# Apply filters to SQL queries

## Project description

My organization is working to make their system more secure. I must investigate any 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 security incident that occurred after business hours (after 18:00) so all failed login attempts needed to be reviewed. I used the SELECT \* FROM log\_in\_attempts command to select all columns from the log\_in\_attempts table. Along with the WHERE login\_time > ’18:00:00’ AND success = 0; line to query all log in times after 6:00 pm that had a success of 0 or a failed log in attempt. The resulting lines are the output of that request.

A screen shot of a computer screen

Description automatically generated

## Retrieve login attempts on specific dates

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

I used the SELECT \* FROM log\_in\_attempts command to select all columns from the log\_in\_attempts table. Along with the WHERE login\_date = ‘2022-05-09’ OR login\_date = ‘2022-05-08’; command to filter all log in attempts using the two conditions of 2022-05-09 to filter all login attempts on that date as well as the second condition of 2022-05-08 to filter logins on 2022-05-08. The following lines are output of that request.A screen shot of a computer

Description automatically generated

## Retrieve login attempts outside of Mexico

After investigating the login attempts it was determined that the issue occurred outside of Mexico so those attempts should be investigated further.

I used the SELECT \* FROM log\_in\_attempts command to select all columns from the log\_in\_attempts table. Using the WHERE NOT to filter out countries other than Mexico. I used LIKE with‘MEX%’; to match all datasets since Mexico is represented as MEX and MEXICO. The percentage sign (%) represents any number of unspecified characters when used alongside LIKE. A screen shot of a computer

Description automatically generated

## Retrieve employees in Marketing

My team wanted to update computers for certain employees in the Marketing department. I needed to get information on which employees machines needed to update.

I used the SELECT \* FROM employees command to select all columns from the employees table. Using WHERE department = ‘Marketing’ AND office Like ‘East%’; allowed me to look at all employees in the department of Marketing along with the operator of LIKE and % allowed me to see the employees in the offices of the East building.

A screen shot of a computer program

Description automatically generated

## Retrieve employees in Finance or Sales

The machines for the employees in the Finance and Sales department also needed to be updated with a different security update. I had to pull information on the employees from only these two departments.

I used the SELECT \* FROM employees command to select all columns from the employees table. Using the WHERE department = ‘Finance’ OR department = ‘Sales’; allowed me to retrieve all employees in the finance or sales department. The resulting lines are the output from this query.

A screen shot of a computer

Description automatically generated

## Retrieve all employees not in IT

One more updated needed to be made on employees who are not part of the Information Technology department. I had to query for the information on these employees.

I used the SELECT \* FROM employees command to select all columns from the employees table. Along with the WHERE NOT department = ‘Information Technology’; The NOT operator gives me all departments that are not the Information Technology department.

## A screen shot of a computer Description automatically generatedSummary

I retrieved a list of failed log in attempts after hours. Due to a suspicious event that occurred on 5-9-22 I queried to review all log in attempts that occurred on the date of 5-9-22 and the day before of 5-8-22. Since the suspicious activity was determined to not be from Mexico I filtered out all Mexico log in attempts. Retrieved a list of employees machines from the Marketing department in the East building that needed security updates. Then retrieved another list of employees machines from the Finance and Sales departments that also needed security updates. One final update was needed that the IT department already received, so a list was made of all other employees who were not part of the IT department that needed this update.