# Apply filters to SQL queries

## Project description

In this project, I utilized SQL queries to retrieve specific data from an organization's employee and login records. Through SQL filtering techniques using `AND`, `OR`, and `NOT` operators, I was able to investigate potential security issues related to login attempts and employee information. This project demonstrates my ability to handle real-world SQL queries to analyze datasets efficiently and to use SQL as a tool for security investigations.

## Retrieve after hours failed login attempts

For this task, I used the following SQL query to retrieve all failed login attempts that occurred after 18:00:

|  |
| --- |
| SELECT event\_id, username, login\_date, login\_time, country, ip\_address  FROM log\_in\_attempts  WHERE login\_time > '18:00:00' AND success = 0; |

This query filters login attempts that happened after 18:00 hours and were marked as failed (`success = 0`).

## Retrieve login attempts on specific dates

To retrieve all login attempts that occurred on 2022-05-08 or 2022-05-09, I used the following SQL query:

|  |
| --- |
| SELECT event\_id, username, login\_date, login\_time, country, ip\_address  FROM log\_in\_attempts  WHERE login\_date = '2022-05-08' OR login\_date = '2022-05-09'; |

This query uses the `OR` operator to find login attempts that occurred on either of the specified dates.

## Retrieve login attempts outside of Mexico

I created this SQL query to identify login attempts that did not originate in Mexico:

|  |
| --- |
| SELECT event\_id, username, login\_date, login\_time, country, ip\_address  FROM log\_in\_attempts  WHERE NOT country LIKE 'MEX%'; |

This query uses the `NOT LIKE` operator to exclude login attempts from both "MEX" and "MEXICO".

## Retrieve employees in Marketing

For this task, I filtered employees working in the Marketing department in the East building using the following query:

|  |
| --- |
| SELECT employee\_id, username, device\_id, department, office  FROM employees  WHERE department = 'Marketing' AND office LIKE 'East%'; |

The `LIKE` keyword is used to select only those offices located in the East building.

## Retrieve employees in Finance or Sales

To identify employees in either the Finance or Sales departments, I used the following query:

|  |
| --- |
| SELECT employee\_id, username, device\_id, department, office  FROM employees  WHERE department = 'Finance' OR department = 'Sales'; |

The `OR` operator is used to retrieve records where the employee belongs to either department.

## Retrieve all employees not in IT

The following SQL query was used to retrieve all employees not in the IT department:

|  |
| --- |
| SELECT employee\_id, username, device\_id, department, office  FROM employees  WHERE department != 'Information Technology'; |

The `!=` operator is used to exclude all employees in the Information Technology department.

## Summary

In this project, I utilized SQL queries to investigate suspicious login attempts and identify specific employees for security updates. By applying `AND`, `OR`, and `NOT` operators, I filtered data based on time, date, location, and department. This project demonstrates my ability to use SQL queries to effectively retrieve and analyze data for cybersecurity purposes.