# 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.

# Apply filters to SQL queries

## Project description

Goal of the project is to practice filtering trough SQL database to access valuable information. In this scenario we will be investigating login attempts made by employers to see any malicious behavior.

## Retrieve after hours failed login attempts

I recently discovered potential security incident that occurred after business hours. To investigate that further we will review login attempts using SQL and filtering. Organization’s business hours end after 18:00.

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie

We know that we store login attempts in log\_in\_attempts table and column called login\_time stores time of login attemp. Column called success stores 0 or 1 values where 1 means successful attempt and 0 means failed attempt . We use command:

SELECT \* FROM log\_in\_attempts WHERE login\_time > ’18:00’ AND success = 0;

- **SELECT** - means from which column we return data, in this case each which is marked with "\*".

- **FROM** – means from which table we want to return data.

- **WHERE** – used to describe the conditions for filtering data.

- **AND** - means that both conditions must be met.

## Retrieve login attempts on specific dates

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

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

In this example we use similar command but instead of **AND** we use **OR** operator which means that from both conditions only one must be met.

## Retrieve login attempts outside of Mexico

Our security team found that suspicious login attempts originated outside of Mexico. We will filter SQL query to return only login attempts outside of Mexico. Here we must remember that columns contains value of MEX or Mexico which we must include in our filtering process

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

To include both MEX and MEXICO values we use LIKE and % operators.

When we use % which means that in its place we can put any characters. When we are using % we must use LIKE operator. For example:

SELECT fruit\_name FROM basket WHERE fruit LIKE ‘A%’ we will get values like apples, ananas.

## Retrieve employees in Marketing

Our team wants to perform security updates on specific employee machines in the Marketing department for all offices in the East building . We are responsible for getting information on these employee machines and will need to query the **employees** table. We will use filters in SQL to create a query that identifies all employees in the Marketing department for all offices in the East building.

Because East can mean very many things we again must filter our SQL query using “%”

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie

Here we combine knowledge from filtering through multiple possible values of column using % and combining conditions using **AND** operator

## Retrieve employees in Finance or Sales

In this example we are interested in returning value for Finance and Sales department. Our team needs to perform a different security update for these departments

## Obraz zawierający tekst, zrzut ekranu, oprogramowanie Opis wygenerowany automatycznie

Here we combine both conditions using **OR** operator to return data about employees from both departments.

## Retrieve all employees not in IT

Our team needs to make another update. This time we must focus only on departments outside of **Information Technology** departments which already implemented new security update. In this example we will use **NOT** operator to filter out all IT employees. Obraz zawierający tekst, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

## Summary

During this project we filtered through various login logs to analyze malicious behavior outside of business hours. Thanks to SQL filtering techniques like **AND, OR, LIKE, %** we extracted data we currently need. We also determined employees in many different departments quickly and without problems. SQL vastly enhances quality, precision and effectiveness of Security Analyst job.