SQL Security Log Analysis

Applying AND, OR, and NOT Filters for Security Investigations

Prepared by: Sambou Kamissoko - LinkedIn: https://www.linkedin.com/in/sambouk/
Project – Cybersecurity / Security Analysis

Project Description

This project demonstrates the use of SQL to investigate potential security incidents by analyzing authentication logs and employee data. Using logical operators (AND, OR, NOT), pattern matching (LIKE), and date/time filtering, I examined login activity to identify suspicious behavior and support security response efforts.

The goal of this analysis is to simulate real-world security investigations such as detecting after-hours access attempts, reviewing anomalous login patterns, and identifying affected employee groups for system updates or remediation.

Environment & Data Sources

The analysis was performed using a MariaDB database containing the following tables:

- **log_in_attempts** – Records authentication attempts, including login date, login time, country, IP address, and success status.
- **employees** – Stores employee information such as department, office location, and assigned devices.
- **machines** – Contains device information including operating system and patch status.

These datasets reflect the types of data commonly reviewed during security monitoring, incident response, and internal audits.

After-Hours Failed Login Attempts

Objective

Identify failed login attempts that occurred after normal business hours, which may indicate brute-force attempts or unauthorized access.

SQL Query

```
SELECT *
FROM log_in_attempts
WHERE login_time > '18:00:00'
  AND success = 0;
```

Explanation

This query filters login attempts that occurred after 6:00 PM and were unsuccessful. The AND operator ensures both conditions are met, allowing the analyst to focus on potentially suspicious activity outside standard working hours.

Login Attempts on Specific Dates

Objective

Review login activity that occurred on May 8 and May 9, 2022, following a reported security concern.

SQL Query

```
SELECT *
FROM log_in_attempts
WHERE login_date = '2022-05-09'
   OR login_date = '2022-05-08';
```

Explanation

The OR operator allows retrieval of login attempts from multiple dates. This type of filtering is commonly used during incident investigations to narrow activity to a known timeframe.

Login Attempts Outside of Mexico

Objective

Identify login attempts that did not originate in Mexico after determining suspicious activity was coming from other locations.

SQL Query

```
SELECT *
FROM log_in_attempts
```

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

Explanation

The LIKE 'MEX%' condition matches both MEX and MEXICO. Using NOT excludes those values, allowing the analyst to focus on login attempts originating outside of Mexico.

Employees in Marketing (East Building)

Objective

Identify employees in the Marketing department located in the East building for targeted security updates.

SQL Query

```
SELECT *
FROM employees
WHERE department = 'Marketing'
  AND office LIKE 'East-%';
```

Explanation

This query uses the AND operator to combine department and office location filters. The LIKE operator enables pattern matching across all East building offices.

Employees in Finance or Sales

Objective

Retrieve employee records for individuals in the Finance or Sales departments who require a security update.

SQL Query

```
SELECT *
FROM employees
WHERE department = 'Finance'
   OR department = 'Sales';
```

Explanation

The OR operator retrieves records from either department, supporting department-wide security actions.

Employees Not in Information Technology

Objective

Identify employees who still require a security update because IT staff were already patched.

SQL Query

```
SELECT *
FROM employees
WHERE NOT department = 'Information Technology';
```

Explanation

This query excludes IT employees, ensuring that updates are applied only to departments that still require remediation.

Security Relevance

This analysis demonstrates how SQL is used in cybersecurity roles to:

- Investigate authentication failures
- Detect anomalous login behavior
- Filter large datasets efficiently during incidents
- Support access reviews and patch management
- Assist SOC and incident response workflows

Summary

In this project, I applied SQL filtering techniques to analyze login attempts and employee records in a security focused scenario. By using logical operators, pattern matching, and date/time filters, I identified suspicious access attempts and isolated affected users and systems.

Appendix: SQL Query Screenshots

This section contains screenshots of all SQL queries executed during the analysis, including:

- After hours failed login attempts
- Date-based login filtering
- Country based exclusions
- Department and office-based employee filtering
- Use of AND, OR, NOT, and LIKE operators

```
MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_time > '18:00:00' AND success = 0;
+----------+----------+------------+------------+---------+-----------------+---
------+
| event_id | username | login_date | login_time | country | ip_address      | s
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 |
|       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   |
```

```
    ->
    -> 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      | 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 |
```

