Project Description

This project demonstrates how I used SQL filtering techniques as a security analyst to analyze login records and employee data. By using SQL operators such as AND, OR, and NOT, along with LIKE and date/time filters, I identified potential security threats within the organization.

1. Retrieve failed login attempts after 6 PM

SQL:

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

Explanation: Filters records where login attempts failed (success = 0) and occurred after 6 PM.

2. Retrieve login attempts on May 8 or May 9, 2022

SQL:

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

Explanation: Selects login records that occurred on either of the two specific dates.

3. Retrieve login attempts not from Mexico

SQL:

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

Explanation: Excludes login records from Mexico using NOT LIKE with wildcard patterns.

4. Retrieve employees in Marketing and Eastern offices

SQL:

```
SELECT *
FROM employees
WHERE department LIKE '%Marketing%' AND office LIKE 'East%';
```

Explanation: Filters employees who are in the Marketing department and located in offices starting with 'East'.

5. Retrieve employees in Sales or Finance departments

SQL:

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

Explanation: Selects employees who work in either Sales or Finance departments.

6. Retrieve all employees not in IT department

SQL:

```
SELECT *
FROM employees
WHERE department NOT LIKE '%Information Technology%';
```

Explanation: Filters out employees from the IT department using the NOT LIKE operator.

Summary

I used SQL queries to detect failed login attempts after hours, investigate suspicious login activity by date and country, and identify employees needing security updates based on their department and office location. This exercise demonstrates the practical use of SQL for cybersecurity investigation and internal system monitoring.