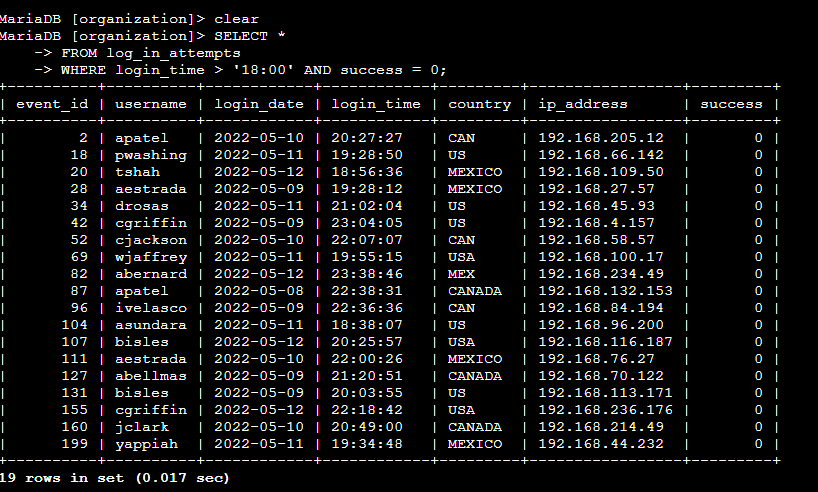
# Apply filters to SQL queries

## Project description

This project was done to obtain specific information about employees, their machines and the departments they belong to from the database. The data gathered is used to investigate potential security issues and to update computers.

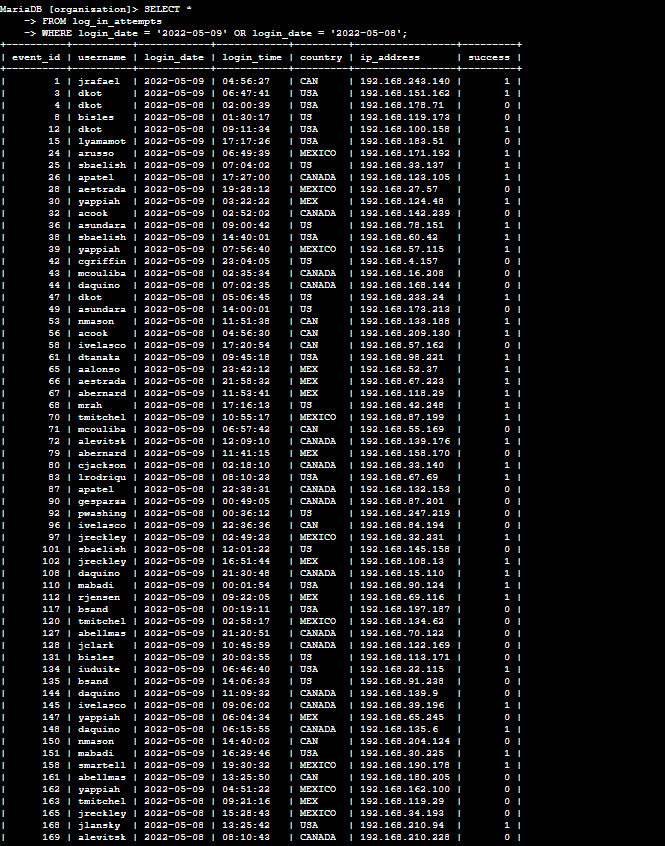
## Retrieve after hours failed login attempts

A possible security incident was recently found to have happened outside of regular business hours. I used a SQL query to retrieve all unsuccessful after-hours login attempts in order to look into this. 

The SQL query used to select all columns from the log\_in\_attempts table where the login\_time and login success values were after hours and false is shown in the first three lines of the screenshot above. The subsequent results showed 19 rows of unsuccessful after-hours login attempts together with the associated information, including the requester's IP address, the country from which the attempt originated, and the identity of the attempter.

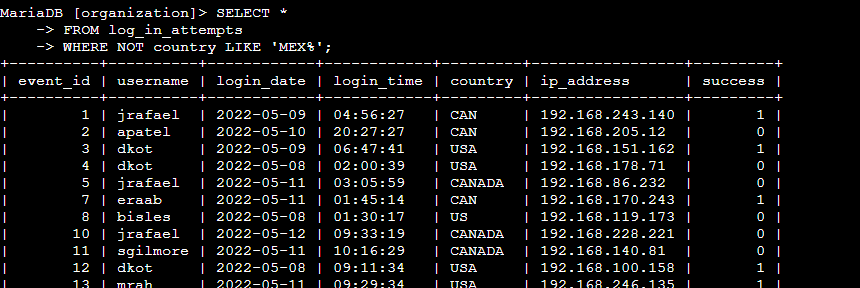
## Retrieve login attempts on specific dates

As part of the investigation into the suspicious activity on *2022-05-09*, we are retrieving all login attempts from *2022-05-08* and *2022-05-09* to identify any relevant patterns or anomalies.



I used SQL's OR operator in the query above to select every column from the log\_in\_attempts table and filter the results to only include attempts that happened on 2022-05-09 and 2022-05-08.

