# Apply filters to SQL queries

## Project description

My organization is requiring a more secure system. Therefore, in order to investigate all potential security issues, the employee computer must be updated for more clarity. The following steps will showcase how I utilized SQL to perform a variety of security-related tasks.

## Retrieve after hours failed login attempts

Due to a known security incident occurring after working business hours (18:00), all login attempts made after 18:00 must be investigated. The following SQL command filtered for any failed login attempts after business hours.



The breakdown of this SQL command is selecting all data from the table named ‘log\_in\_attempts’. This stores all the data from the server, so the ‘WHERE’ statement allows for the filtering to be after the login time of 18:00 with a conjoining failed attempt.

## Retrieve login attempts on specific dates

IT was notified of a suspicious event occurring on 2022-05-09. This requires all login attempts for this date to be investigated on the day and one day prior. The following SQL command will filter for these requirements.



Once again, this SQL command selects all data from the same login attempt table with a filter on the dates ‘2022-05-09’ and ‘2022-05-08’ for analysis.

## Retrieve login attempts outside of Mexico

After investigating the organization’s data on login attempts, there seems to be an issue with attempts that occurred outside of Mexico. This provides a new requirement for the analysis of data. The following SQL command will filter for all login attempts outside of Mexico.



The same selection of all data and login attempts table is the same as the last queries with the difference utilizing the ‘NOT’ function to preclude the inclusion of login attempts from Mexico.

## Retrieve employees in Marketing

The IT team requires updating the computers for employees in the Marketing department. To achieve this, the employee machines need to be identified. The following SQL command will filter the employee list with the Marketing department and their location in the East building as the qualifiers.



The SQL command only pulls data from the employees table when the data contains both the correct department (Marketing) and the correct office (East).

## Retrieve employees in Finance or Sales

Piggybacking on updating the computers on the server, both the Finance and Sales departments require some updates as well. This update requires a different security update, therefore, the query will only be regulated to these two new departments.



The qualifiers in the ‘WHERE’ command focus on specifically the two aforementioned departments belonging to both Finance and Sales. This information was pulled from the employees table.

## Retrieve all employees not in IT

The IT team requires one last security update on employees, which will include all except those belonging to the Information Technology department. To create this filter of data, the SQL query will preclude the admission of only the IT department.



This SQL query returns all employees not in the Information Technology department. The ‘NOT’ command achieves this function. This information was pulled from the employees table.

## Summary

I applied filters to a variety of SQL queries that allowed for specific information to be pulled regarding login attempts and various employee machines. I utilized two different tables (‘login\_in\_attempts’, ‘employees’) and five different SQL commands (AND, OR, NOT, LIKE, %) to achieve the necessary filtering of data.