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

```
MariaDB [organization]>
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 |
```

```
MariaDB [organization]>
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 | k242l212m542 | jlansky  | Finance    | South-109   |
|        1011 | l748m120n401 | drosas   | Sales      | South-292   |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271   |
|        1017 | r550s824t230 | jclark   | Finance    | North-188   |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE NOT department = 'Information 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   |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE department = 'Sales' OR department = 'Finance'
    ->
    -> ORDER BY department;
+-------------+--------------+----------+------------+-------------+
| employee_id | device_id    | username | department | office      |
+-------------+--------------+----------+------------+-------------+
|        1195 | n516o853p957 | orainier | Finance    | East-346    |
|        1136 | g299h520i457 | jhawes   | Finance    | West-416    |
|        1122 | s103t952u851 | btorres  | Finance    | West-319    |
|        1105 | b551c837d758 | kmei     | Finance    | Central-232 |
```

```
MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_date > '2022-05-09';
+----------+----------+------------+------------+---------+-----------------+---
------+
| event_id | username | login_date | login_time | country | ip_address      | su
ccess |
+----------+----------+------------+------------+---------+-----------------+---
------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12  |
    0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |
    0 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168.3.24    |
    0 |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_date BETWEEN '2022-05-09' AND '2022-05-11';
+----------+----------+------------+------------+---------+-----------------+---
------+
| 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 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.232  |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT event_id, username, login_date
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE event_id BETWEEN 100 AND 150;
+----------+----------+------------+
| event_id | username | login_date |
+----------+----------+------------+
|      100 | tmitchel | 2022-05-12 |
|      101 | sbaelish | 2022-05-08 |
|      102 | jreckley | 2022-05-09 |
|      103 | jhill    | 2022-05-11 |
|      104 | asundara | 2022-05-11 |
|      105 | cjackson | 2022-05-12 |
|      106 | tmitchel | 2022-05-12 |
|      107 | bisles   | 2022-05-12 |
|      108 | daquino  | 2022-05-09 |
|      109 | mcouliba | 2022-05-10 |
```

```
MariaDB [organization]> clear
MariaDB [organization]> SELECT device_id, operating_system
    ->
    -> FROM machines;
+--------------+------------------+
| device_id    | operating_system |
+--------------+------------------+
| a184b775c707 | OS 1             |
| a192b174c940 | OS 2             |
| a305b818c708 | OS 3             |
| a317b635c465 | OS 1             |
| a320b137c219 | OS 2             |
| a398b471c573 | OS 3             |
| a667b270c984 | OS 1             |
| a821b452c176 | OS 2             |
| a998b568c863 | OS 3             |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT device_id, operating_system
    ->
    -> FROM machines
    ->
    -> WHERE operating_system = 'OS 2';
+--------------+------------------+
| device_id    | operating_system |
+--------------+------------------+
| a192b174c940 | OS 2             |
| a320b137c219 | OS 2             |
| a821b452c176 | OS 2             |
| b157c491d493 | OS 2             |
| b264c773d977 | OS 2             |
| b265c937d713 | OS 2             |
| b806c503d354 | OS 2             |
| b979c871d361 | OS 2             |
```

```
   ->
   -> FROM employees
   ->
   -> WHERE department = 'Finance';
+-------------+--------------+----------+------------+-------------+
| 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   |
|        1010 | k2421212m542 | jlansky  | Finance    | South-109   |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271   |
|        1017 | r550s824t230 | jclark   | Finance    | North-188   |
|        1018 | s310t540u653 | abellmas | Finance    | North-403   |
|        1022 | w237x430y567 | arusso   | Finance    | West-465    |
|        1029 | d336e475f676 | ivelasco | Finance    | East-156    |
|        1044 | s429t157u159 | tbarnes  | Finance    | West-415    |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE office = 'South-109';
+-------------+-------------+----------+------------+-----------+
| employee_id | device_id   | username | department | office    |
+-------------+-------------+----------+------------+-----------+
|        1010 | k2421212m542 | jlansky  | Finance    | South-109 |
+-------------+-------------+----------+------------+-----------+
1 row in set (0.001 sec)
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT *
    ->
    -> FROM employees
    ->
    -> WHERE office LIKE 'South-%';
+-------------+-------------+----------+------------------------+-----------+
| employee_id | device_id   | username | department             | office    |
