# Apply filters to SQL queries

## Project description

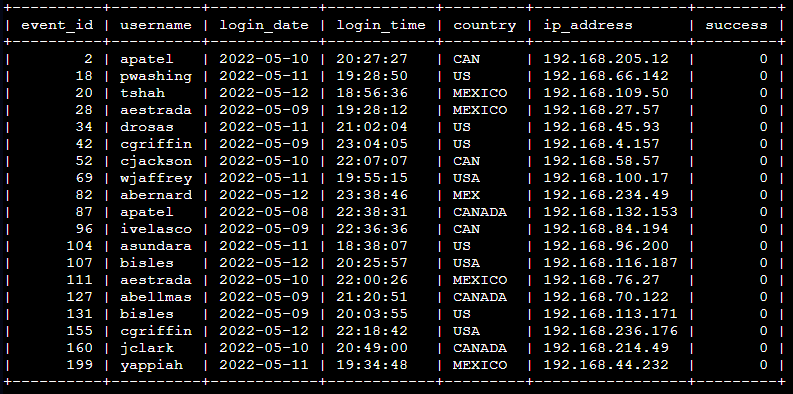
In this scenario the organization is working to make their system more secure. My role as a cybersecurity analyst is to investigate potential security issues within the organization by analyzing data from two tables (“log\_in\_attempts” and “employees”). The goal is to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

## Retrieve after hours failed login attempts

To investigate potential security incidents that occurred after business hours (in this case 18:00), I will query the “log\_in\_attempts” table using SQL filter and for the filter itself will be from “login\_time” and “success” columns. The **success** column contains a value of **0** when a login attempt fails.

SELECT \*

FROM log\_in\_attempts  
WHERE login\_time > ‘18:00;00’ and success = 0;

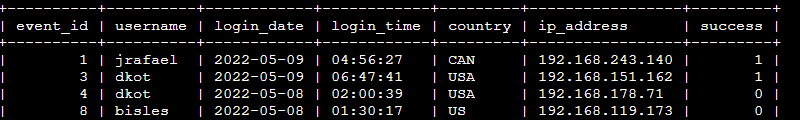


## Retrieve login attempts on specific dates

To investigate a suspicious event, I will query the ‘log\_in\_attemps’ with a login\_date filter that occurred on 2022-05-08 and 2022-05-09.

SELECT \*

FROM log\_in\_attempts  
WHERE login\_date ‘2022-05-08’ OR login\_date ‘2022-05-09’;



## Retrieve login attempts outside of Mexico

To examine login attempts outside Mexico, I will use SQL to query the database from the log\_in\_attempts table using filter ‘WHERE,’ ‘LIKE’ the country ‘NOT’ ‘MEXICO’ an ‘MEX’.

SELECT \*

FROM log\_in\_attempts  
WHERE NOT country LIKE ‘MEX%’;



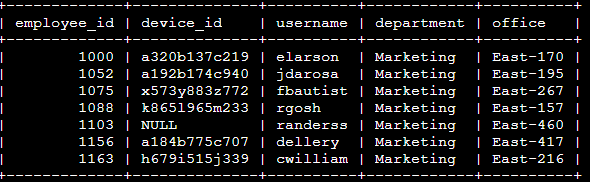
## Retrieve employees in Marketing

My team wants to perform security updates on specific employee machines in the Marketing department which is located at the East building. To retrieve the data I will SQL query the ‘employees’ table and apply SQL filters.

SELECT \*

FROM employees

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



## Retrieve employees in Finance or Sales

My team needs to perform a different security update on machines for employees in the Sales and Finance departments. To retrieve the data I will use filters in SQL to create a query from the ‘employees’ table that identifies all employees in the’ Sales’ or ‘Finance’ departments. (The department of the employee is found in the department column, which contains values that include ‘Sales’ and ‘Finance’.)

SELECT \*

FROM employees

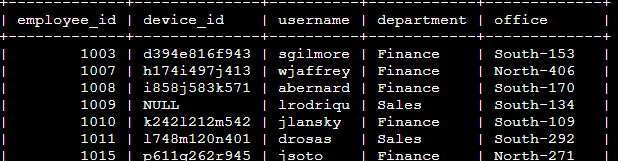
WHERE department = ‘Finance’ OR department = ‘Sales’;

Alternative

SELECT \*

FROM employees

WHERE department IN ('Finance','Sales');



## Retrieve all employees not in IT

My team needed to make an update to employee machines, but the employees in the IT department already had the update. To retrieve the data I will SQL query the ‘employees’ table and apply a ‘NOT’ filter to retrieve data other than IT department.

SELECT \*

FROM employees

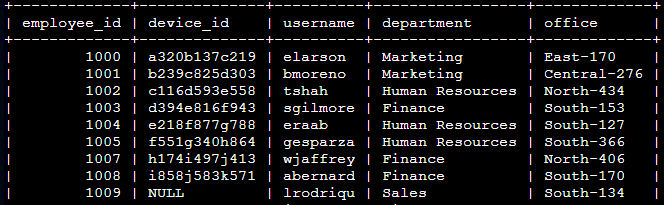
WHERE NOT department = ‘Information Technology’;

Alternative

SELECT \*

FROM employees

WHERE department != ‘Information Technology’;



## Summary

Through SQL queries, i’ve conducted a comprehensive analysis into potential security issues, like:

* After-hours login attempts
* including after-hours login attempts,
* suspicious login attempts on specific dates,
* login attempts from outside Mexico,
* employee details based on department and location

I use two different tables, ‘log\_in\_attempts’ and ‘employees’ and I used the ‘AND’, ‘OR’, and ‘NOT’ operators to filter for the specific information needed for each task. I also used ‘LIKE’ and the percentage sign (‘%’) wildcard to filter for patterns.