Apply filters to SQL queries

Project description

My task is to analyze the organization's data in the employees and log_in_attempts tables. I will use SQL filters to retrieve records from these datasets. The goal is to investigate potential security issues.

Retrieve after hours failed login attempts

Suspicious activities occurred after business hours, specifically after 18:00. All failed login attempts during this time require investigation. I developed a SQL query in MariaDB to filter for these failed login attempts.

```
MariaDB [organization]> select * from log_in_attempts where login_time > '18:00' a
nd success = false;
+----------+----------+------------+------------+---------+-----------------+-----
----+
| event_id | username | login_date | login_time | country | ip_address      | succ
ess |
+----------+----------+------------+------------+---------+-----------------+-----
----+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |
  0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142  |
  0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50  |
  0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |
  0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93   |
  0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157   |
  0 |
|       52 | cjackson | 2022-05-10 | 22:07:07   | CAN     | 192.168.58.57   |
  0 |
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA     | 192.168.100.17  |
  0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX     | 192.168.234.49  |
  0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.168.132.153 |
  0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN     | 192.168.84.194  |
  0 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US      | 192.168.96.200  |
  0 |
|      107 | bisles   | 2022-05-12 | 20:25:57   | USA     | 192.168.116.187 |
  0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.168.76.27   |
  0 |
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122  |
  0 |
|      131 | bisles   | 2022-05-09 | 20:03:55   | US      | 192.168.113.171 |
  0 |
|      155 | cgriffin | 2022-05-12 | 22:18:42   | USA     | 192.168.236.176 |
  0 |
|      160 | jclark   | 2022-05-10 | 20:49:00   | CANADA  | 192.168.214.49  |
```

The results come from the log_in_attempts table, focusing on records where the login_time is after 18:00 and the login attempts are marked as failed (0). The * command retrieves all columns from this table. A status of zero indicates a failure, while one indicates success. Consequently, there were 19 failed login attempts after 18:00.

Retrieve login attempts on specific dates

A suspicious event took place on May 9, 2022. My duties require investigating any login activity from that day and the day before. I constructed a SQL query to filter login attempts for these specific dates.

```
MariaDB [organization]> select * from log_in_attempts where login_date = '2022-0
5-09' or login_date = '2022-05-08';
+----------+----------+------------+------------+---------+-----------------+---
------+
| event_id | username | login_date | login_time | country | ip_address      | su
ccess |
+----------+----------+------------+------------+---------+-----------------+---
------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |
    1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |
    1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |
    0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |
    0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |
    1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.51  |
    0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.192 |
    1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.137  |
    1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.105 |
    1 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57   |
    0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.48  |
    1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.239 |
    0 |
|       36 | asundara | 2022-05-08 | 09:00:42   | US      | 192.168.78.151  |
    1 |
|       38 | sbaelish | 2022-05-09 | 14:40:01   | USA     | 192.168.60.42   |
    1 |
|       39 | yappiah  | 2022-05-09 | 07:56:40   | MEXICO  | 192.168.57.115  |
    1 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157   |
```

```
    0 |
|       189 | nmason    | 2022-05-08 | 05:37:24   | CANADA  | 192.168.168.117 |
    1 |
|       190 | jsoto     | 2022-05-09 | 05:09:21   | USA     | 192.168.25.60   |
    0 |
|       191 | cjackson  | 2022-05-08 | 06:46:07   | CANADA  | 192.168.7.187   |
    0 |
|       193 | lrodriqu  | 2022-05-08 | 07:11:29   | US      | 192.168.125.240 |
    0 |
|       197 | jsoto     | 2022-05-08 | 09:05:09   | US      | 192.168.36.21   |
    0 |
+-----------+-----------+------------+------------+---------+-----------------+---
------+
75 rows in set (0.001 sec)

MariaDB [organization]>
```

I queried the log_in_attempts table using specific filtering criteria. By employing the where clause in conjunction with the or operator, I narrowed down the results to display only the login attempts that took place on either May 5, 2022, or May 8, 2022. The query revealed that a total of 75 login attempts were recorded across these two dates.

Retrieve login attempts outside of Mexico

After analyzing the data and patterns, there is strong evidence that login attempts from outside Mexico should be investigated. I have created a SQL query to filter and identify these login attempts for further review.

```
MariaDB [organization]> select * from log_in_attempts where not country like 'me
x%';
+----------+----------+------------+------------+---------+----------------+---
------+
| event_id | username | login_date | login_time | country | ip_address     | su
ccess |
+----------+----------+------------+------------+---------+----------------+---
------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.140 |
    1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |
    0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.162 |
    1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |
    0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |
    0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.243 |
    1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |
    0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.221 |
    0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.81  |
    0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.158 |
    1 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.135 |
    1 |
```

```
|       188 | jsoto    | 2022-05-11 | 00:39:09   | USA     | 192.168.21.88   |
|     0 |
|       189 | nmason   | 2022-05-08 | 05:37:24   | CANADA  | 192.168.168.117 |
|     1 |
|       190 | jsoto    | 2022-05-09 | 05:09:21   | USA     | 192.168.25.60   |
|     0 |
|       191 | cjackson | 2022-05-08 | 06:46:07   | CANADA  | 192.168.7.187   |
|     0 |
|       192 | bisles   | 2022-05-10 | 08:32:03   | USA     | 192.168.201.40  |
|     1 |
|       193 | lrodriqu | 2022-05-08 | 07:11:29   | US      | 192.168.125.240 |
|     0 |
|       194 | jclark   | 2022-05-12 | 14:11:04   | CAN     | 192.168.197.247 |
|     0 |
|       195 | alevitsk | 2022-05-11 | 06:59:13   | CANADA  | 192.168.236.78  |
|     1 |
|       196 | acook    | 2022-05-10 | 09:56:48   | CAN     | 192.168.52.90   |
|     0 |
|       197 | jsoto    | 2022-05-08 | 09:05:09   | US      | 192.168.36.21   |
|     0 |
|       200 | jclark   | 2022-05-12 | 01:11:45   | CANADA  | 192.168.91.103  |
|     1 |
+----------+----------+------------+------------+---------+-----------------+---
------+
144 rows in set (0.031 sec)
```

