Portfolio piece #4. Apply filters to SQL queries

Project Description

As part of a cybersecurity team in a large organization, I investigated suspicious login attempts and employee access behavior. I used SQL to analyze data from the log_in_attempts and employees tables, looking for failed logins, unusual locations, and patterns tied to specific departments. This project showed my ability to use SQL operators like AND, OR, NOT, and LIKE to find meaningful insights and support security investigations.

Retrieve after-hours failed login attempts

```
Unset
Query:

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

Explanation: This query filters the log_in_attempts table to return all rows where the login attempt occurred after 6:00 PM ('18:00:00') and the login was unsuccessful (success = 0). This helps identify potentially suspicious activity after business hours.

Retrieve login attempts on specific dates

```
Unset
Query:

sql
Copy
Edit
SELECT *
FROM log_in_attempts
```

```
WHERE login_date = '2022-05-08'
   OR login_date = '2022-05-09';
```

Explanation: This query uses the OR operator to select all login attempts made on either May 8 or May 9, 2022. This helps investigate events around a specific suspicious date.

Retrieve login attempts from outside of Mexico

```
Unset
Query:

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

Explanation: This query filters out any login attempts where the country field includes "MEX" or "MEXICO", using NOT LIKE '%MEX%'. This helps isolate logins from outside Mexico for further investigation.

Retrieve employees in Marketing in the East building

```
Unset
Query:

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

Explanation: This query returns employees who are in the Marketing department and located in an office that starts with “East-”. The LIKE operator is used with 'East-%' to match any East building office.

Retrieve employees in Finance or Sales

```
Unset
Query:

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

Explanation: This query finds all employees who work in either the Finance or Sales departments. The OR operator lets us match both conditions.

Retrieve all employees not in IT

```
Unset
Query:

sql
Copy
Edit
SELECT *
FROM employees
WHERE department != 'Information Technology';
```

Explanation: This query uses != (or NOT) to exclude any employee in the Information Technology department, returning only those who still need the update.

Summary

In this project, I used SQL to filter and investigate security-related activity. By applying AND, OR, and NOT operators, I was able to identify failed login attempts outside business hours, activity on specific days, and employee access based on department and location. I also used the LIKE operator to match partial values for office and country data. These queries show how SQL can help spot potential cybersecurity risks and support smarter security decisions.