# Apply filters to SQL queries

## Project description

My organization is focused on enhancing the security of its system. My role involves ensuring the system's safety, examining any potential security concerns, and updating employee computers as necessary. Below are examples of how I utilized SQL with filters to carry out security-related tasks.

## Retrieve after hours failed login attempts

A potential security incident took place after business hours (post 18:00). It is essential to investigate all failed login attempts during this time.

The code below illustrates how I constructed a SQL query to filter for failed login attempts that occurred after hours.



The first part of the screenshot is my query, and the second part is a portion of the output. This query filters for failed login attempts that occurred after 18:00. First, I started by selecting all data from the log\_in\_attempts table. Then, I used a WHERE clause with an AND operator to filter my results to output only login attempts that occurred after 18:00 and were unsuccessful. The first condition is login\_time > '18:00', which filters for the login attempts that occurred after 18:00. The second condition is success = FALSE, which filters for the failed login attempts.

## Retrieve login attempts on specific dates

A suspicious event took place on May 9, 2022. Any login activities on that date or the previous day require investigation.

The code below shows how I developed a SQL query to filter for login attempts that occurred on those specific dates.



## Retrieve login attempts outside of Mexico

After investigating the organization’s data on login attempts, I believe there is an issue with the login attempts that occurred outside of Mexico. These login attempts should be investigated.

The following code demonstrates how I created a SQL query to filter for login attempts that occurred outside of Mexico.



## Retrieve employees in Marketing

My team wants to update the computers for certain employees in the Marketing department. To do this, I have to get information on which employee machines to update.

The following code demonstrates how I created a SQL query to filter for employee machines from employees in the Marketing department in the East building.



## Retrieve employees in Finance or Sales

The machines for employees in the Finance and Sales departments also need to be updated. Since a different security update is needed, I have to get information on employees only from these two departments.

The following code demonstrates how I created a SQL query to filter for employee machines from employees in the Finance or Sales departments.



## Retrieve all employees not in IT

The machines for employees in the Finance and Sales departments also need to be updated. Since a different security update is needed, I have to get information on employees only from these two departments.

The following code demonstrates how I created a SQL query to filter for employee machines from employees in the Finance or Sales departments.



## Summary

I applied filters to SQL queries to get specific information on login attempts and employee machines. I used two different tables, log\_in\_attempts and employees. 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.