SQL Skills Report

Project Description

In this project, I assume the role of a security professional within a large organization, aiming to develop skills for investigating security issues and maintaining system security. The purpose is to identify and address potential security issues related to login attempts and employee machines. Through this case, I will apply specific SQL queries to examine and filter relevant data from the employees and log_in_attempts tables, demonstrating my ability to handle similar situations in a real environment.
Applied SQL Queries

Retrieve Failed Login Attempts After Hours

Problem/Need: A potential security incident has been detected outside normal working hours. To investigate, it is essential to identify all failed login attempts that occurred after 6:00 PM.

SQL Query:

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

Retrieve Login Attempts on Specific Dates

Problem/Need: A suspicious event was reported on May 9, 2022. To better understand the event, it's necessary to review login attempts that occurred on that day and the previous day.

SQL Query:

```
SELECT *
```

```
FROM log_in_attempts
WHERE login_date BETWEEN '2022-05-08' AND '2022-05-09';
```

Retrieve Login Attempts Outside of Mexico

Problem/Need: Suspicious login activity has been identified that did not originate in Mexico. The goal is to investigate login attempts that occurred outside Mexico to determine the source of the suspicious activity.

SQL Query:

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

Retrieve Employees in the Marketing Department

Problem/Need: The security team needs to implement updates on employee machines in the Marketing department. It is crucial to identify all these employees in the East Building offices.

SQL Query:

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

Retrieve Employees in Finance or Sales

Problem/Need: A security update on employee machines in the Sales and Finance departments is necessary. Therefore, these employees must be identified.

SQL Query:

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

Retrieve All Employees Not in IT

Problem/Need: For specific analysis, a list of all employees not in the Information Technology department is needed.

SQL Query:

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

Technical Details

Use of LIKE: The LIKE clause is used to search for a pattern within text. I used LIKE 'Mex%' to filter countries starting with "Mex," covering both "MEX" and "MEXICO."

Date and Time Filtering: I used BETWEEN to filter records between two specific dates and direct comparisons (>, <) for times, allowing for precise segmentation of temporal data.

Use of AND and OR: These clauses allow combining multiple conditions. AND was used to require both conditions to be true simultaneously, while OR allows any of the conditions to be true to include a record.

Use of NOT: NOT was used to exclude certain records, such as in NOT LIKE 'Mex%', ensuring that records not matching the given pattern are filtered out.

Summary

This report demonstrates my skills in applying effective SQL queries to investigate security issues within a simulated environment. Through the use of filtering techniques such as LIKE for pattern searches, temporal data management, and combining conditions with AND, OR, and NOT, I have developed a deep understanding of how to address potential security issues in an organization. These skills enable detailed and precise investigations for maintaining system security.