# Apply Filters to SQL Queries Portfolio

## Project Description

In this project, I acted as a cybersecurity professional investigating potential login-based security incidents in a large organization. Using SQL queries, I applied filters to identify suspicious login attempts and isolate employee data related to specific departments and locations. This work supports auditing efforts and helps ensure data security across systems.

## Retrieve After Hours Failed Login Attempts

SQL Query:

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

This query retrieves all failed login attempts (success = 0) that occurred after 6:00 PM (18:00). It helps identify unauthorized activity outside of standard 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 returns all login attempts that occurred on May 8 or May 9, 2022—two days under investigation for suspicious activity.

## Retrieve Login Attempts Outside of Mexico

SQL Query:

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

This query excludes login attempts from any entries containing 'MEX' in the country field, filtering out both 'MEXICO' and 'MEX' to show only access attempts from outside Mexico.

## Retrieve Employees in Marketing (East Building)

SQL Query:

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

This query filters employees who are part of the Marketing department and whose office is located in the East building (e.g., East-170, East-320).

## Retrieve Employees in Finance or Sales

SQL Query:

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

This query lists employees in either the Finance or Sales departments, which are both undergoing a new round of system updates.

## Retrieve All Employees Not in IT

SQL Query:

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

This query returns all employees except those in the Information Technology department. These individuals still need to receive the most recent system updates.

## Summary

Throughout this portfolio project, I used SQL filters—such as AND, OR, NOT, and LIKE—to target specific data in employee and login datasets. I identified unauthorized login behavior and isolated groups for system patching and security audits. This demonstrates my ability to query effectively and securely in support of organizational cybersecurity goals.