# Apply filters to SQL queries

## Project description

My organization is working to make their system more secure. It is my job to ensure the system is safe, investigate all potential security issues, and update employee computers as needed. The following steps provide examples of how I used SQL with filters to perform security-related tasks.

## Retrieve after hours failed login attempts

There was a potential security incident that occurred after business hours (after 18:00). All after hours login attempts that failed need to be investigated.

The following code demonstrates how I created a SQL query to filter for failed login attempts that occurred after business hours.



I used the SELECT statement to query the logs database, specifically the login attempts from log\_in\_attempts table. I used WHERE clause to make sure I only get entries where login\_time > ’18:00’ and to make sure the login attempt was failed I used success = FALSE

## Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09. Any login activity that happened on 2022-05-09 or on the day before needs to be investigated.

The following code demonstrates how I created a SQL query to filter for login attempts that occurred on specific dates.



I used a WHERE clause with an OR operator to filter my results to output only login attempts that occurred on either 2022-05-09 or 2022-05-08. The first condition is login\_date = '2022-05-09', which filters for logins on 2022-05-09. The second condition is login\_date = '2022-05-08', which filters for logins on 2022-05-08.

## 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.



I used a WHERE clause with NOT to filter for countries other than Mexico. The data has Mexico represented as MEXICO and MEX, so I had to use LIKE with ‘MEX%’ to catch all the representations of Mexico and get only those login attempts which are made 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.



I used a WHERE clause with AND to filter employees who work in the Marketing department and the East building. I used LIKE with ‘EAST%’ as the pattern to match the office column for East building locations.

## 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.



I applied a WHERE clause with OR to filter employees in either the Finance or Sales departments. The conditions are department = ‘Finance’ or department = ‘SALES’, which select employees from each respective department.

## Retrieve all employees not in IT

My team needs to make one more security update on employees who are not in the Information Technology department. To make the update, I first have to get information on these employees.

The following demonstrates how I created a SQL query to filter for employee machines from employees not in the Information Technology department.



I used a WHERE clause with NOT to filter for employees not in this department.