Apply filters to SQL queries

Project description

In this project, I used SQL queries to investigate potential security issues by filtering and retrieving data from the log_in_attempts and employees tables. This involved identifying failed login attempts, examining suspicious login dates, and gathering information on specific employees and departments.

Retrieve after hours failed login attempts

```
MariaDB [organization]> SELECT * FROM log_in_attempts WHERE login_time > '18:00' AND success = 0;
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |       0 |
```

This query selects all records from the `log_in_attempts` table where the `login_time` is after 18:00 and the `success` column is 0, indicating failed login attempts after business hours.

Retrieve login attempts on specific dates

```
MariaDB [organization]> SELECT * FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |       0 |
```

This query retrieves all login attempts from the `log_in_attempts` table that occurred on May 8th or May 9th, 2022, to investigate suspicious activity on these dates.

Retrieve login attempts outside of Mexico

```
MariaDB [organization]> SELECT * FROM log_in_attempts WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |       1 |
```

This query selects all login attempts from the `log_in_attempts` table where the `country` column does not start with "MEX," identifying login attempts originating outside of Mexico.

Retrieve employees in Marketing

```
MariaDB [organization]> SELECT * FROM employees WHERE department = 'Marketing' AND office LIKE 'East%';
+-------------+--------------+----------+------------+----------+
| employee_id | device_id    | username | department | office   |
+-------------+--------------+----------+------------+----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
```

This query retrieves all employees from the `employees` table who work in the Marketing department and have offices located in the East building, as identified by the `office` column starting with "East."

Retrieve employees in Finance or Sales

```
MariaDB [organization]> SELECT * FROM employees WHERE department = 'Finance' OR department = 'Sales';
+-------------+--------------+----------+------------+-------------+
| employee_id | device_id    | username | department | office      |
+-------------+--------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
```

This query selects all employees from the `employees` table who belong to either the Finance or Sales departments, as indicated by the `department` column.

Retrieve all employees not in IT

```
MariaDB [organization]> SELECT * FROM employees WHERE NOT department = 'Information Technology';
+-------------+--------------+----------+-----------------+-------------+
| employee_id | device_id    | username | department      | office      |
+-------------+--------------+----------+-----------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-276 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-434   |
```

This query retrieves all employees from the `employees` table who are not in the Information Technology department, ensuring they receive necessary updates.

Summary

This project involved using SQL queries to investigate security issues by filtering and retrieving data from the organization's `log_in_attempts` and `employees` tables. By applying specific filters, I was able to identify after-hours failed login attempts, investigate suspicious login dates, determine the origin of login attempts, and gather information on employees from various departments. This process is crucial for maintaining the security and integrity of the organization's systems.