# Apply Filters to SQL Queries Portfolio

## Project Description

In this project, I simulated the role of a cybersecurity professional investigating potential security incidents within an organization. I used SQL queries to filter and retrieve specific data from the `employees` and `log\_in\_attempts` tables, focusing on login activity, departmental access, and geographic filtering. This project demonstrates my ability to use SQL commands to isolate critical data points for security analysis.

## Retrieve After Hours Failed Login Attempts

SQL Query:

SELECT \* FROM log\_in\_attempts  
WHERE login\_time > '18:00:00' AND success = 0;

This query filters the log\_in\_attempts table to show only failed login attempts (success = 0) that occurred after 18:00 (6 PM). This helps identify unauthorized activity during non-business hours.

## Retrieve Login Attempts on Specific Dates

SQL Query:

SELECT \* FROM log\_in\_attempts  
WHERE login\_date = '2022-05-08' OR login\_date = '2022-05-09';

This query filters for all login attempts that occurred on May 8 or May 9, 2022, allowing the team to analyze activity surrounding a suspicious event.

## Retrieve Login Attempts Outside of Mexico

SQL Query:

SELECT \* FROM log\_in\_attempts  
WHERE country NOT LIKE '%MEX%';

This query retrieves all login attempts from countries other than Mexico, filtering out any records where the country includes 'MEX' or 'MEXICO' using the NOT LIKE clause.

## Retrieve Employees in Marketing (East Building)

SQL Query:

SELECT \* FROM employees  
WHERE department = 'Marketing' AND office LIKE 'East%';

This query filters the employees table to return all users in the Marketing department located in any East building office.

## Retrieve Employees in Finance or Sales

SQL Query:

SELECT \* FROM employees  
WHERE department = 'Finance' OR department = 'Sales';

This query identifies all employees in either the Finance or Sales departments for targeted security updates.

## Retrieve All Employees Not in IT

SQL Query:

SELECT \* FROM employees  
WHERE department != 'Information Technology';

This query filters out employees from the Information Technology department to focus updates on all others.

## Summary

In this project, I applied SQL filters to investigate security incidents and identify relevant employee and login activity. I used AND, OR, NOT, and LIKE to refine queries based on time, date, location, and department. These skills are essential for examining suspicious patterns and narrowing down large datasets for focused security reviews.