To filter out login attempts from Mexico, I employed the `where` clause with the `not` operator. Considering variations like "Mex" or "MEX", I opted for the like operator with the pattern `mex%`. This approach captures all Mexico-related entries, regardless of capitalization or full spelling. The % wildcard accommodates any additional characters. This query revealed 144 login attempts originating outside Mexico.

Retrieve Employees in Marketing

My team intends to update certain computers in various departments. I wrote a SQL query to identify employee machines used by staff in the Marketing department in the East building.

```
MariaDB [organization]> select * from employees;
+-------------+--------------+----------+-----------------------+-------------+
| employee_id | device_id    | username | department            | office      |
+-------------+--------------+----------+-----------------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing             | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing             | Central-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   |
|        1006 | g329h357i597 | alevitsk | Information Technology | East-320    |
|        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   |
|        1012 | m756n668o146 | nmason   | Information Technology | North-160   |
|        1013 | n205o559p243 | zbernal  | Information Technology | South-229   |
|        1014 | NULL         | asundara | Information Technology | West-219    |
|        1015 | p611q262r945 | jsoto    | Finance               | North-271   |
|        1016 | q793r736s288 | sbaelish | Human Resources       | North-229   |
|        1017 | r550s824t230 | jclark   | Finance               | North-188   |
|        1018 | s310t540u653 | abellmas | Finance               | North-403   |
```

```
|        1189 | h784i120j837 | slefkowi | Human Resources | West-342    |
|        1190 | NULL         | kcarter  | Marketing       | Central-270 |
|        1191 | NULL         | shakimi  | Marketing       | Central-366 |
|        1194 | m340n287o441 | zwarren  | Human Resources | West-212    |
|        1195 | n516o853p957 | orainier | Finance         | East-346    |
|        1198 | q308r573s459 | jmartine | Marketing       | South-117   |
|        1199 | r520s571t459 | areyes   | Human Resources | East-100    |
+-------------+--------------+----------+-----------------+-------------+
161 rows in set (0.001 sec)

MariaDB [organization]>
```

I began by retrieving all data from the employee table. Then, I applied a where clause with the not operator to exclude employees working in the IT department from the results.

```
MariaDB [organization]> select * from employees where department = 'marketing' a
nd 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 (0.002 sec)
```

Retrieve employees in Finance or Sales

There is a significant amount of employee data that needs updating across departments. I wrote a SQL query to filter for employee machines used by staff in the Finance or Sales 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   |
```

```
|        1176 | u849v569w521 | nliu      | Sales       | West-220    |
|        1181 | z803a233b718 | sessa     | Finance     | South-207   |
|        1185 | d790e839f461 | revens    | Sales       | North-330   |
|        1186 | e281f433g404 | sacosta   | Sales       | North-460   |
|        1187 | f963g637h851 | bbode     | Finance     | East-351    |
|        1188 | g164h566i795 | noshiro   | Finance     | West-252    |
|        1195 | n516o853p957 | orainier  | Finance     | East-346    |
+-------------+--------------+-----------+-------------+-------------+
71 rows in set (0.001 sec)

MariaDB [organization]>
```

I selected the Finance department and Sales department. By using the `where` clause and `or` operator I altered the outputs to make sure all employees who are members of both departments are listed. As a result, there are 71 people who happen to be members of both departments.

Retrieve all employees not in IT

I wrote a SQL query. The query filters for employee machines. It excludes employees in the Information Technology department.

```
MariaDB [organization]> select * from employees where not department = 'informat
ion technology';
+-------------+--------------+----------+-----------------+-------------+
| employee_id | device_id    | username | department      | office      |
+-------------+--------------+----------+-----------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-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 | k2421212m542 | jlansky  | Finance         | South-109   |
|        1011 | l748m120n401 | drosas   | Sales           | South-292   |
|        1188 | g164h566i795 | noshiro  | Finance         | West-252    |
|        1189 | h784i120j837 | slefkowi | Human Resources | West-342    |
|        1190 | NULL         | kcarter  | Marketing       | Central-270 |
|        1191 | NULL         | shakimi  | Marketing       | Central-366 |
|        1194 | m340n287o441 | zwarren  | Human Resources | West-212    |
|        1195 | n516o853p957 | orainier | Finance         | East-346    |
|        1198 | q308r573s459 | jmartine | Marketing       | South-117   |
|        1199 | r520s571t459 | areyes   | Human Resources | East-100    |
+-------------+--------------+----------+-----------------+-------------+
161 rows in set (0.001 sec)

MariaDB [organization]>
```

I began by selecting all data from the employee table. Next, I applied a `where` clause. I used the `not` operator in this clause. This filtered out employees in the IT department.

Summary

I applied filters to SQL queries. These queries targeted the `employee` and `log_in_attempts` tables. I used `and`, `or`, and `not` operators for specific filtering. `like` and the `%` wildcard helped me filter for patterns. These methods allowed me to extract precise information.