Apply filters to SQL queries

Project description

In this project, I worked as a security professional investigating suspicious login activity and employee machine information using SQL. I used filters like AND, OR, and NOT to find important data in the company's log_in_attempts and employees tables. These filters helped me look more closely at specific times, departments, and countries. This helped my team understand potential security risks and decide where updates were needed.

Retrieve after hours failed login attempts

```
SELECT *
FROM log_in_attempts
WHERE login_time > '18:00'
AND success = 0;
```

This SQL query finds all login attempts that happened after 6 PM and were not successful. It helps identify possible suspicious activity that occurred outside normal working hours.

Retrieve login attempts on specific dates

```
SELECT *
FROM log_in_attempts
WHERE login_date = '2022-05-09'
OR login_date = '2022-05-08';
```

We want to see login attempts from two specific days. The login_date = '2022-05-09' finds logins on May 9, and the OR login_date = '2022-05-08' finds ones from the day before.

Retrieve login attempts outside of Mexico

```
SELECT *
FROM log_in_attempts
WHERE country NOT LIKE '%MEX%';
```

This query helps us find login attempts that did not come from Mexico. The %MEX% part matches both "MEX" and "MEXICO",

Retrieve employees in Marketing

```
SELECT *
FROM employees
WHERE department = 'Marketing'
```

This query gets a list of all employees who work in the Marketing department. It's helpful for checking which employees belong to that specific team.

Retrieve employees in Finance or Sales

```
SELECT *
FROM employees
WHERE department = 'Finance'
OR department = 'Sales';
```

This query finds employees who are either in the Finance department or the Sales department. It's used to gather information about people in either of these two important business areas.

Retrieve all employees not in IT

```
SELECT *
FROM employees
WHERE department != 'Information Technology';
```

This query shows all employees who are not part of the Information Technology department. It helps to isolate employees from other departments for analysis or reporting.

Summary

In this activity, I used SQL to find failed login attempts after hours, look at logins from specific dates, and identify login locations outside Mexico. I also used SQL to find employee information based on their department and office locations. These queries helped simulate how a real security professional might investigate unusual activity and assist with system updates.