+-------------+-------------+----------+------------------------+-----------+
|        1003 | d394e816f943 | sgilmore | Finance                | South-153 |
|        1004 | e218f877g788 | eraab    | Human Resources        | South-127 |
|        1005 | f551g340h864 | gesparza | Human Resources        | South-366 |
|        1008 | i858j583k571 | abernard | Finance                | South-170 |
|        1009 | NULL         | lrodriqu | Sales                  | South-134 |
|        1010 | k2421212m542 | jlansky  | Finance                | South-109 |
|        1011 | l748m120n401 | drosas   | Sales                  | South-292 |
```

```
+----------+---------+
200 rows in set (0.001 sec)

MariaDB [organization]>
MariaDB [organization]> SELECT username, login_date, login_time
    ->
    -> FROM log_in_attempts;
+----------+------------+------------+
| username | login_date | login_time |
+----------+------------+------------+
| jrafael  | 2022-05-09 | 04:56:27   |
| apatel   | 2022-05-10 | 20:27:27   |
| dkot     | 2022-05-09 | 06:47:41   |
| dkot     | 2022-05-08 | 02:00:39   |
| jrafael  | 2022-05-11 | 03:05:59   |
| arutley  | 2022-05-12 | 17:00:59   |
| eraab    | 2022-05-11 | 01:45:14   |
| bisles   | 2022-05-08 | 01:30:17   |
| yappiah  | 2022-05-11 | 13:47:29   |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT device_id, operating_system, OS_patch_date
    ->
    -> FROM machines;
+--------------+------------------+---------------+
| device_id    | operating_system | OS_patch_date |
+--------------+------------------+---------------+
| a184b775c707 | OS 1             | 2021-09-01    |
| a192b174c940 | OS 2             | 2021-06-01    |
| a305b818c708 | OS 3             | 2021-06-01    |
| a317b635c465 | OS 1             | 2021-03-01    |
| a320b137c219 | OS 2             | 2021-03-01    |
| a398b471c573 | OS 3             | 2021-12-01    |
| a667b270c984 | OS 1             | 2021-03-01    |
| a821b452c176 | OS 2             | 2021-12-01    |
| a998b568c863 | OS 3             | 2021-12-01    |
| b157c491d493 | OS 2             | 2021-03-01    |
| b239c825d303 | OS 1             | 2021-03-01    |
| b264c773d977 | OS 2             | 2021-03-01    |
| b265c937d713 | OS 2             | 2021-09-01    |
| b433c245d868 | OS 1             | 2021-06-01    |
| b551c837d758 | OS 3             | 2021-03-01    |
| b566c710d544 | OS 1             | 2021-06-01    |
| b806c503d354 | OS 2             | 2021-12-01    |
| b979c871d361 | OS 2             | 2021-03-01    |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts;
+----------+----------+------------+------------+---------+-----------------+--
------+
| event_id | username | login_date | login_time | country | ip_address      | s
uccess |
+----------+----------+------------+------------+---------+-----------------+--
------+
|        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 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168.3.24    |
      0 |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> ORDER BY login_date;
+----------+----------+------------+------------+---------+-----------------+---
------+
| event_id | username | login_date | login_time | country | ip_address      | su
ccess |
+----------+----------+------------+------------+---------+-----------------+---
------+
|      145 | ivelasco | 2022-05-08 | 09:06:02   | CANADA  | 192.168.39.196  |
    1 |
|      163 | tmitchel | 2022-05-08 | 09:21:16   | MEX     | 192.168.119.29  |
    0 |
|       36 | asundara | 2022-05-08 | 09:00:42   | US      | 192.168.78.151  |
    1 |
|      165 | jreckley | 2022-05-08 | 15:28:43   | MEXICO  | 192.168.34.193  |
    0 |
|      168 | jlansky  | 2022-05-08 | 13:25:42   | USA     | 192.168.210.94  |
    1 |
```

```
MariaDB [organization]>
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> ORDER BY login_date, login_time;
+----------+----------+------------+------------+---------+-----------------+---
------+
| event_id | username | login_date | login_time | country | ip_address      | s
ccess |
+----------+----------+------------+------------+---------+-----------------+---
------+
|      117 | bsand    | 2022-05-08 | 00:19:11   | USA     | 192.168.197.187 |
    0 |
|       92 | pwashing | 2022-05-08 | 00:36:12   | US      | 192.168.247.219 |
    0 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.173 |
    0 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.71  |
    0 |
```

```
clear
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 10.5.29-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    -> FROM machines;
+--------------+-----------------+---------------+--------------+-----------
-+
| device_id    | operating_system | email_client   | OS_patch_date | employee_i
 |
+--------------+-----------------+---------------+--------------+-----------
-+
| a184b775c707 | OS 1            | Email Client 1 | 2021-09-01    |        115
 |
| a192b174c940 | OS 2            | Email Client 1 | 2021-06-01    |        105
 |
| a305b818c708 | OS 3            | Email Client 2 | 2021-06-01    |        118
 |
| a317b635c465 | OS 1            | Email Client 2 | 2021-03-01    |        113
 |
| a320b137c219 | OS 2            | Email Client 2 | 2021-03-01    |        100
 |
```