Apply filters to SQL queries

Project description

Using the SQL through Linux bash shell to access the MariaDB, dataset named ”organization” to perform this SQL practice.

This scenario, my team retrieve information about employees, their machines, and their department to investigate potential security issues, and update the computers.

Retrieve after hours failed login attempts

I check the failed log in attempts made after business hour: 18:00, using condition of login_time > “18:00” and success = 0 because
MySQL stores successful and failed log in attempts as 1 and 0 respectively.

```
MariaDB [organization]> select * from log_in_attempts where login_
time > "18:00" and success = 0 order by login_date;
+----------+----------+------------+------------+---------+-------
----------+---------+
| event_id | username | login_date | login_time | country | ip_add
ress      | success |
+----------+----------+------------+------------+---------+-------
----------+---------+
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.16
8.132.153 |       0 |
|      131 | bisles   | 2022-05-09 | 20:03:55   | US      | 192.16
8.113.171 |       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.16
8.27.57   |       0 |
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.16
8.70.122  |       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.16
8.4.157   |       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN     | 192.16
8.84.194  |       0 |
|      160 | jclark   | 2022-05-10 | 20:49:00   | CANADA  | 192.16
8.214.49  |       0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.16
8.76.27   |       0 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.16
8.205.12  |       0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN     | 192.16
8.58.57   |       0 |
|      199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.16
8.44.232  |       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.16
8.66.142  |       0 |
```

Retrieve login attempts on specific dates

The second scenario is, my team is investigating a suspicious event occurred in 2022-05-09, we are checking the log in attempts from 8/5 - 9/5.
I use or operator to prevent misleading when using and and between and.

```
MariaDB [organization]> select * from log_in_attempts where login_
date =  "2022-05-08" or login_date = "2022-05-09" order by login_d
ate;
+----------+----------+------------+------------+---------+-------
----------+---------+
| event_id | username | login_date | login_time | country | ip_add
ress      | success |
+----------+----------+------------+------------+---------+-------
----------+---------+
|      117 | bsand    | 2022-05-08 | 00:19:11   | USA     | 192.16
8.197.187 |       0 |
|       56 | acook    | 2022-05-08 | 04:56:30   | CAN     | 192.16
8.209.130 |       1 |
|      169 | alevitsk | 2022-05-08 | 08:10:43   | CANADA  | 192.16
8.210.228 |       0 |
|      168 | jlansky  | 2022-05-08 | 13:25:42   | USA     | 192.16
8.210.94  |       1 |
|       66 | aestrada | 2022-05-08 | 21:58:32   | MEX     | 192.16
8.67.223  |       1 |
|      165 | jreckley | 2022-05-08 | 15:28:43   | MEXICO  | 192.16
8.34.193  |       0 |
|       68 | mrah     | 2022-05-08 | 17:16:13   | US      | 192.16
8.42.248  |       1 |
|      163 | tmitchel | 2022-05-08 | 09:21:16   | MEX     | 192.16
8.119.29  |       0 |
|       80 | cjackson | 2022-05-08 | 02:18:10   | CANADA  | 192.16
8.33.140  |       1 |
|       83 | lrodriqu | 2022-05-08 | 08:10:23   | USA     | 192.16
8.67.69   |       1 |
```

Retrieve login attempts outside of Mexico

My team is investigating log attempts not originate from Mexico. I use like “MEX%” to include terms of MEX and MEXICO, to select login attempts outside of Mexico.

```
MariaDB [organization]> select * from log_in_attempts where not co
untry like "MEX%" order by login_date;
+----------+----------+------------+------------+---------+-------
----------+---------+
| event_id | username | login_date | login_time | country | ip_add
ress      | success |
+----------+----------+------------+------------+---------+-------
----------+---------+
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.16
8.132.153 |       0 |
|      184 | alevitsk | 2022-05-08 | 03:09:48   | CAN     | 192.16
8.33.70   |       0 |
|       80 | cjackson | 2022-05-08 | 02:18:10   | CANADA  | 192.16
8.33.140  |       1 |
|       36 | asundara | 2022-05-08 | 09:00:42   | US      | 192.16
8.78.151  |       1 |
|      117 | bsand    | 2022-05-08 | 00:19:11   | USA     | 192.16
8.197.187 |       0 |
|      189 | nmason   | 2022-05-08 | 05:37:24   | CANADA  | 192.16
8.168.117 |       1 |
|       44 | daquino  | 2022-05-08 | 07:02:35   | CANADA  | 192.16
8.168.144 |       0 |
|      101 | sbaelish | 2022-05-08 | 12:01:22   | US      | 192.16
8.145.158 |       0 |
|      191 | cjackson | 2022-05-08 | 06:46:07   | CANADA  | 192.16
8.7.187   |       0 |
|       47 | dkot     | 2022-05-08 | 05:06:45   | US      | 192.16
```

