# Apply filters to SQL queries in a security context

## Project description

I am a security professional at a large organization. Part of my job is to investigate security issues to help keep the system secure. I recently discovered some potential security issues that involve login attempts and employee machines.

My task is to examine the organization’s data in their **employees** and **log\_in\_attempts** tables. Here, I will need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

## Retrieve after hours failed login attempts

The company works until 18:00:00 everyday and in SQL True is 1 and False is 0. So this SQL statement will work like so:

SELECT \* FROM log\_in\_attempts

WHERE login\_time > ‘18:00:00’

AND

Success = 0;

## Retrieve login attempts on specific dates

To receive login attempts on specific dates we can say

SELECT \* FROM log\_in\_attempts

WHERE login\_date LIKE ‘01-02-2022’;

For 2 dates I can say:

SELECT \* FROM log\_in\_attempts

WHERE login\_date LIKE ‘01-02-2022’

OR login\_date LIKE ‘01-02-2022’;

And for a range of dates I can say:

SELECT \* FROM log\_in\_attempts

WHERE login\_date BETWEEN ‘01-02-2022’

AND ‘01-03-2022’;

Start and end date is inclusive here.

## Retrieve login attempts outside of Mexico

SELECT \* FROM log\_in\_attempts

WHERE country NOT LIKE ‘Mex%’;

% is a wildcard which means any number of unknown letters after whatever is specific before. In this case it will catch any row that has “MEX” or any row with “MEXICO”.

## Retrieve employees in Marketing

SELECT \* FROM employees

WHERE department LIKE ‘Marketing’;

## Retrieve employees in Finance or Sales

SELECT \* FROM employees

WHERE department LIKE ‘Finance’

OR department LIKE ‘Sales’;

## Retrieve all employees not in IT

SELECT \* FROM employees

WHERE department NOT LIKE ‘IT’;

## Summary

This activity gave me a good overall understanding of working with logs in a cybersecurity context within an organisation. Although I had a good base in SQL i still found this extremely helpful.