Apply filters to SQL queries

Project description

The following examples demonstrate how I used SQL to update computers, investigate potential security issues and make sure I do my job in a way that aligns with my companies interests.

Retrieve after hours failed login attempts

To investigate a potential security issue after hours I used the following SQL code to look into after hours log in attempts.

```
MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_time > '18:00' AND success = FALSE;
+----------+----------+------------+------------+---------+-----------------
------+
| event_id | username | login_date | login_time | country | ip_address
ccess |
+----------+----------+------------+------------+---------+-----------------
------+
|        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 |
```

Using WHERE and FALSE allows me to filter my results to find the failed login attempts I am looking for.

Retrieve login attempts on specific dates

Suspicious login activity occurred on the date 5/9/22 so activity on said day and the day before were investigated.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
+----------+----------+------------+------------+---------+-----------------
------+
| event_id | username | login_date | login_time | country | ip_address
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 |
```

Retrieve login attempts outside of Mexico

After further investigation it appeared there was suspicious activity outside of Mexico. So the results were filtered to return all attempts not including Mexico.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+-----------------
------+
| event_id | username | login_date | login_time | country | ip_address
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 |
```

Retrieve employees in Marketing

The team needs to update certain computers for employees in marketing so after finding out relevant info I refined my search to include the employees I need.

```
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 |
+-------------+-------------+----------+------------+----------+
```

Retrieve employees in Finance or Sales

Employees in Finance and Sales also needed updates so a new search was used to include these employees.

```
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 |
```

Retrieve all employees not in IT

A new update needs to go out to everyone that is not a part of IT. The screenshot below demonstrates the SQL filtering used to exclude the IT department from the returned results.

```
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE NOT department = 'Information Technology';
+-------------+--------------+----------+----------------+
| employee_id | device_id    | username | department     |
+-------------+--------------+----------+----------------+
|        1000 | a320b137c219 | elarson  | Marketing      |
|        1001 | b239c825d303 | bmoreno  | Marketing      |
|        1002 | c116d593e558 | tshah    | Human Resources
```

Summary

By using different SQL operators I was able to refine my searches to include suspicious login activity, look up specific departments, exclude specific criteria, and look up activity on specific dates.