# Apply filters to SQL queries

## Project description

I’m a security analyst at Milo incorporation . I recently discovered some potential security issues that involve login attempts and employee machines. I used SQL filters to retrieve records from different datasets and investigated the potential security issues.

## Retrieve after hours failed login attempts

To identify all failed login attempts that occurred after the company’s business hour (18:00) , the following sql filters were used. Failed logins that occurred after 18:00 was retrieved.

SELECT\*

FROM log\_in\_attempts

WHERE login\_time > ‘18:00’ AND success = ‘FALSE’;

The SELECT\* was used to return all the columns in the dataset.while the FROM indicated which table to query which was the log\_in\_attempts table.The WHERE syntax indicate the condition for the filter which is login\_time > ‘18:00’ AND success = ‘FALSE’; . The AND filter indicates that both conditions (login time after 18:00 and failed login) must be met simultaneously.

## Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09. To investigate this event, all login attempts which occurred on this day and the day before (2022-05-08) were reviewed.

SQL was used to create a query that filters and identifies all login attempts that occurred on 2022-05-09 or 2022-05-08.

SELECT\*

FROM log\_in\_attempts

WHERE login\_date = ‘2022-05-09’ or login\_date = ‘2022-05-08’;

The SELECT\* was used to return all columns in the dataset.while the FROM indicated which table to query which was the log\_in\_attempts table.The login\_date of both '2022-05-09' or ‘2022-05-08’ were filtered using the WHERE syntax. The or filter specifies that either condition ('2022-05-09' or ‘2022-05-08’ ) must be met.

## Retrieve login attempts outside of Mexico

There’s been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. Now, you need to investigate login attempts that occurred outside of Mexico.

SELECT\*

FROM log\_in\_attempts

WHERE NOT country LIKE MEX%;

The SELECT\* was used to return all the columns in the dataset.while the FROM indicated which table to query which was the log\_in\_attempts table.The WHERE syntax indicates the condition of the filter which is the country. NOT country LIKE MEX% describes all countries except the mexico. The NOT filter was used to filter all data that does not match a condition.

## Retrieve employees in Marketing

The security team needed to perform security updates on specific employee machines in the Marketing department in the East building. The following sql filters were used to perform these actions.

SELECT\*

FROM employees

WHERE department = ‘Marketing’ AND office like East%;

The SELECT\* was used to return all the columns in the dataset. The datasets were returned from the employees table. WHERE describes what condition should be filtered which is the department (Marketing) and office found in the East building.

% is a wild card used to substitute any other character .For example East% could be used to describe East103, EastT111 and East2@ .like is used to apply wildcards to the filter.

## Retrieve employees in Finance or Sales

To perform a different security update on machines for employees in the Sales and Finance departments. The following filters in SQL were used to create a query ;

SELECT\*

FROM employees

WHERE department = ‘Finance’ AND department = ‘Sales’;

The SELECT\* was used to return all the columns in the employees table. WHERE describes what condition should be filtered which is both departments (Marketing and Sales).

## Retrieve all employees not in IT

The security team needed to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it.

SELECT\*

FROM employees

WHERE NOT department = 'Information Technology’;

The SELECT\* was used to return all the columns in the dataset.while the FROM indicated which table to query which was the employees table.The WHERE NOT WHERE NOT department = 'Information Technology’; describes all departments except the information technology.

## Summary

I work as a security analyst at Milo Incorporation, where I've recently uncovered potential security concerns related to login attempts and employee machines. Using SQL filters, I accessed various datasets to thoroughly investigate these issues.