Apply Filters to SQL Queries Portfolio

Name: Abubakari-Sadique Hamidu

Date: April 22, 2025

Course: Tools of the Trade (SQL)

Project Description

In this project, I took on the role of a security professional investigating potential login anomalies within a company. Using basic SQL commands and filtering techniques, I examined patterns in login attempts and employee department data. This allowed me to identify suspicious behaviors such as failed logins after work hours and access from unusual locations.

Step 1 - Filter Failed Logins

Used SQL to retrieve all failed login attempts for further analysis.

```
SELECT *
FROM log_in_attempts
WHERE status = 'failed';
```

Step 2 - Filter Logins from Mexico

Filtered login attempts that originated from Mexico.

```
SELECT *
FROM log_in_attempts
WHERE country = 'Mexico';
```

Step 3 - Review After-Hours Failed Logins

Filtered failed logins that occurred after 6 PM.

```
SELECT *
FROM log_in_attempts
WHERE status = 'failed' AND login_time > '18:00:00';
```

Step 4 - Retrieve Login Attempts on Specific Dates

Filtered all login attempts that occurred on March 1, 2023.

```
SELECT *
FROM log_in_attempts
WHERE login_date = '2023-03-01';
```

Step 5 - Retrieve Login Attempts Outside of Mexico

Retrieved login attempts not coming from Mexico using NOT.

```
SELECT *
FROM log_in_attempts
WHERE NOT country = 'Mexico';
```

Step 6 - Retrieve Employees in Marketing

Filtered for employees in the Marketing department.

```
SELECT *
FROM employees
WHERE department = 'Marketing';
```

Step 7 - Retrieve Employees in Finance or Sales

Filtered employees who are in either Finance or Sales.

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

Step 8 - Retrieve Employees NOT in IT

Used NOT to filter employees who are not in the IT department.

```
SELECT *
FROM employees
WHERE NOT department = 'IT';
```

Summary

This project highlights my ability to analyze cybersecurity-related data using SQL filters. By combining logical operators like AND, OR, and NOT, I was able to identify patterns and possible threats. The insights drawn from failed login attempts, departments, and locations provide valuable context for protecting digital assets.

Expected Results and Impact

Through these SQL queries, I expect to uncover suspicious login activities such as late-hour access and unrecognized geographic locations. This analysis is crucial in identifying potential breaches or policy violations. The ability to apply basic SQL in real-world security scenarios strengthens my role as a reliable entry-level cybersecurity professional and supports proactive threat mitigation.
