# Apply filters to SQL queries

## Project description

## My role involves enhancing the security of our organization's systems, proactively identifying and addressing potential security vulnerabilities, and ensuring that employee computers are updated and secure.

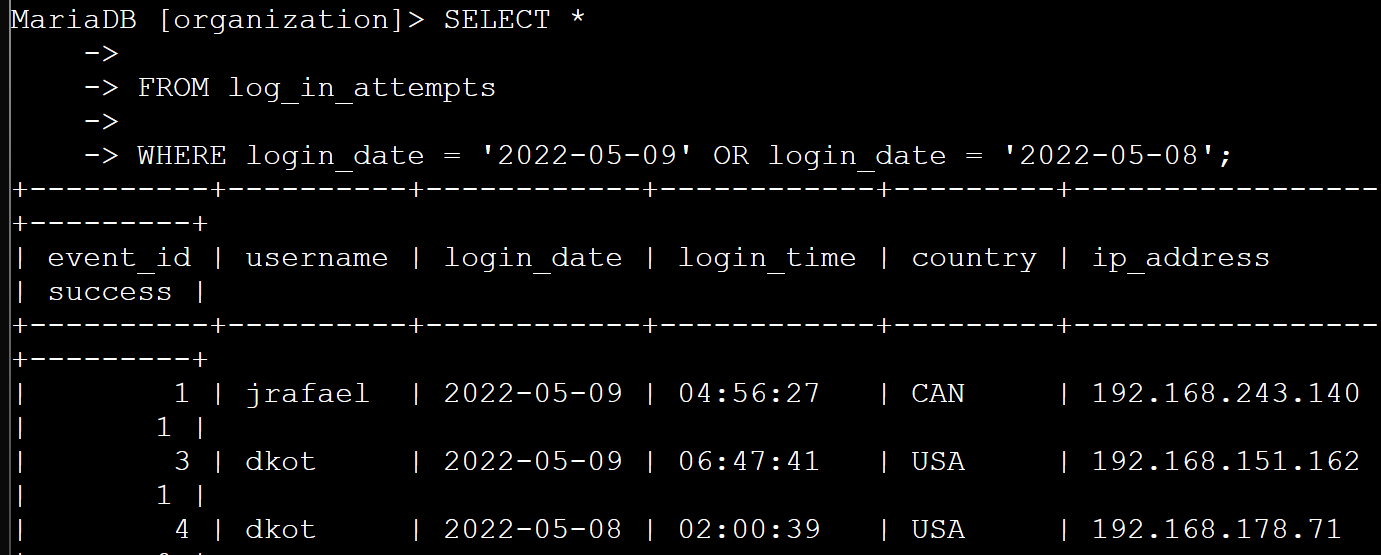
## Retrieve after hours failed login attempts

There was a potential security incident involving failed login attempts that occurred after business hours (after 18:00). To investigate, I wrote a SQL query to identify these incidents.

The query is designed to filter for failed login attempts that occurred after 18:00. To achieve this, I started by selecting all data from the log\_in\_attempts table. Then, I applied a WHERE clause combined with an AND operator to narrow down the results. The first condition, login\_time > '18:00', captures login attempts made after 18:00. The second condition, success = FALSE, filters for those attempts that were unsuccessful.

## Retrieve login attempts on specific dates

A suspicious event was detected on 2022-05-09. To ensure a thorough investigation, it's essential to review all login activity that took place on 2022-05-09 and the day before.



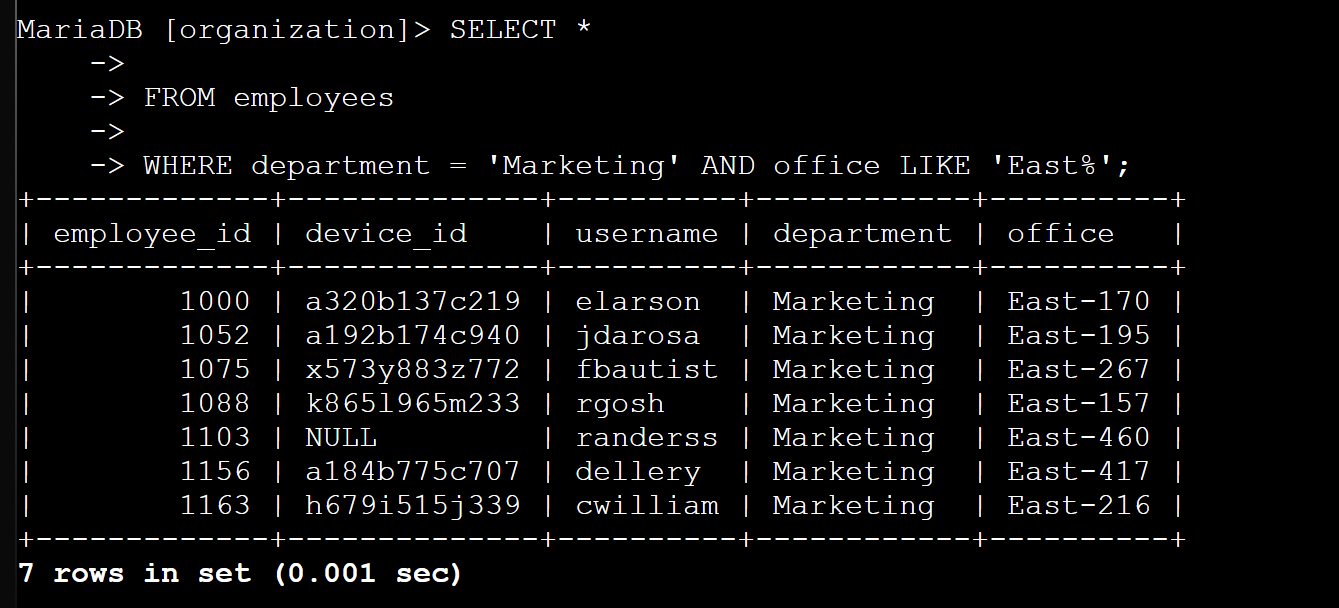
## Retrieve login attempts outside of Mexico

After reviewing the organization's data on login attempts, I've identified potential issues with logins originating from outside of Mexico. Below is an screenshot of a SQL query to filter for login attempts that occurred outside of Mexico.

## Retrieve employees in Marketing

Here's how I created a SQL query to identify employees in the Marketing department located in the East building.

The query filters for employees in the Marketing department (department = 'Marketing') and in the East building (office LIKE 'East%'). This ensures that only those relevant employees are returned from the employees table.



## Retrieve employees in Finance or Sales

Here’s how I created a SQL query to filter for employee machines in the Finance or Sales departments.

The query is designed to return only employees in the Finance or Sales departments. I used a WHERE clause with an OR condition, filtering the results to include only those in the Finance (department = 'Finance') or Sales (department = 'Sales') departments. This query ensures that only the relevant employee machines are identified for the security update.

## Retrieve all employees not in IT

My team needs to execute a final security update for employees not in the Information Technology department. To facilitate this, I need to collect data on these employees.

Here’s how I formulated a SQL query to identify employees outside the Information Technology department.

The query retrieves all employees who do not belong to the Information Technology department. I began by selecting all records from the `employees` table and then applied a `WHERE` clause with the `NOT` operator to exclude those in the Information Technology department, ensuring that the results include only employees from other departments.

## Summary

I used SQL filters in order to get specific information on employees and login attempts. I used two tables that had the data of employees and the login logs. I used AND, OR, NOT operators to search for specific information. I also used LIKE and % to search for relevant informations, filtering for patters.