# Apply filters to SQL queries

## Project description

Potential security issues have been detected within my organization’s security system that involve login attempts and employee machines in departments need to be updated to suffice security standards. My organization’s data needs to be examined and investigated to uncover these potential security threats using SQL filters. The following prompts provide examples of how I used SQL filters to perform these tasks.

## Retrieve after hours failed login attempts

Using filters in SQL to run a query in regards to unsuccessful login attempts after 18:00 (office hours end at this time), it was observed that there were 19 failed login attempts that occurred after office hours ended. To retrieve the information the following code was used retrieve the output:

* **SELECT** \* **FROM**  log\_in\_attempts **WHERE**  login\_time > ‘18:00’ **AND** success = FALSE;

## Retrieve login attempts on specific dates

Suspicious activity was detected that occurred on May, 09 2022. Login attempts that occurred on this day and the day before needed to be retrieved to investigate this incident. Using SQL filters it was observed that there were 75 login attempts in these two days. To retrieve this information the following code was used retrieve the output:

* **SELECT** \* **FROM** log\_in\_attempts **WHERE** login\_date = ‘2022-05-09’ **OR** login-date = ‘2022-05-08’;

## Retrieve login attempts outside of Mexico

The team has observed suspicious activity with login attempts that did not originate in Mexico. Login attempts that occurred outside of Mexico needed to be retrieved to investigate this activity. SInce both values, MEX and MEXICO, are contained in the country column, **LIKE** with % needs to be implemented within the query. It was observed there were 144 login attempts made outside of Mexico. The following code was used retrieve the output:

* **SELECT** \* **FROM** log\_in\_attempts **WHERE NOT** country **LIKE**  ‘MEX%’;

## Retrieve employees in Marketing

The security team needs to perform security updates on specific machines within our organization, specifically the Marketing department. All employees who are located in offices within the East building need to be identified. To satisfy the query criteria, both **AND** & **LIKE** need to be included in the command. Using SQL filters we were able to retrieve the list of employees to complete this task. The following code used retrieve the output:

* **SELECT** \* **FROM** employees **WHERE** department = ‘Marketing’ **AND** office **LIKE** ‘East%’;

## Retrieve employees in Finance or Sales

The security team needs to perform security updates on specific machines for employees in the Sales and Finance departments of the organization. Since the command contains names for two different departments, OR needs to be included in the command to satisfy query criteria. Using SQL filters we were able to identify all employees that are in the Finance and Sales departments. The following code was used retrieve the output:

* **SELECT** \* **FROM** employees **WHERE** department = ‘Finance’ **OR**  department = ‘Sales’;

## Retrieve all employees not in IT

The security team needs to perform an update to employee machines to employees in all other departments excluding the Information Technology department. The employees within the IT department have already had the update applied to their machines. To satisfy the query criteria, **NOT** needs to be implemented in the command. Using SQL filters, all employees in all other departments were identified. The following code was used retrieve the output:

* **SELECT** \* **FROM** employees **WHERE NOT** department = ‘Information Technology’;

## Summary

Using the proper SQL filters I was successful investigating failed login in attempts after hours, on specific dates, and outside of Mexico. I was also successful in retrieving multiple lists of employees in the Marketing, Finance, Sales, and all other departments within the organization that needed updates to their employee machines. The IT department did not need these updates due to the employees already having the update applied to their employee machines.