Apply filters to SQL queries

Project description

Recently the security team has noticed that there have been multiple failed account logins and this could be due to a potential security issue. It's my job to sort and organize the data from the DB(database) to investigate a potential breach.

//This is just a scenario, no official events will be shared

Retrieve after hours failed login attempts

Login attempts outside of normal working hours are considered to be suspicious so it's best to start there. This can be done by entering this database request:

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

This here will show every login after 18:00(6 PM) that was unsuccessful

Retrieve login attempts on specific dates

According to the security team, the suspicious activity occurred on 2022-05-09. To ensure we have the necessary information, we will be querying for 2022-05-08 and 2022-05-09 dates for all login attempts between said dates

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

Retrieve login attempts outside of Mexico

Reports from the security team claim that the suspicious activity did NOT originate from Mexico. With this information we can narrow down the country search to get a cleaner picture of where the potential suspicious activity originates from

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

This will search the table for every country that isn't Mexico(DB sometimes stores Mexico as MEX and MEXICO, so a wildcard is used in conjunction with the LIKE call)

Retrieve employees in Marketing

The IT team has noticed that specific employee machines may need to have security updates, however they are unsure what ones need to be updated. It's our responsibility to provide a list of the machines that need to be updated to the IT department. These machines belong to the **marketing** department and are located in the **East** office.

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

Retrieve employees in Finance or Sales

In addition to the last IT team request, a different security update is required for other employees' machines. The IT team has requested that the machines from the **sales** and **finance** departments be updated and need a list of appropriate machines

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

Retrieve all employees not in IT

Lastly, the IT department needs to update all branches of the company EXCEPT the IT department itself(They already have the update) however they need a list of all machines they need to update

```
SELECT *
FROM employees
WHERE department <> 'Information Technology';
```

Summary

This is the end of the portfolio project, I always like working with SQL due to its ease of use and very clear syntax. I would love to work more with it and become a true database professional!