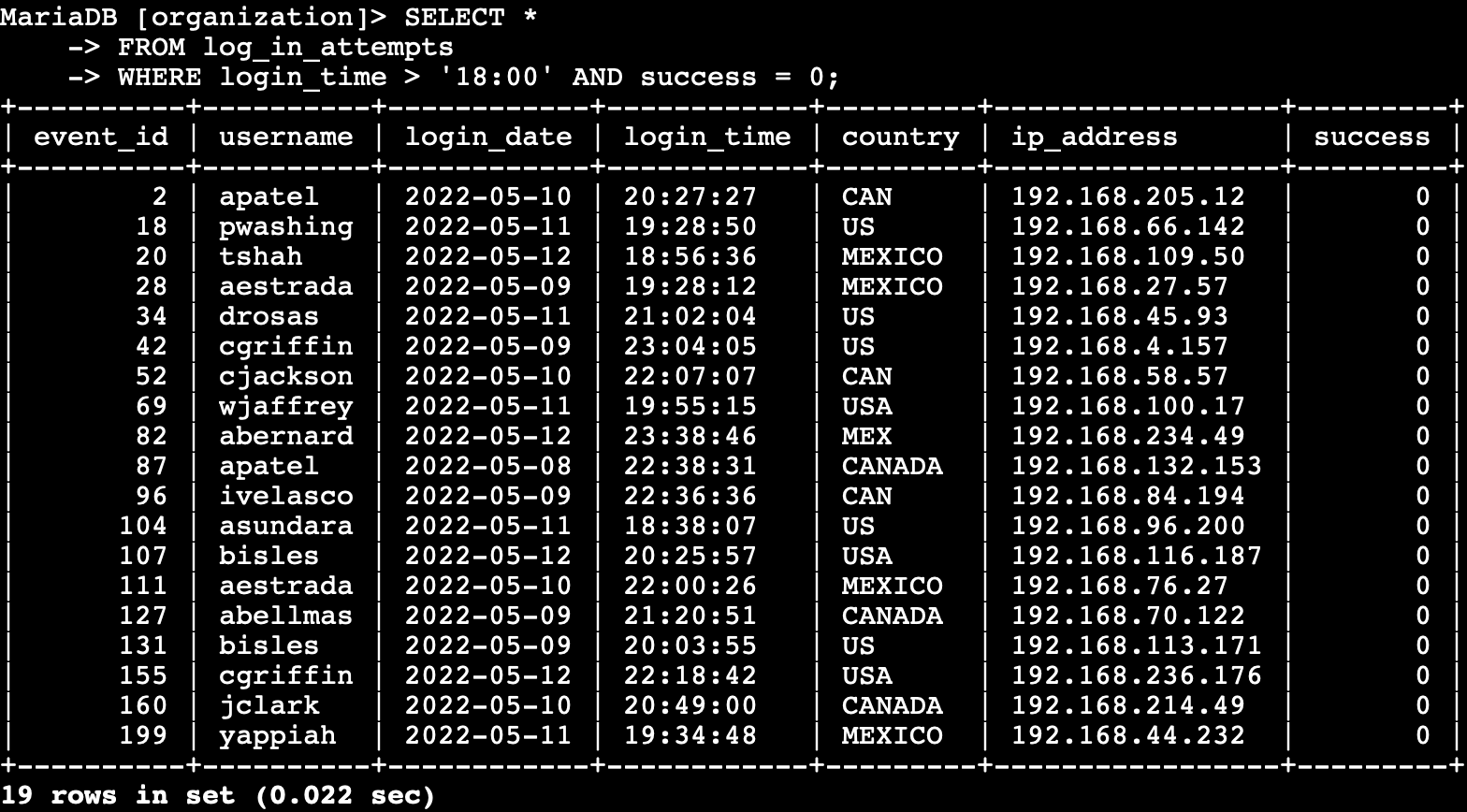
# Apply filters to SQL queries

## Project description

As a security professional my organization has tasked me with investigating potential security issues involving login attempts and employee machines. To ensure the system is secure I will need to use SQL filters to retrieve records from different datasets and investigate the potential security concerns.

