# Apply filters to SQL queries

## Project description

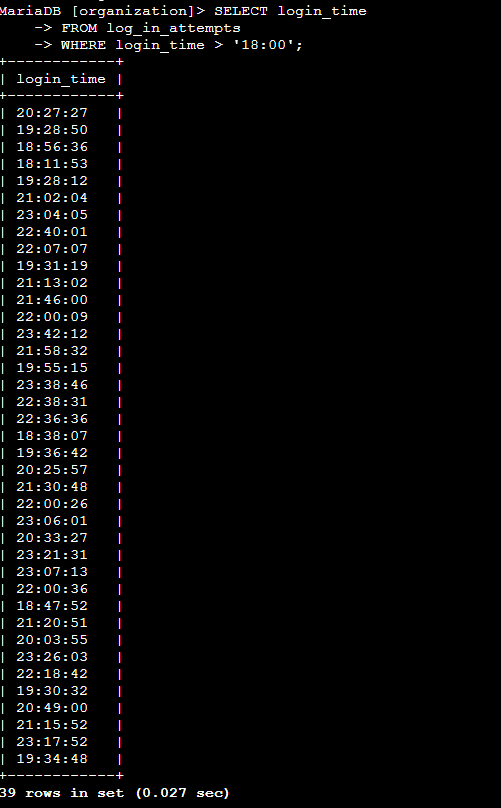
You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines.

Your task is to examine the organization’s data in their **employees** and **log\_in\_attempts** tables. You’ll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

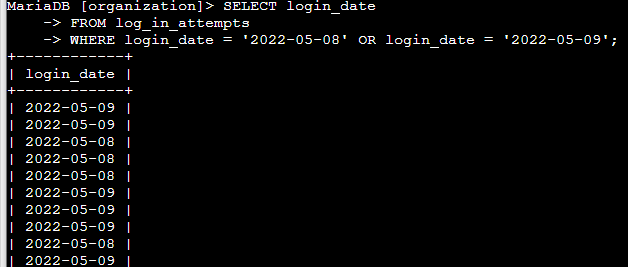
***Note:*** This scenario involves the same queries as the ones the ***Filter with AND, OR, and NOT*** lab. You can revisit the lab to get screenshots to include in your portfolio document. If you choose, it's also possible to complete this activity without revisiting the lab by typing your queries in the template

## Retrieve after hours failed login attempts

Investigating failed login attempts that were made after business hours. You want to retrieve this information from the login activity. You’ll identify all unsuccessful attempts after 18:00.Retrieve login attempts on specific dates

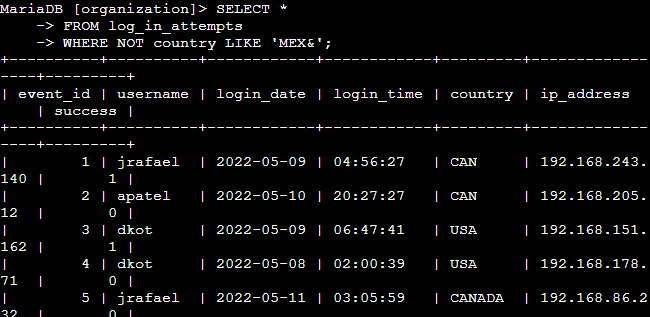


Team is investigating a suspicious event that occurred on '2022-05-09'. You want to retrieve all login attempts that occurred on this day and the day before ('2022-05-08').



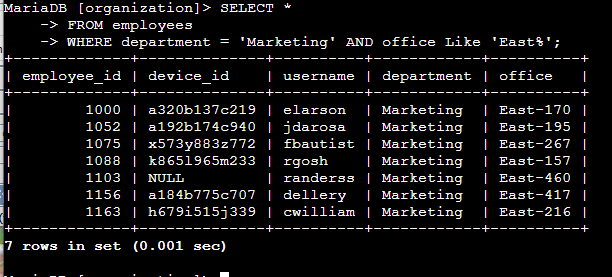
## Retrieve login attempts outside of Mexico

Team is investigating logins that did not originate in Mexico, and you need to find this information. Note that the country field includes entries with 'MEX' and 'MEXICO'. You should use the NOT and LIKE operators and the matching pattern 'MEX%'.



