Apply Filters to SQL Queries

Portfolio Activity — File Permissions Investigation (Coursera)

Project description

In this project, I used SQL queries to investigate potential security issues related to employee login attempts. By applying filters with AND, OR, NOT, and LIKE operators, I retrieved specific records to analyze failed logins, suspicious login locations, and employee machine assignments. These SQL queries helped identify unusual login behavior, enforce access policies, and support security response actions.

Retrieve after-hours failed login attempts

SQL Query:

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

Explanation:

This query retrieves all failed login attempts (`success = 0`) that occurred after business hours (`login_time > '18:00:00'`). The AND operator ensures both conditions must be true.

Retrieve login attempts on specific dates

SQL Query:

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

Explanation:

This query uses OR to retrieve login attempts that occurred on either **2022-05-09** or **2022-05-08**, allowing investigation of potential activities around the suspicious event date.

Retrieve login attempts outside of Mexico

SQL Query:

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

Explanation:

The `NOT LIKE '%MEX%'` filter excludes all attempts where the country value contains **MEX** or **MEXICO**, helping locate login attempts originating outside of Mexico. The `%` wildcard allows matching partial text.

Retrieve employees in Marketing

SQL Query:

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

Explanation:

This query identifies employees in the **Marketing** department located in any **East building office**. The LIKE keyword with `%` matches patterns such as *Marketing Coordinators* or *East-170*, *East-320*, etc.

Retrieve employees in Finance or Sales

SQL Query:

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

Explanation:

This filters employees working in **Finance** or **Sales**, using OR to capture entries related to both departments.

Retrieve all employees not in IT

SQL Query:

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

Explanation:

This query retrieves employees from any department except **Information Technology**, using `NOT LIKE` to exclude IT staff from further updates.

Summary

In this activity, I used SQL to examine login attempts and employee records to investigate potential security incidents. Using filters with AND, OR, NOT, and LIKE, I isolated failed login attempts after hours, logins from outside Mexico, and account activity on suspicious dates. I also retrieved employee data based on department and office conditions. These SQL filtering techniques helped support access control, threat investigation, and incident response planning.