## Retrieve after hours failed login attempts

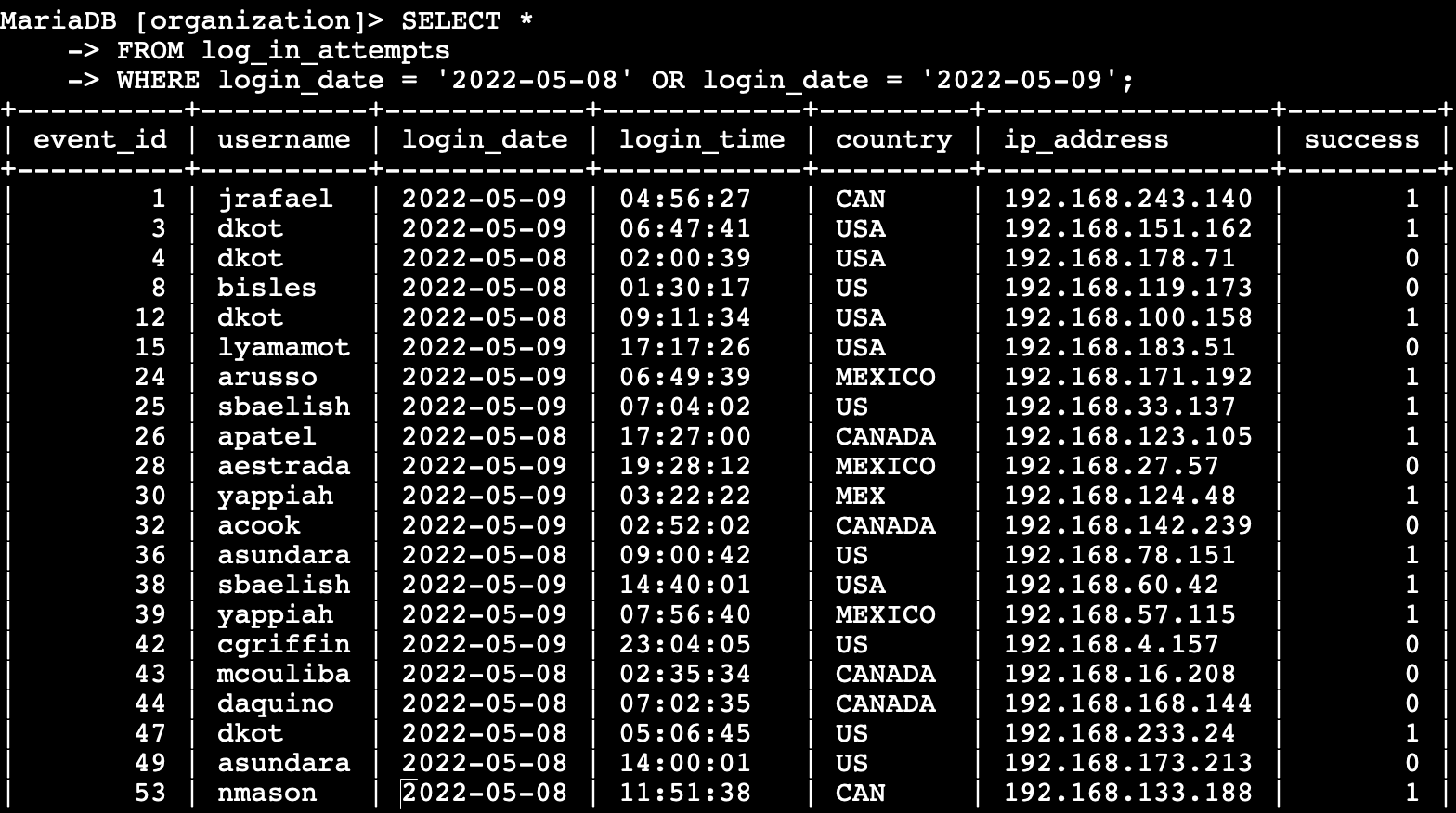
I discovered a potential security incident that occurred after business hours. To investigate this, I wrote a SQL query to show all failed login attempts that occurred after normal business hours (6:00pm).



Using \*, the query returns all login attempts from the log\_in\_attempts table. Then with the conditional WHERE it filters to those made after 6:00pm and only attempts that failed, which is represented by a value of 0 in the success column.