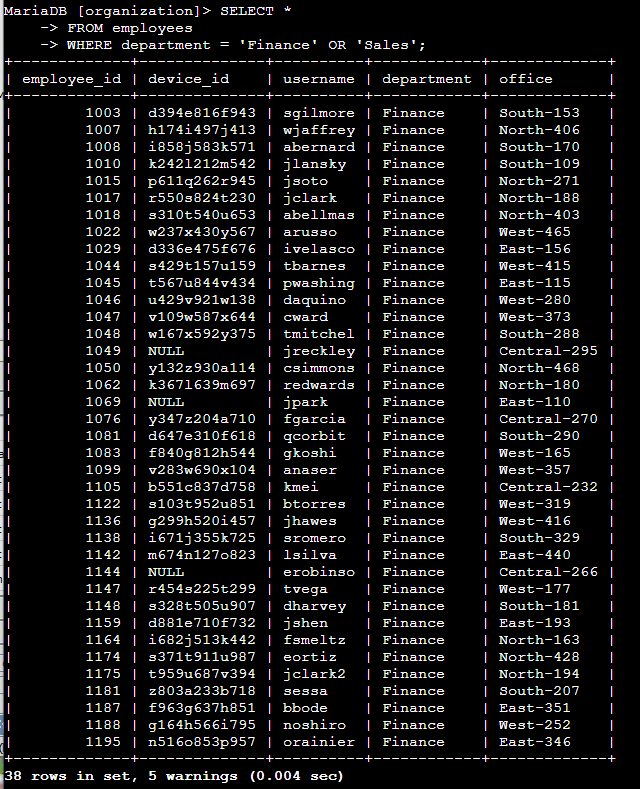
## Retrieve employees in Marketing

Team is updating employee machines, and you need to obtain the information about employees in the 'Marketing' department who are located in all offices in the East building (such as 'East-170' or 'East-320').



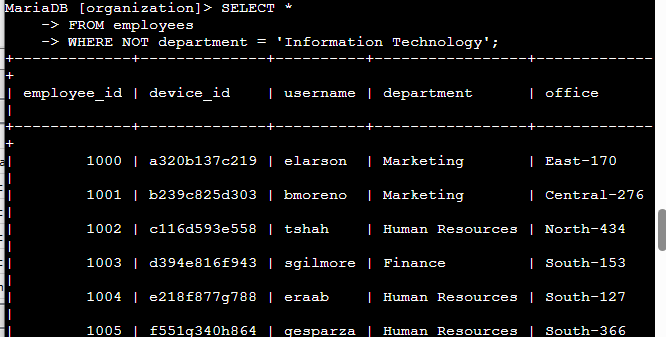
## Retrieve employees in Finance or Sales

## Team needs to perform a different update to the computers of all employees in the Finance or the Sales department, and you need to locate information on these employees.



## Retrieve all employees not in IT

Team needs to make one more update. This update was already made to employee computers in the Information Technology department. The team needs information about employees who are not in that department. You should use the NOT operator to identify these employees.



Summary

In this investigation, SQL filtering techniques using AND, OR, and NOT were applied to retrieve data critical to analyzing potential security issues and performing updates:

* After-hours failed login attempts were isolated to identify unusual activity.
* Specific date-based queries helped investigate potential breach timelines.
* Geo-location filtering revealed unauthorized logins from outside of Mexico.
* Department and location filters assisted in targeted device updates across departments like Marketing, Finance, Sales, and non-IT teams.

These queries enhance the organization's ability to act on suspicious login patterns and manage internal IT operations securely and efficiently.