Apply filters to SQL queries

Project description

Using SQL, I filtered data from tables to identify suspicious login attempts and retrieve information about employees in various departments. This activity demonstrates my ability to write complex SQL queries for data investigation, filtering based on dates, times, and string patterns using operators like `LIKE`, `AND`, `OR`, and `NOT`.

Retrieve after hours failed login attempts

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

This query selects all records from the `log_in_attempts` table where login attempts occurred after 18:00 and failed (indicated by `success = 0`). It's useful for investigating unusual login patterns after work hours.

Retrieve login attempts on specific dates

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

This query retrieves all login attempts that happened on May 8 and May 9, 2022, helping to pinpoint suspicious activity on these specific dates.

Retrieve login attempts outside of Mexico

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

The query retrieves login attempts that did not originate from Mexico, accounting for both "MEX" and "MEXICO" variations using the `NOT LIKE` keyword.

Retrieve employees in Marketing

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

This retrieves all employees in the Marketing department located in the East building, filtering based on department and office location using `LIKE`.

Retrieve employees in Finance or Sales

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

This identifies employees in the Finance or Sales departments, helping to isolate specific groups of employees for targeted security updates.

Retrieve all employees not in IT

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

This query finds all employees outside of IT, ensuring that updates are applied to other departments without redundancy.

Summary

"In this project, I identified patterns in login activity and gathered data on employees in specific departments. By using SQL filters, including `LIKE` for pattern matching, and conditional operators such as `AND`, `OR`, and `NOT`, I showcased my ability to extract relevant information from large datasets to support security investigations.