SQL query to get filter data to get information on the employees that are not in IT department:

```
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-276 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-434   |
```

The first part of the screenshot shows the query I made and the second part shows the output of my query.

First I started by selecting all the data from the employees table. Then I applied the WHERE clause with NOT operator the condition NOT department = ‘Information Technology’ selects all the employees that are not in the IT department.

Summary

I applied many SQL queries to filter the login attempts and employee machines.
I used queries to filter data from two different tables log_in_attemps and employees. I used different operators like AND, OR, NOT, to make sure that I can get precise data for my team to use. I also use the LIKE operator to filter data with (%) wildcards based on string patterns.