Apply filters to SQL queries Report

Project description

In this project, I used SQL queries to investigate potential security issues related to login attempts and employee data. By applying filters such as `AND`, `OR`, `NOT`, `LIKE`, and date/time conditions, I was able to isolate specific events of interest. These queries demonstrate my ability to analyze large datasets for cybersecurity analysis and system integrity checks.

Retrieve after hours failed login attempts

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

Explanation:
This query selects all rows from the `log_in_attempts` table where the login occurred after 6:00 PM (18:00) and the login was **not successful** (`success = 0`). This helps identify unauthorized or suspicious access attempts happening after business hours.

Retrieve login attempts on specific dates

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

Explanation:
This query retrieves login attempts that happened on **either** May 8 or May 9, 2022. This is useful when investigating a specific suspicious event that occurred during those days.

Retrieve login attempts outside of Mexico

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

Explanation:
This query filters out any login attempts where the country column contains “MEX” or “MEXICO.” By using `NOT LIKE 'MEX%'`, we exclude both abbreviations and full names that reference Mexico, helping isolate external access sources.

Retrieve employees in Marketing

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

Explanation:
This query finds all employees in the **Marketing** department whose **office location starts with “East”** (like East-170, East-320, etc.). We use the `LIKE` keyword with `%` to capture partial matches in both columns.

Retrieve employees in Finance or Sales

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

Explanation:
This query selects all employees who work in **either** the Finance or Sales departments. The `OR` operator is used to include rows matching **any** of the conditions.

Retrieve all employees not in IT

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

Explanation:
This query filters out employees in the **Information Technology** department and selects all others. This is helpful when applying an update only to non IT staff.

Summary

In this project, I used SQL to perform targeted data analysis using a variety of filtering techniques including `AND`, `OR`, `NOT`, `LIKE`, and conditions based on dates and times. These

queries helped investigate login attempts, isolate suspicious access patterns, and organize employee data based on department and office location. The skills demonstrated here are fundamental to securing organizational systems and responding to potential security incidents using data analysis.