## Retrieve login attempts on specific dates

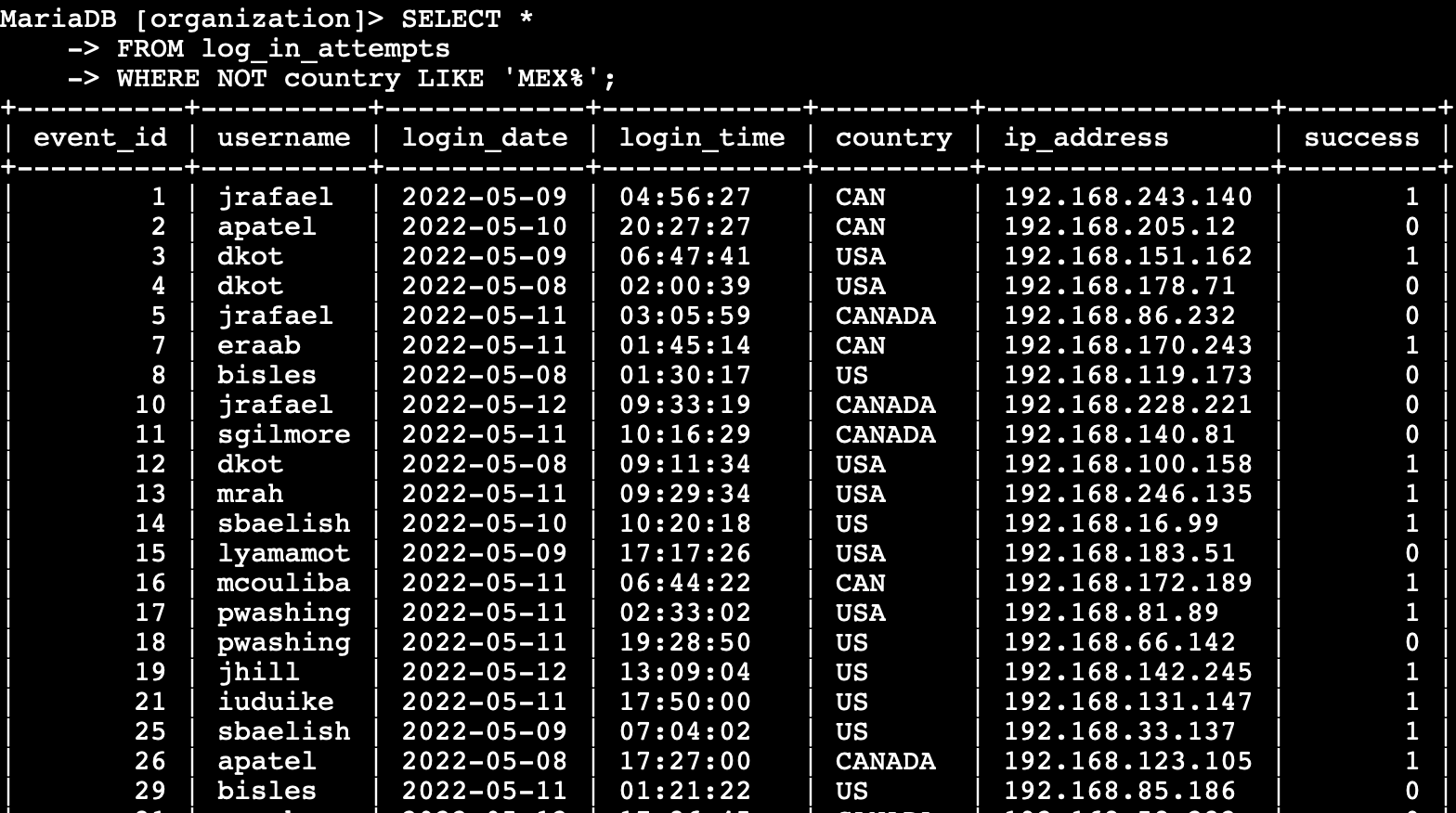
A suspicious event occurred on 2022-05-09, to investigate the event I reviewed all events on this day and the day before.



I again SELECT all using \* from the log\_in\_attempts table and using the WHERE conditional filter the display attempts made the day of the event or the day before. The OR conditional means it will show results that meet either date.

