# Apply filters to SQL queries

## Project description

In this project, I will use SQL to obtain important data from an organization’s database to improve security measures. By applying different filters, I can retrieve specific information related to employee login behaviors and resource access, which helps in monitoring and securing IT infrastructure effectively.

## Retrieve after hours failed login attempts

SELECT \*

FROM log\_in\_attempts

WHERE login\_time > '18:00:00' AND success = 0;

This query fetches all records of failed login attempts that occurred after typical business hours, helping identify potential unauthorized access attempts.

## Retrieve login attempts on specific dates

SELECT \*

FROM log\_in\_attempts

WHERE login\_date = '2022-05-08' OR login\_date = '2022-05-09';

This query returns all login attempts that occurred on the dates of interest, useful for pinpointing activity on specific days related to a security incident.

## Retrieve login attempts outside of Mexico

SELECT \*

FROM log\_in\_attempts

WHERE country NOT LIKE 'MEX%';

This query filters out login attempts originating outside Mexico, useful for detecting external threats or breaches.

## Retrieve employees in Marketing

SELECT \*

FROM employees

WHERE department = 'Marketing' AND office LIKE 'East-%';

This query extracts details about employees in the Marketing department located in any office prefixed with "East-", ensuring proper access control and audit.

## Retrieve employees in Finance or Sales

SELECT \*

FROM employees

WHERE department = 'Finance' OR department = 'Sales';

This query gathers information about all employees either in the Finance or Sales departments, helping manage access to sensitive financial data.

## Retrieve all employees not in IT

SELECT \*

FROM employees

WHERE department NOT 'Information Technology';

This query lists all employees who are not part of the IT department, used to confirm that non-IT staff do not have access to IT-specific resources and tools.

## Summary

The SQL queries made and utilized in the project contribute to tightening security protocols and providing detailed oversight over employee activities and system accesses. This structured query approach ensures that data handling is both efficient and secure.