# Apply filters to SQL queries

## Project description

You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines. Using various SQL statement I examine the organizations data to retrieve record and find potential security risks.

## Retrieve after hours failed login attempts

You recently discovered a potential security incident that occurred after business hours. To investigate this, you need to query the **log\_in\_attempts** table and review after hours login activity. Use filters in SQL to create a query that identifies all failed login attempts that occurred after 18:00.

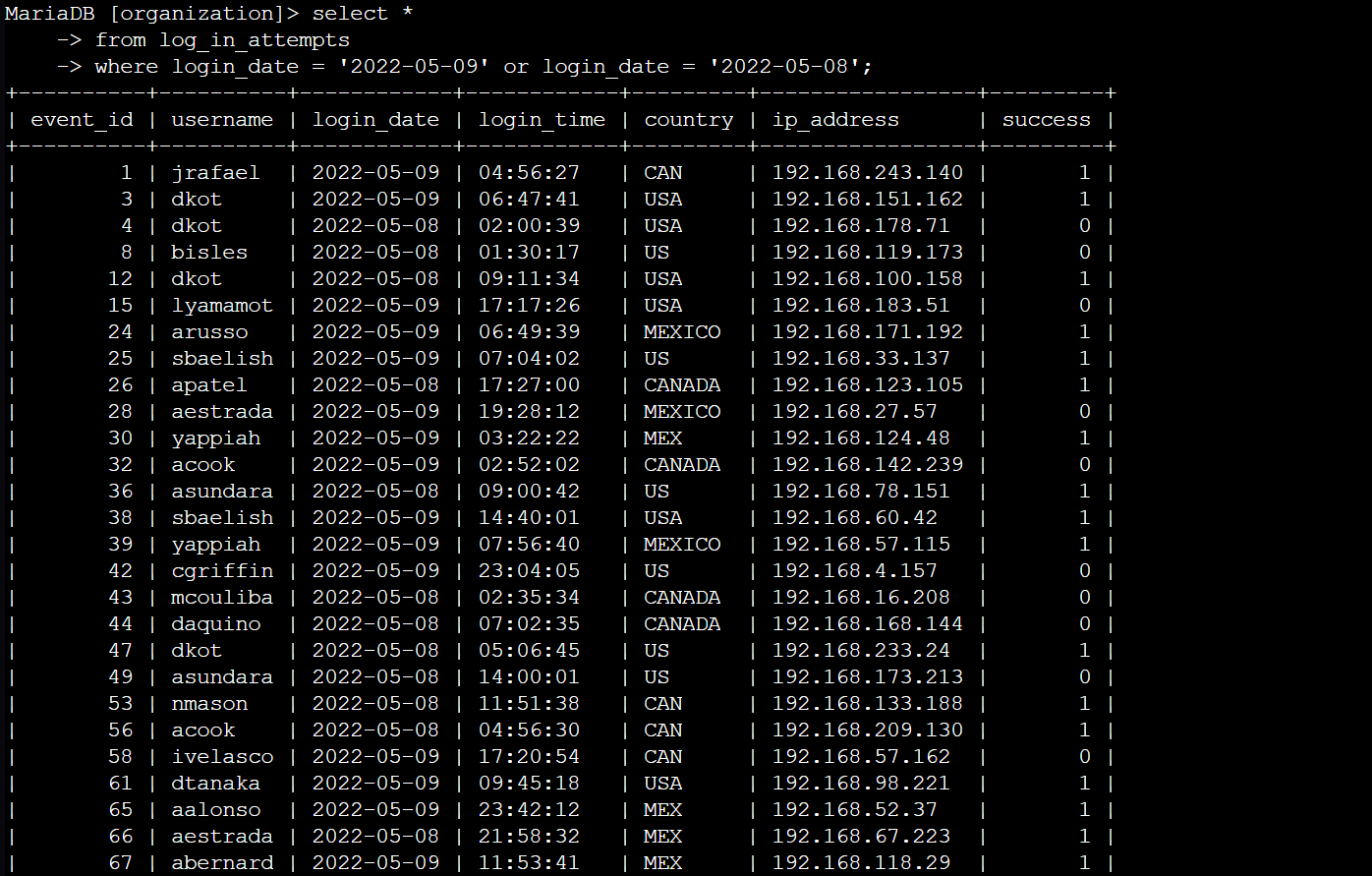
A screenshot of a computer screen

AI-generated content may be incorrect.

Using ‘select \*’ I query everything in the ‘log\_in\_attempts’ table. I then filter the table to only show logins that failed (which is shown be the 0 in the success column) and that happen after 18:00 hours.

## Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09. To investigate this event, you want to review all login attempts which occurred on this day and the day before. Use filters in SQL to create a query that identifies all login attempts that occurred on 2022-05-09 or 2022-05-08.



Using ‘select \*’ I query everything in the ‘log\_in\_attempts’ table. I then filter the table to only show logins that happened on ‘2022-05-09’ OR ‘2020-05-08’.

## 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. Now, you need to investigate login attempts that occurred outside of Mexico. Use filters in SQL to create a query that identifies all login attempts that occurred outside of Mexico.

A screen shot of a computer screen

AI-generated content may be incorrect.

Using ‘select \*’ I query everything in the ‘log\_in\_attempts’ table. I then filter the table to only show logins that are not from Mexico. I do that using ‘not’ and ‘like MEX%’ to tell the terminal to only print values where country does not start with ‘MEX’.

## Retrieve employees in Marketing

Your team wants to perform security updates on specific employee machines in the Marketing department. You’re responsible for getting information on these employee machines and will need to query the **employees** table. Use filters in SQL to create a query that identifies all employees in the Marketing department for all offices in the East building.

A screen shot of a computer

AI-generated content may be incorrect.

Using ‘select \*’ I query everything in the ‘employees’ table. I then filter the table to only show employees from the Marketing department who are also in the East wing.

## Retrieve employees in Finance or Sales

Your team now needs to perform a different security update on machines for employees in the Sales and Finance departments. Use filters in SQL to create a query that identifies all employees in the Sales or Finance departments.

A screenshot of a computer screen

AI-generated content may be incorrect.

Using ‘select \*’ I query everything in the ‘employees’ table. I then filter the table to only show employees from the Sales department or the Finance department.

## Retrieve all employees not in IT

Your team needs to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it. Use filters in SQL to create a query which identifies all employees not in the IT department.

A screen shot of a computer

AI-generated content may be incorrect.

Using ‘select \*’ I query everything in the ‘employees’ table. Then using ‘not’ I filter the table to show employees from every department except IT (or Information Technology).

## Summary

Using SQL statements such as ‘LIKE, AND, OR, and NOT’ allowed me to go through the organizations data more efficiently to find relevant data. I was able to find suspicious login attempts and get data on what machines the organization needed updates for, which should improve the organization security posture.