## Retrieve login attempts outside of Mexico

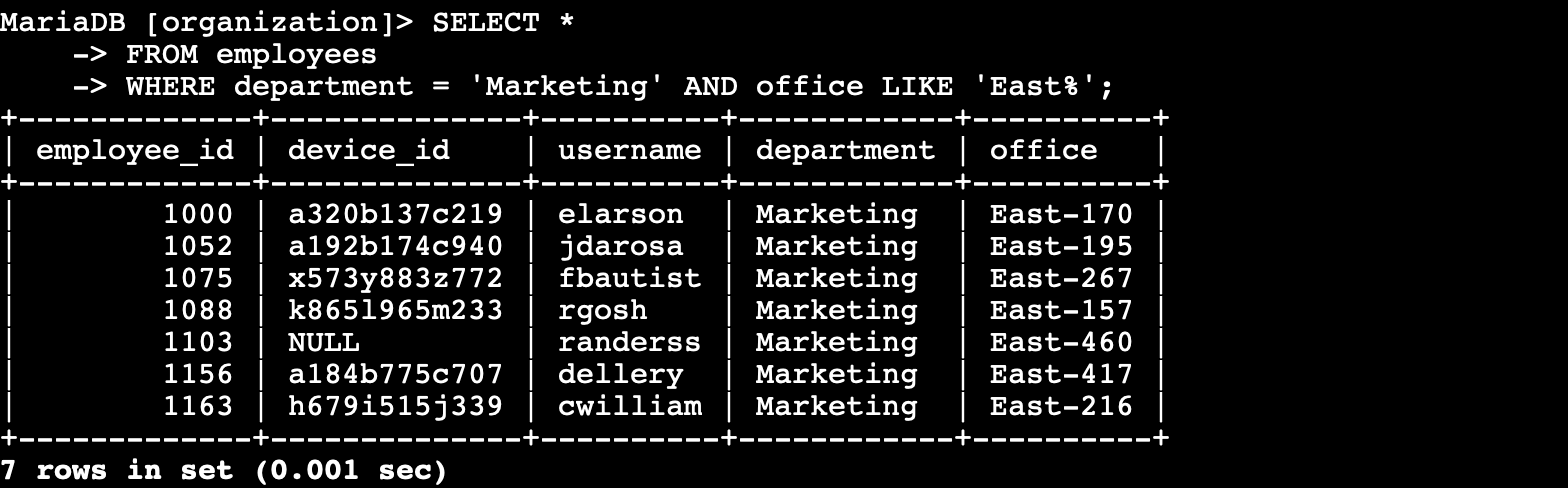
The team determines there have been suspicious login attempts made but it’s known they did not originate from Mexico. I investigate all login attempts that occurred outside of Mexico.



In this SQL filter I used the NOT conditional to clarify I wanted to display all results not matching Mexico. Using LIKE with the % after MEX ensures it will show results including MEX and any variation with letters after like MEXICO.

## Retrieve employees in Marketing

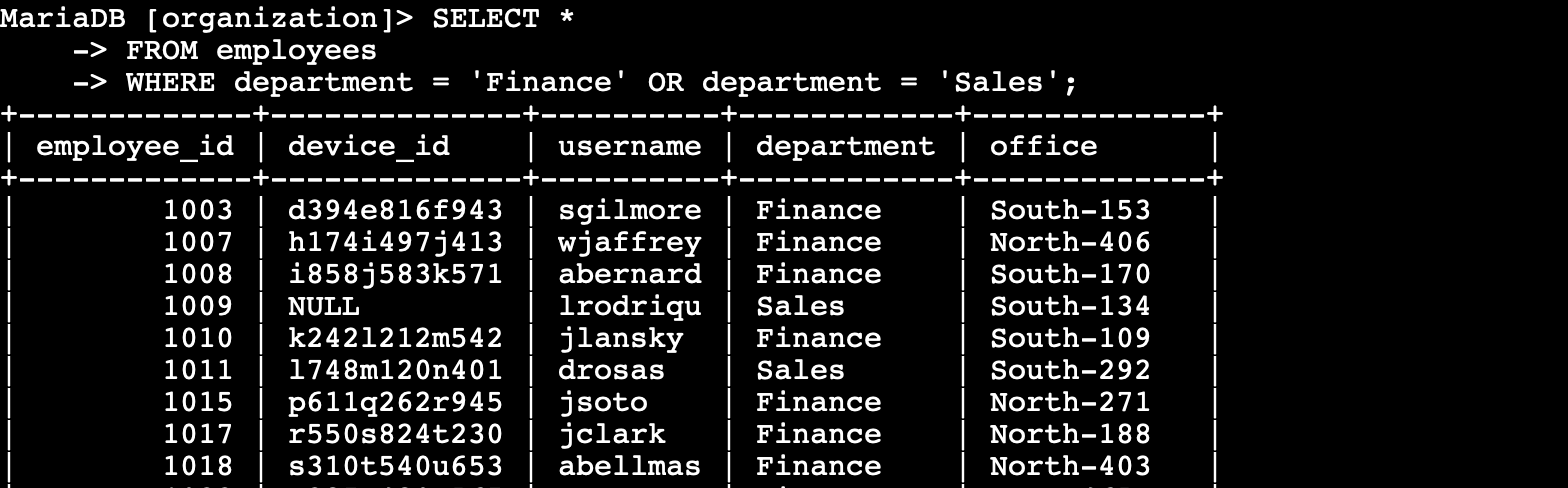
The team wants to perform security updates on specific employee machines in the Marketing department. I am responsible for getting information on these employee machines and will need to query the employees table.



