# Apply filters to SQL queries

## Project description

As part of my organization’s security tasks, I can use SQL to quickly retrieve database information and further investigations into potential security issues. The information within the database can be overwhelming, but using filters allows for quick and easy selection of the desired fields and conditions.

## Retrieve after hours failed login attempts

The following shows how database information can be retrieved and displayed with SQL to investigate events occurring after business hours (17:00). This query selects all data from the log\_in\_attempts table and displays only the data where both the login\_time is after business hours and the login failed.



## Retrieve login attempts on specific dates

In response to a suspicious event, it is desired to retrieve all login data for a specified date. The following query displays event data where the login\_date is the entered date or dates.



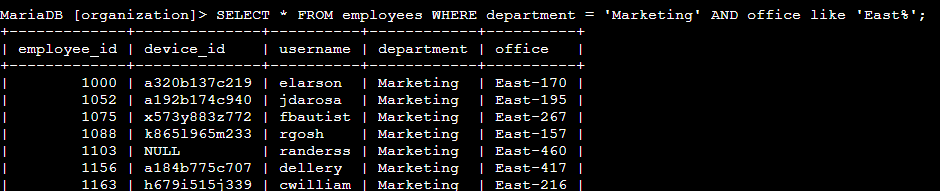
## Retrieve login attempts outside of Mexico

The following screenshot shows a query to retrieve the data from the log\_in\_attempts table and filters out any entries where the country begins with the first three characters MEX. This query displays only non-Mexico countries and is useful if there are login issues from every country except Mexico.

## 

## Retrieve employees in Marketing

Suppose that employee information was desired in relation to a security-related task. The query shown below can be used to display data from the employees table for all users of a specific department and who are in a specific building, in this case the “East” building.

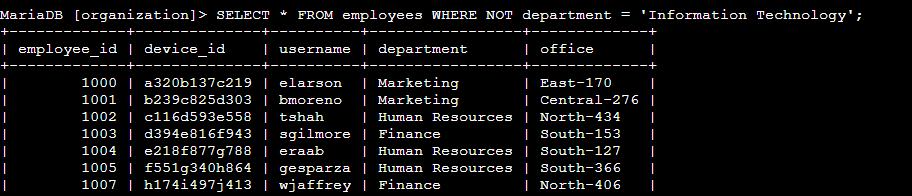


## Retrieve employees in Finance or Sales

Related to the previous query, this query shows how to retrieve data for multiple departments at a time and combines them into a single output. In this case, we were looking for employees from either the Finance or Sales departments.

## Retrieve all employees not in IT

Lastly, we can also exclude employees of a certain department. For example, the following query shows how to display employee information where all employees from the IT department are excluded from the output.



## Summary

Using the filters shown here like the AND, OR, and NOT operators, it is possible to use SQL to retrieve a significant amount of data matching the desires conditions quickly. Retrieving data in this way can greatly speed up investigations and various security-related tasks.