# Apply filters to SQL queries

## Project description In this project, the goal is to investigate suspicious login activity within an organization’s system using SQL queries. Through the use of filters, the task involves identifying specific login attempts based on various conditions such as time, department, location, and country. The objective is to efficiently retrieve relevant data from the log\_in\_attempts and employees tables to identify potential security risks and ensure targeted updates to employee machines across the organization.

## Retrieve after hours failed login attempts

## SELECT \*

## FROM log\_in\_attempts

## WHERE success = 0

## AND CAST(strftime('%H', login\_time) AS INTEGER) > 18; *Retrieves all login attempts that failed (success = 0) and occurred after 18:00, helping identify suspicious activity outside business hours.* Retrieve login attempts on specific dates

## SELECT \*

## FROM log\_in\_attempts

## WHERE login\_date = '2022-05-08' OR login\_date = '2022-05-09'; *Retrieves all login attempts that occurred on either 2022-05-08 or 2022-05-09, useful for investigating events around a specific incident date.* Retrieve login attempts outside of Mexico

## SELECT \*

## FROM log\_in\_attempts

## WHERE country NOT LIKE 'MEX%'

## AND country NOT LIKE 'MEXICO%'; *Retrieves all login attempts where the country is not listed as MEX or MEXICO, helping focus the investigation on activity from outside Mexico.* Retrieve employees in Marketing

## SELECT \*

## FROM employees

## WHERE department = 'Marketing'

## AND office LIKE 'East-%'; *Retrieves all employees who work in the Marketing department and are located in offices that begin with "East-", targeting specific machines for updates.* Retrieve employees in Finance or Sales

## SELECT \*

## FROM employees

## WHERE department = 'Sales'

## OR department = 'Finance'; *Retrieves employees who belong to either the Sales or Finance departments to identify machines that need a specific security update.* Retrieve all employees not in IT SELECT \*

## FROM employees

## WHERE department != 'Information Technology';

## *Retrieves all employees who are not in the Information Technology department, so updates can be applied only to those who haven't received them yet.* Summary

The SQL queries developed in this project focus on identifying suspicious login attempts and employee machine details for security updates. They address tasks such as retrieving after-hours failed logins, filtering login attempts based on specific dates, and targeting employees in specific departments or locations. By using the LIKE keyword and other filtering techniques, the queries ensure precise results, helping to streamline the investigation of security incidents and perform timely updates across the organization.