Retrieve employees in Marketing

My team is updating employee's machine, we get information of all employees from Marketing department who locates in the east office using where department = "Marketing", and office like "East%". Use East% to select office code starts with East

```
MariaDB [organization]> select * from employees where department =
 "Marketing" and office like "East%";
+-------------+--------------+----------+------------+----------+
| employee_id | device_id    | username | department | office   |
+-------------+--------------+----------+------------+----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267 |
|        1088 | k8651965m233 | rgosh    | Marketing  | East-157 |
|        1103 | NULL         | randerss | Marketing  | East-460 |
|        1156 | a184b775c707 | dellery  | Marketing  | East-417 |
|        1163 | h679i515j339 | cwilliam | Marketing  | East-216 |
+-------------+--------------+----------+------------+----------+
7 rows in set (0.024 sec)
```

Retrieve employees in Finance or Sales

My team is performing a different updates to employees from finance and sales department, I use or to select data from both departments.

```
MariaDB [organization]> select * from employees where department =
 "Finance" or department = "Sales";
+-------------+-------------+----------+------------+------------
-+
| employee_id | device_id    | username | department | office
 |
+-------------+-------------+----------+------------+------------
-+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153
 |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406
 |
|        1008 | i858j583k571 | abernard | Finance    | South-170
 |
|        1009 | NULL         | lrodriqu | Sales      | South-134
 |
|        1010 | k2421212m542 | jlansky  | Finance    | South-109
 |
|        1011 | l748m120n401 | drosas   | Sales      | South-292
 |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271
 |
|        1017 | r550s824t230 | jclark   | Finance    | North-188
 |
|        1018 | s310t540u653 | abellmas | Finance    | North-403
 |
|        1022 | w237x430y567 | arusso   | Finance    | West-465
 |
|        1024 | y976z753a267 | iuduike  | Sales      | South-215
 |
|        1025 | z381a365b233 | jhill    | Sales      | North-115
 |
|        1029 | d336e475f676 | ivelasco | Finance    | East-156
 |
```

Retrieve all employees not in IT

Updates to the computer is already made in IT department, I sort data to select all departments except IT department with the not command.

```
MariaDB [organization]> select * from employees where not departme
nt = "Information Technology";
+-------------+-------------+----------+-----------------+-------
------+
| employee_id | device_id    | username | department      | office
     |
+-------------+-------------+----------+-----------------+-------
------+
|        1000 | a320b137c219 | elarson  | Marketing       | East-1
70    |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Centra
l-276 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-
434   |
|        1003 | d394e816f943 | sgilmore | Finance         | South-
153   |
|        1004 | e218f877g788 | eraab    | Human Resources | South-
127   |
|        1005 | f551g340h864 | gesparza | Human Resources | South-
366   |
|        1007 | h174i497j413 | wjaffrey | Finance         | North-
406   |
|        1008 | i858j583k571 | abernard | Finance         | South-
170   |
|        1009 | NULL         | lrodriqu | Sales           | South-
134   |
|        1010 | k242l212m542 | jlansky  | Finance         | South-
109   |
|        1011 | l748m120n401 | drosas   | Sales           | South-
292   |
|        1015 | p611q262r945 | jsoto    | Finance         | North-
271   |
```

Summary

I practice to maintain security of workplace by - checking suspicious log in attempts on regular basis, doing post-work to find source of security incidents, lowering security risk by updating computers of specific employees by using commands including select, from, where, and, or, and not, e.t.c..