Apply filters to SQL queries

Project description

In this task, I am responsible for detecting potential security threats by analyzing data from the "log_in_attempts" and "employees" tables. Using SQL queries, I extract specific information to identify unusual activities such as logins during non-working hours, access attempts on specific dates, unauthorized logins from outside Mexico, and employee records filtered by department and location.

Retrieve after hours failed login attempts

To analyze potential security incidents that occur late in the evening, I will use SQL to filter data from the "log_in_attempts" table. The objective is to identify all failed login attempts that happened after 8:00 PM (20:00).

```
SELECT *
FROM log_in_attempts
WHERE success = 0 AND TIME(login_time) > '20:00:00';
```

Retrieve login attempts on specific dates

To investigate a specific incident, I will run a SQL query on the "log_in_attempts" table to retrieve all login attempts that occurred on October 10 or October 11, 2025.

```
SELECT *

FROM log_in_attempts

WHERE login_date IN ('2025-10-10', '2025-10-11');
```

Retrieve login attempts outside of Mexico

To investigate suspicious login attempts originating outside of Mexico, I'll apply SQL filters to the log_in_attempts table. The goal is to retrieve all records where the country is not identified as "MEX" or "MEXICO".

```
SELECT *
```

```
FROM log_in_attempts

WHERE country NOT LIKE 'MEX%';
```

Retrieve employees in Marketing

To gather information on employees who work in the Marketing department and are located in the East building, I'll run a SQL query on the employees table with the appropriate filters.

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

Retrieve employees in Finance or Sales

To identify employees who work in either the Finance or Sales departments, I'll run a SQL query on the employees table that filters for those two departments.

```
SELECT *
FROM employees
WHERE department IN ('Finance', 'Sales');
```

Retrieve all employees not in IT

To generate a list of employees who are not part of the IT department, I'll run a query on the employees table that filters out anyone assigned to Information Technology.

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

Summary

By using targeted SQL queries, I performed a detailed review of several potential security concerns such as after-hours login attempts, unusual activity on specific dates, access from outside Mexico, and employee records filtered by department or location. These queries help strengthen the organization's security posture by pinpointing potential vulnerabilities and enabling timely corrective action.