Apply filters to SQL queries

Project description

[As a security analyst, my job is to ensure that the system is secure. SQL is important tool used to investigate security issues to help keep an organisation's sysytem secure. My task as a security analyst is to examine my organisation's data in their tables and then use SQL filters to retrieve records from different datasets and investigate the potential security issues. ]

Retrieve after hours failed login attempts

[A potential security incident was discovered after business hours which ends at 6pm. I queried the log\_in\_attempts to review after hours login activity using SQL filters to identify all failed login attempts That occured after 6pm (18:00). The time of the login attempts is found in the login\_time column. The success column contains a value of 0 when a login attempt failed.

The SQL filter used is as shown below;

**SELECT \***

**FROM** log\_in\_attempts

**WHERE** login\_time > '18:00' AND success = FALSE;



Retrieve login attempts on specific dates

[A suspicious event occurred on 2022-05-09. The SQL filter used to create a query that identify all login attempts that occurred on 2022-05-09 or 2022-05-08 is as shown below;

**SELECT \***

**FROM** log\_in\_attempts

**WHERE** login\_date = '2022-05-08' OR login\_date = '2022-05-09';

Retrieve login attempts outside of Mexico

[**SELECT \***

**FROM** log\_in\_attempts

**WHERE NOT** country LIKE 'MEX%';

The \* sign means to select all the columns in the table. The LIKE operator is used to filter for patterns in columns. The % symbol is a wildcard. The wildcard is a special character that can be substituted with another character. In this case the country column has both MEX and MEXICO. Therefore the % symbol placed after MEX returns all possible characters that start with MEX]

Retrieve employees in Marketing

[My team wants to perform security updates on specific employee machines in the Marketing department. The SQL filter is used to create a query that identifies all employees in the Marketing department for all offices in the East Building

**SELECT \***

**FROM** employees

**WHERE** department = 'Marketing' AND office LIKE 'East%'; ]

Retrieve employees in Finance or Sales

[A security updates needs to be performed for employees in the Sales and Finance departments.

**SELECT \***

**FROM** employees

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

Retrieve all employees not in IT

[The SQL filter shown below create a query which identifies all employees not in the IT department. The department of the employee is found in the department column which contains values that include Information Technology

**SELECT \***

**FROM** employees

**WHERE NOT** department = 'Information Technology'; ]

Summary

[Each of the queries created illustrates how I used SQL filters to examine an organisation's data and investigate to retrieve records from different datasets and investigate the potential security issues. What I accomplished through the use of SQL is to provide relevant information which is used in investigating security issues in order to ensure the digital safety of the organisation I work with.