# Apply filters to SQL queries

## Project description

As a security professional at a large organization, part of the role involves investigating security issues to help keep the system secure. Recently some potential security issues that involve login attempts and employee machines were discovered.

## Retrieve after hours failed login attempts

A screenshot of a computer screen

Description automatically generated

In order to investigate a potential security incident that occurred after business hours, we used SQL to query the log\_in\_attempts table and review the all the failed login attempts that occurred during after hours login.

SELECT \*

FROM employees

WHERE login\_time > ’18:00’ AND success = 0;

This query selects all the columns in the employees database where the login time is after 18:00 and where the success has failed which is represented as FALSE or 0.

## Retrieve login attempts on specific dates

A screen shot of a computer

Description automatically generated

A suspicious event occurred on 2022-05-09, to investigate the event we want to review all login attempts that occurred on this day and the day before.

SELECT \*

FROM log\_in\_attempts

WHERE login\_date = ’2022-05-08’ OR login\_date = ‘2022-05-09;

This queries all the columns with all the information from those two login dates.

## Retrieve login attempts outside of Mexico

The team has determined that the suspicious activity did not occur in Mexico. To further filter the query we utilize the following:

A screen shot of a computer

Description automatically generated

This query uses the NOT key word which queries all the countries except for Mexico. Since some entries have MEX or MEXICO we utilize the % to account for both.

## Retrieve employees in Marketing

A screenshot of a computer

Description automatically generated

The team wants to perform security updates on specific employee machines in the Marketing department in all the offices in the East building.

## Retrieve employees in Finance or Sales

## A screenshot of a computer screen Description automatically generated

## The security team needs to perform a different security update on machines for employees in the Sales and Finance departments. This query utilizing the keyword OR, queries all employees in these two departments.

## Retrieve all employees not in IT

The team needs to make one more update to the employee machines. The employees in the IT department already gave the update, so the following query excludes this department.

A screenshot of a computer program

Description automatically generated

All other departments are queried here.

## Summary

In this case, the security team had to query different departments to conduct investigations and then to update its software. Through SQL, security analysts are able to filter out specific columns, and rows based on the desired output. Employees can be filtered by department, office, location and more.