I used a SQL query to select all employees whose department is Marketing and whose office starts with East using the WHERE, AND, and LIKE conditionals to filter.

## Retrieve employees in Finance or Sales

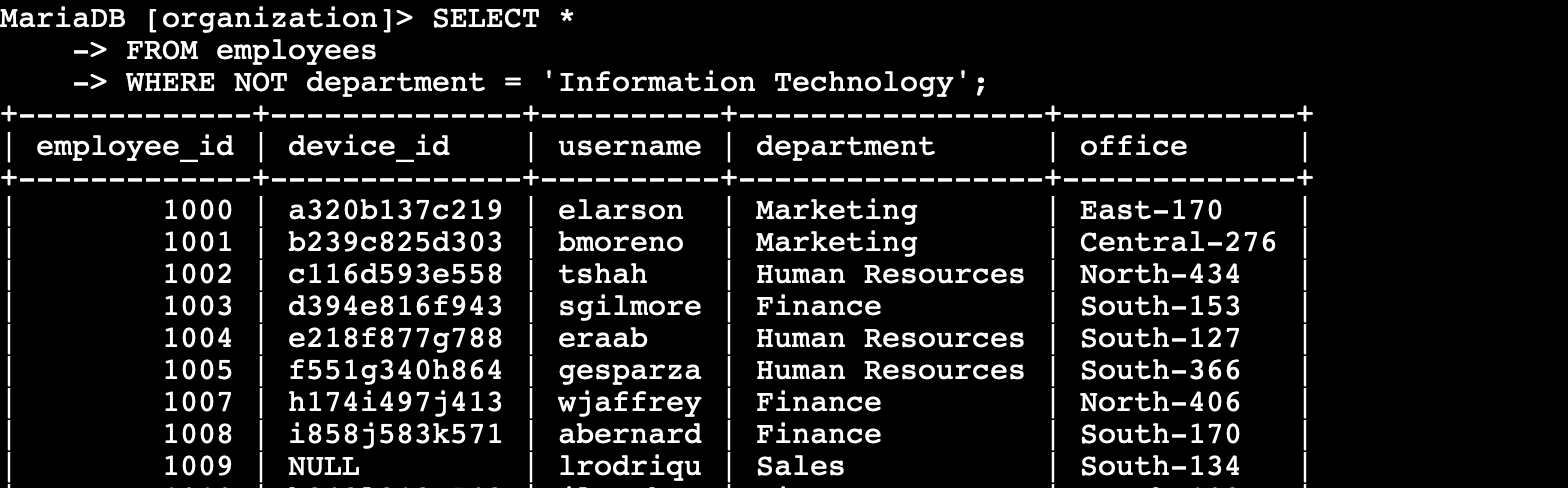
Another security update is required on machines from the Sales and Finance departments.



Using a SQL query I selected all employees who were in the department of ‘Finance’ or ‘Sales’, OR meaning only one condition must be fulfilled and being sure to specify department as the column in both conditions.

## Retrieve all employees not in IT

The team requires another security update to employee machines although the employees in the Information Technology department already received this update.



This time I used the NOT condition to select all employees whose department is not Information Technology.

## Summary

To ensure a secure system my organization tasked me with investigating possible security concerns with login attempts and machine updates. Using SQL queries and conditional filters, such as AND, NOT , and OR, I was able to obtain the data needed to check for potential failed login attempts after business hours and from different locations and dates. I was then able to filter employees from different departments to ensure and complete proper security updates on their machines ensuring a secure system.