**Apply filters to SQL queries**

**Project description**

I am a security professional at a large organization. My task is to examine the organization’s data in their *employees* and *log\_in\_attempts* tables. I will need SQL filters to retrieve records from different datasets and investigate the potential security issues.

**Retrieve after hours failed login attempts**

I will create a query that identifies all failed login attempts that occurred after 18:00.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

On the top part of the screenshot is my query. I selected all the data from *log\_in\_attempts* table. Then using SQL filtering I displayed the data I needed. Using *WHERE login\_time > ‘18’* I specified login attempts made after 18:00. Then using *AND* operator I made a second condition in which the login attempt is unsuccessful. I achieved this by command *success=FALSE;*

**Retrieve login attempts on specific dates**

A suspicious event occurred on 2022-05-09. Login activity registered on this date and the day before needs to be investigated.

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

To get login activity on these dates I used two conditions connected with *OR* operator. There first one is *login\_date=’2022-05-08’* and the second one is *login\_date=’2022-05-09’*. These two conditions helped me display a table with login attempts made only on these two dates.

**Retrieve login attempts outside of Mexico**

I became suspicious with activity login attempts but the security team determined that this activity didn’t originate in Mexico. I will investigate attempts made outside of Mexico.

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

To achieve this I needed to use command *WHERE NOT* which specifies all the attempts that does not fulfill the criteria. In this case it’s *country LIKE ‘MEX%’;.* The percentage character make us sure that we will not get any results with *MEX* as a beginning.

**Retrieve employees in Marketing**

Security team wants to perform security updates on specific employee machines in the Marketing department. I am responsible for getting information on these employee machines and will need to query the employees table. The Marketing department is placed in the East building.

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

I achieved this by selecting all data from *employees* table and making two conditions. The department value must have been equal to MARKETING. I made that with command *where department = ‘MARKETING’*. I connected this condition using operator AND with the second condition. *And office LIKE ‘East%’;.*

**Retrieve employees in Finance or Sales**

Security team now needs to perform a different security update on machines for employees in the Sales and Finance departments.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

I achieved this by selecting all data in employees table and again making two conditions connected with operator *OR*.

**Retrieve all employees not in IT**

Security team needs to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it. I will use filters in SQL to create a query which identifies all employees not in the IT department.

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

To display a table with results with department not equal to INFROMATION TECHNOLOGY I used a command *WHERE NOT department = ‘INFORMATION TECHNOLOGY’;.*

**Summary**

I created multiple queries using SQL. I got all the information I wanted. I worked on two different tables: *log\_in\_attempts* and *employees*. I used operators like *OR, AND, NOT*. I also used wildcard (‘%’) to filter for patterns.