# Apply filters to SQL queries

## Project description

We are going to investigate security issues to help keep the system of the organization secure. Recently we discovered some potential security issues that involve login attempts and employee machines.

In this project we will examine the organization’s data in their employees and log\_in\_attempts tables. We will use SQL filters to retrieve records from different datasets and investigate the potential security issues.

## Retrieve after hours failed login attempts

There’s a potential security incident that occurred after business hours. To discover more about this incident, we started by investigating the records on log\_in\_attempts table and filter all after hours suspicious login activity: we create a query to identify all failed login attempts occurred after 18:00.

The time of the login attempt is found in the login\_time column. The success column contains the value of 0 when the login attempt failed:

|  |
| --- |
| MariaDB [organization]> SELECT \*  -> FROM log\_in\_attempts  -> WHERE login\_time > '18:00' AND success = FALSE; |

In this query we retrieve all the columns from the log\_in\_attempts table, and filter only those records with failed attempts AND that occurred past 18:00.

## Retrieve login attempts on specific dates

Another suspicious event occurred on 2022-05-09. To investigate this incident, we will review all the records from this day and the day before (2022-05-08). The date of the login attempt is found in the login\_date column:

|  |
| --- |
| MariaDB [organization]> SELECT \*  -> FROM log\_in\_attempts  -> WHERE login\_date = '2022-05-09' OR login\_date = '2022-05-08'; |

In this query, we’ve used two filters for the same column to retrieve any records that matches one date OR the other.

## Retrieve login attempts outside of Mexico

There’s been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. We needed to investigate login attempts that occurred outside of Mexico. When referring to Mexico, the country column contains values of both MEX and MEXICO:

|  |
| --- |
| MariaDB [organization]> SELECT \* ->  -> FROM log\_in\_attempts  -> WHERE NOT country LIKE 'MEX%'; |

In this query, we need to filter by all countries that are NOT Mexico, and we do this by using the LIKE keyword and the value ’MEX%’ to specify that it must start with MEX followed by any kind of string.

## Retrieve employees in Marketing

The team wants to perform security updates on specific employee machines in the Marketing department. The information on those employee machines is in the employees table. We needed to identify all employees in the Marketing department for all offices in the East building.

The department of the employee is found in the department column, which contains values that include Marketing. The office is found in the office column. Some examples of values in this column are East-170, East-320, and North-434:

|  |
| --- |
| MariaDB [organization]> SELECT \*  -> FROM employees  -> WHERE department = 'Marketing' AND office LIKE 'East%'; |

In this query, we retrieve information filtering by the Marketing department, AND office that starts with ‘East’.

## Retrieve employees in Finance or Sales

To perform a different security update on machines for employees in the Sales and Finance departments, we needed a different query on the same table, on the department column:

|  |
| --- |
| MariaDB [organization]> SELECT \*  -> FROM employees  -> WHERE department = 'Finance' OR department = 'Sales'; |

In this query, we filter to retrieve all the records where department has the value of Finance or Sales.

## Retrieve all employees not in IT

To make one more update to employee machines, we needed another query on the department column. The employees who are in the Information Technology department already had this update, but employees in all other departments need it.

|  |
| --- |
| MariaDB [organization]> SELECT \*  -> FROM employees  -> WHERE NOT department = 'Information Technology'; |

In this query, we will retrieve all the records where department column doesn’t have the value ’Information Technology’.

## Summary

To solve the different security issues, we had to investigate the logs recorded in the database by using SQL to retrieve the information we need with each of the steps.