# Apply filters to SQL queries

## Project description

n this project, I investigated potential security issues related to login attempts and employee machines within a large organization. Using SQL queries, I filtered data from the employees and log\_in\_attempts tables to identify suspicious activities and gather information needed for security updates. The queries employed various SQL filtering techniques, including AND, OR, NOT, and LIKE, to achieve the desired results.

## Retrieve after hours failed login attempts

**Query:**

SELECT \*

FROM log\_in\_attempts

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

**Description:** This query retrieves all records from the log\_in\_attempts table where the login attempt failed (success = 0) and the login time is after 18:00. This helps identify failed login attempts that occurred after business hours, which might indicate suspicious activity.

## Retrieve login attempts on specific dates

**Query:**

SELECT \*

FROM log\_in\_attempts

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

**Description:** This query retrieves all records from the log\_in\_attempts table where the login date is either 2022-05-08 or 2022-05-09. This helps investigate login attempts around the time of a suspicious event.

## Retrieve login attempts outside of Mexico

**Query:**

SELECT \*

FROM log\_in\_attempts

WHERE country NOT LIKE 'MEX%' AND country NOT LIKE 'MEXICO%';

**Description:** This query retrieves all records from the log\_in\_attempts table where the country is not Mexico. The LIKE keyword with % is used to match both 'MEX' and 'MEXICO' variations. This helps exclude login attempts from Mexico when investigating suspicious activity.

## Retrieve employees in Marketing

**Query:**

SELECT \*

FROM employees

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

**Description:** This query retrieves all records from the employees table where the department is Marketing and the office is in the East building. The LIKE keyword with % is used to match any variations of 'Marketing' and any office in the East building. This helps identify employees in Marketing for security updates.

## Retrieve employees in Finance or Sales

**Query:**

SELECT \*

FROM employees

WHERE department LIKE '%Finance%' OR department LIKE '%Sales%';

**Description:** This query retrieves all records from the employees table where the department is either Finance or Sales. The LIKE keyword with % is used to match any variations of 'Finance' and 'Sales'. This helps identify employees in these departments for security updates.

## Retrieve all employees not in IT

**Query:**

SELECT \*

FROM employees

WHERE department NOT LIKE '%Information Technology%';

**Description:** This query retrieves all records from the employees table where the department is not Information Technology. The LIKE keyword with % is used to match any variations of 'Information Technology'. This helps identify employees in all other departments for security updates.

## Summary

The SQL queries developed in this project addressed specific security concerns by retrieving relevant data on failed login attempts, login activity on particular dates, and employee information for targeted security updates. By effectively applying SQL filters, I was able to isolate and analyze critical data, contributing to the overall security and integrity of the organization's systems.