Apply filters to SQL queries

Project description

I am a security professional at a large organization. Part of my job is to investigate security issues to help keep the system secure. I recently discovered some potential security issues that involve login attempts and employee machines.

My task is to examine the organization's data in their employees and log_in_attempts tables. I will need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

Retrieve after-hours failed login attempts

A potential security incident occurred after business hours. To investigate this, I need to query the log_in_attempts table and review the after-hours login activity. I used filters in SQL to create a query that identifies all failed login attempts that occurred after 18:00.

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

Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09. To investigate this event, I want to review all login attempts which occurred on this day and the day before. I used filters in SQL to create a query that identifies all login attempts that occurred on 2022-05-09 or 2022-05-08.

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

Retrieve login attempts outside of Mexico

There’s been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. Now, I need to investigate login attempts that occurred outside of Mexico. I used filters in SQL to create a query that identifies all login attempts that occurred outside of Mexico.

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

Retrieve employees in Marketing

The team wants to perform security updates on specific employee machines in the Marketing department. I am responsible for getting information on these employee machines and will need to query the employees' table. I used filters in SQL to create a query that identifies all employees in the Marketing department for all offices in the East building.

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

Retrieve employees in Finance or Sales

The team now needs to perform a different security update on machines for employees in the Sales and Finance departments. I used filters in SQL to create a query that identifies all employees in the Sales or Finance departments.

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

Retrieve all employees not in IT

The team needs to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it. I used filters in SQL to create a query which identifies all employees not in the IT department.

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

Summary

As a security professional at a large organization, part of my responsibilities includes investigating security issues to ensure the system remains secure. In this assignment, I identified potential security concerns related to login attempts and employee machines.

To address these concerns, I analyzed data from the organization's **employees** and **log_in_attempts** tables using SQL queries such as `LIKE`, `WHERE`, and `OR`. My investigation involved applying SQL filters to retrieve relevant records, cross-referencing datasets, and extracting insights to uncover suspicious activity. This approach allowed me to systematically evaluate login patterns, detect anomalies, and identify potential vulnerabilities or unauthorized access attempts.

This analysis is an essential step in strengthening the organization's cybersecurity posture by proactively addressing potential risks.