Scenario

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

Your task is to examine the organization's data in their **`employees`** and **`log_in_attempts`** tables. You'll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

Table formats

This document describes how the tables used for this portfolio activity are organized. The `organization` database contains the following two tables:

- `log_in_attempts`
- `employees`

log_in_attempts

The `log_in_attempts` table has the following columns:

- `event_id`: The identification number assigned to each login event
- `username`: The username of the employee
- `login_date`: The date the login attempt was recorded
- `login_time`: The time the login attempt was recorded
- `country`: The country where the login attempt occurred
- `ip_address`: The IP address of that employee's machine
- `success`: The success of the login attempt; `FALSE` indicates a failed attempt

In the MariaDB shell, these columns are returned as:

```
+----------+----------+------------+------------+---------+-----------------+---------+
| event_id | username | login_date | login_time | country | ip_address      | success |
+----------+----------+------------+------------+---------+-----------------+---------+
```

employees

The `employees` table has the following columns:

- `employee_id`: The identification number assigned to each employee

- `device_id`: The identification number assigned to each device used by the employee
- `username`: The username of the employee
- `department`: The department the employee is in
- `office`: The office the employee is located in

In the MariaDB shell, these columns are returned as:

```
+-------------+-------------+----------+-----------------------+-------------+
| employee_id | device_id   | username | department            | office      |
+-------------+-------------+----------+-----------------------+-------------+
```

Apply filters to SQL queries

Project description

Recently, potential security issues have been identified that necessitate a thorough investigation. These issues are related to login attempts and employee machines, and this project aims to analyze the relevant data to uncover patterns, anomalies, and potential threats. Below I will just supply the command I would have used to complete the different tasks.

Retrieve after hours failed login attempts

```
SELECT * FROM log_in_attempts
WHERE login_time > "18:00" and success = 0;
```

Retrieve login attempts on specific dates

```
SELECT * FROM log_in_attempts
WHERE login_date = "2022-05-08" AND login_date = "2022-05-09";
```

Retrieve login attempts outside of Mexico

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

Retrieve employees in Marketing

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

Retrieve employees in Finance or Sales

```
SELECT *
FROM employees
WHERE department = "Finance" OR department = "Sales"
```

Retrieve all employees not in IT

```
SELECT *
FROM employees
WHERE NOT department = "Information Technology"
```

Summary

This project focuses on investigating potential security issues related to login attempts and employee machines by analyzing relevant data using SQL queries. The objective is to uncover patterns, anomalies, and potential threats to enhance the organization's security posture.