Project Description

In this project, I utilized SQL to investigate security incidents related to login attempts and employee devices. By applying various filters using AND, OR, and NOT operators, I aimed to retrieve critical information that could help identify potential security breaches within the organization.

Retrieve After Hours Failed Login Attempts

To identify failed login attempts that occurred after business hours (after 18:00), I executed the following SQL query:

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

This query retrieves all records from the log_in_attempts table where the login attempt failed (success = 0) and the time of the login attempt was after 18:00. The combination of conditions ensures that only relevant failed attempts are captured for further investigation.

Retrieve Login Attempts on Specific Dates

To find login attempts on specific dates, I used the following query:

```sql
SELECT *
FROM log_in_attempts
WHERE login_date = '2023-10-01';
```

This query filters the records to show only those login attempts that occurred on October 1, 2023.

Retrieve Login Attempts Outside of Mexico

To filter for login attempts that occurred outside of Mexico, I applied the following query:

```sql
```

SELECT *

FROM log_in_attempts

WHERE country != 'Mexico';

```

This query retrieves all records where the country is not Mexico, helping to focus on international login attempts.

**Retrieve Employees in Marketing**

To identify employees working in the Marketing department, I used:

```**sql**

SELECT *

FROM employees

WHERE department = 'Marketing';

```

This query lists all employees who are part of the Marketing team, providing insight into the personnel involved in that department.

**Retrieve Employees in Finance or Sales**

To find employees in either the Finance or Sales departments, I used the following query:

```**sql**

SELECT *

FROM employees

WHERE department = 'Finance' OR department = 'Sales';

```

This query effectively captures all employees in these two departments for analysis.

**Retrieve All Employees Not in IT**

To exclude employees in the IT department, I utilized:

```**sql**

SELECT *

FROM employees

WHERE department != 'IT';

```

This query retrieves all employees who do not belong to the IT department, which is essential for understanding the workforce outside of that technical area.

**Summary**

Through this project, I effectively applied SQL filtering techniques to analyze login attempts and employee data within the organization. By using AND, OR, and NOT operators, I could narrow down large datasets to obtain critical insights into potential security issues. This exercise not only strengthened my SQL skills but also provided practical experience in handling real-world data security investigations.

**Instructions for Including SQL Queries**

When presenting SQL queries in a portfolio, it's crucial to format them clearly. I used a monospaced font for better readability and included relevant comments to explain each section.

**Table Formats**

**1. log_in_attempts:**

- event_id
- username
- login_date
- login_time
- country
- ip_address
- success

2. **employees:**

- employee_id
- device_id
```

- username
- department
- office