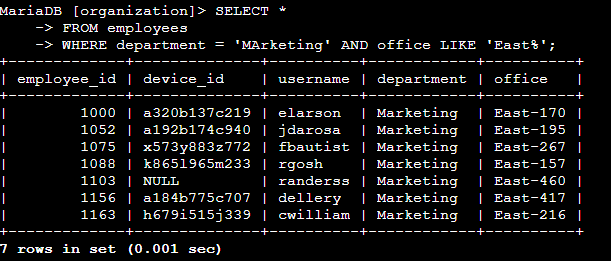
## Retrieve login attempts outside of Mexico

Suspicious login activity was also detected from countries other than Mexico. I used SQL to filter and retrieve all login attempts that originated outside of Mexico.

To find every login attempt that didn't come from Mexico, I combined the LIKE operator, the % wildcard, and SQL's NOT operator. Since "MEX" or "MEXICO" are possible alternatives in the country field, I used the wildcard pattern "MEX%" to match any value that begins with "MEX." I was able to extract only the logins from other nations by using NOT LIKE 'MEX%', which excluded all such entries.

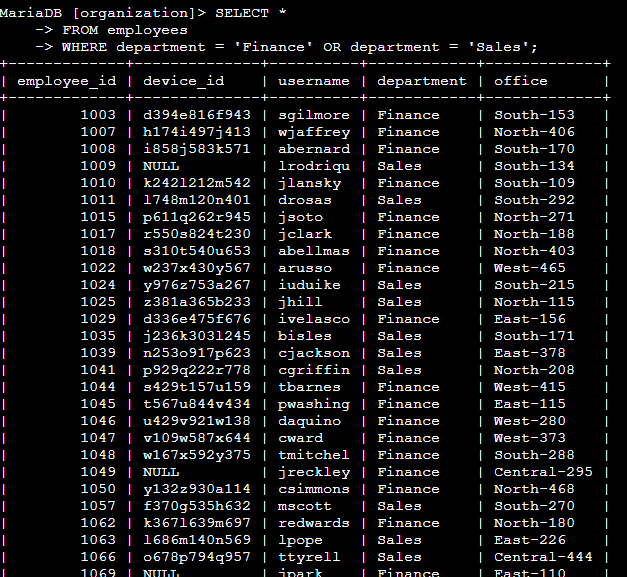
## Retrieve employees in Marketing

The marketing department's specific personnel computers were the target of security updates from the security team. I had to ask every member of the marketing team who worked in every office in the east building.



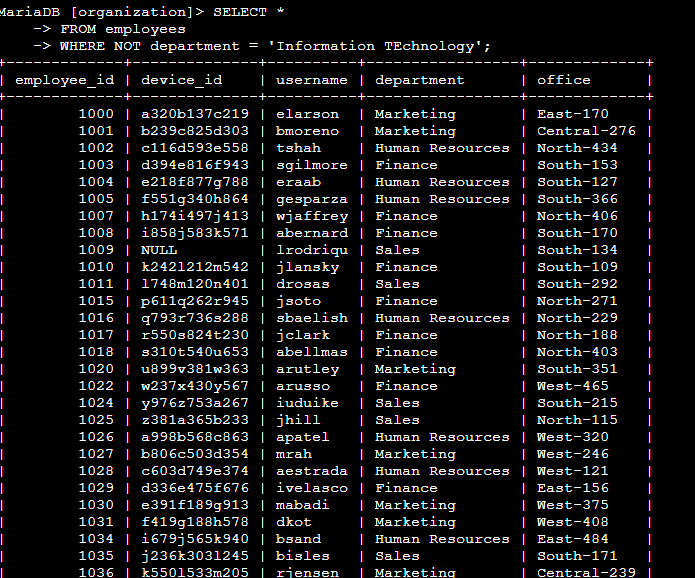
I filtered the personnel table using SQL's AND and LIKE operators to locate every employee in the east office building who was assigned to the "Marketing" department. I once more used the % operator to look for values in the office column that start with "East," since the office building may have a wide range of numbers, such "East-170" or "East-460."

## Retrieve employees in Finance or Sales

Different security updates were required for machines used by staff members in the finance and sales departments. To locate every person in these departments, I used SQL to filter the employee table. I filtered the department field in the above query for every employee in the Finance or Sales departments using SQL's OR operator.

## Retrieve all employees not in IT

A new security upgrade was already available to IT staff, but it was required for the other departments to acquire it as well. To locate every employee and system that wasn't related to IT, I used SQL. Making use of the



To identify all rows where the department is not "Information Technology," I use the NOT operator to filter the department column.

## Summary

I gave my security team comprehensive reports on employee behavior and login events pertaining to questionable login attempts and system security updates by utilizing SQL queries. In order to separate login attempts on specific dates, from specific countries, unsuccessful logins, and people from targeted departments, I effectively filtered through thousands of entries using SQL operators like AND, NOT, LIKE, and %. This experiment showed how SQL allowed me to find important information in a fraction of the time it would have taken to do a manual search.