Apply Filters to SQL Queries

Project description

This project demonstrates how to use SQL filters to investigate login activity and employee department data in a security context. By filtering with AND, OR, NOT, and LIKE, we can extract relevant information from login and employee tables to support incident response and IT operations.

Retrieve after hours failed login attempts

SQL Query:

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

Explanation:
This query selects all records from the log_in_attempts table where the login_time is after 18:00 and the login attempt failed (success = 0). The AND operator ensures both conditions are true to identify potential after-hours suspicious activity.

Retrieve login attempts on specific dates

SQL Query:

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

Explanation:
This query retrieves all login attempts made on either May 8 or May 9, 2022. The OR operator is used to match either of the two specified dates in the login_date column.

Retrieve login attempts outside of Mexico

SQL Query:

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

Explanation:
This query finds login attempts that did not originate from Mexico. The NOT LIKE '%MEX%' condition filters out all entries that contain “MEX” or “MEXICO” in the country field.

Retrieve employees in Marketing

SQL Query:

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

Explanation:
This query identifies employees whose department includes “Marketing” and who work in the East building. The LIKE keyword with % is used to match values that contain “Marketing” and start with “East-”.

Retrieve employees in Finance or Sales

SQL Query:

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

Explanation:
This query filters for employees who are in either the Finance or Sales department. It uses the OR operator and the LIKE keyword to match partial text in the department column.

Retrieve all employees not in IT

SQL Query:

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

Explanation:
This query filters out employees in the Information Technology department by using NOT LIKE. It selects all others who still need the security update.

Summary

In this project, I used SQL to retrieve information about login activity and employee departments using filtering conditions. I applied filters using AND, OR, NOT, and LIKE to answer targeted security-related questions. These queries supported tasks such as identifying suspicious login times and locations, and filtering employees for IT updates by department.