Project Description

This is a project for the Google Cybersecurity Certificate. I take on the role of a Cybersecurity analyst working in a medium sized company. The company is attempting to trace malicious login attempts and secure systems. I use the SQL database for my security investigations, specifically making use of SQL filters.

1. Retrieve After Hours Failed Login Attempts

A security incident occured after office hours. I attempt to trace the origin of the incident to the compromise of a user account. The first portion of the screenshot shows the SQL query I used, and the second portion of the screenshot shows the output returned in the SQL database.

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

Image 1.1: A truncated list of failed login attempts after office hours.

i) SELECT *
FROM log_in_attempts
WHERE login_time > ‘18:00’ AND success = FALSE;

Office hours end at 6 PM; the AND operator combines the first condition specified (office hours) with the second boolean FALSE condition (failed login attempts).

ii) SELECT COUNT(event_id)
FROM log_in_attempts
WHERE login_time > ‘18:00’ AND success = FALSE;

```
MariaDB [organization]> SELECT COUNT(event_id)
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = FALSE;
+-----------------+
| COUNT(event_id) |
+-----------------+
|              19 |
+-----------------+
1 row in set (0.017 sec)
```

Image 1.2: There are 19 failed login attempts after office hours. This information is also specified at the end of the full printout of Image 1.1 (truncated in image 1.1).

2. Retrieve Login Attempts on Specific Dates

Further investigation suggests that another security incident occured either on 8 May or 9 May 2022. I consider all logins on these dates when investigating the login attempts database.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '20
22-05-08';
+----------+----------+------------+------------+---------
+-----------------+---------+
| event_id | username | login_date | login_time | country
| ip_address      | success |
+----------+----------+------------+------------+---------
+-----------------+---------+
|        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 |
```

Image 2.1 Logins on 9 May and 8 May 2022.

SELECT *
FROM log_in_attempts
WHERE login_date = ‘2022-05-09’ OR login_date = ‘2022-05-08’

The OR operator is used to select logins from both days. The AND operator is not used because all the logins have only 1 associated login_date, this means there would be no logins returned if the AND operator was used instead.

3. Retrieve Login Attempts Outside Mexico

My team tells me that there is an issue with the logins outside of Mexico. I therefore look for login attempts from other countries.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------
+-----------------+---------+
| event_id | username | login_date | login_time | country
| ip_address      | success |
+----------+----------+------------+------------+---------
+-----------------+---------+
|        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 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US
| 192.168.16.99   |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA
| 192.168.183.51  |       0 |
```

Image 3.1: Truncated list of login attempts from outside of Mexico.

```
SELECT *
FROM log_in_attempts
WHERE NOT country LIKE ‘MEX%’;
```

The % wildcard operator matches both MEX and MEXICO. The NOT operator is added to select countries other than Mexico.

4. Retrieve Employees in Marketing

It is discovered that the computers in the East office belonging to the Marketing department are outdated. I perform a search to identify which computers to update.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office LIKE 'Eas
t%';
+-------------+-------------+----------+------------+----
------+
| employee_id | device_id    | username | department | off
ice   |
+-------------+-------------+----------+------------+----
------+
|        1000 | a320b137c219 | elarson  | Marketing  | Eas
t-170 |
|        1052 | a192b174c940 | jdarosa  | Marketing  | Eas
t-195 |
|        1075 | x573y883z772 | fbautist | Marketing  | Eas
t-267 |
|        1088 | k8651965m233 | rgosh    | Marketing  | Eas
t-157 |
|        1103 | NULL         | randerss | Marketing  | Eas
t-460 |
|        1156 | a184b775c707 | dellery  | Marketing  | Eas
t-417 |
|        1163 | h679i515j339 | cwilliam | Marketing  | Eas
t-216 |
+-------------+-------------+----------+------------+----
------+
7 rows in set (0.020 sec)
```

Image 4.1: List of marketing employees in the East office.

SELECT *
FROM employees
WHERE department = ‘Marketing’ AND office LIKE ‘East%’;

5. Retrieve Employees in Finance or Sales

I am told that computers used by Finance and Sales require a different update. I isolate the affected systems in the database that require my attention.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = 'Sales
';
+-------------+--------------+----------+------------+----
---------+
| employee_id | device_id    | username | department | off
ice      |
+-------------+--------------+----------+------------+----
---------+
|        1003 | d394e816f943 | sgilmore | Finance    | Sou
th-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | Nor
th-406   |
|        1008 | i858j583k571 | abernard | Finance    | Sou
th-170   |
|        1009 | NULL         | lrodriqu | Sales      | Sou
th-134   |
|        1010 | k2421212m542 | jlansky  | Finance    | Sou
th-109   |
|        1011 | l748m120n401 | drosas   | Sales      | Sou
th-292   |
|        1015 | p611q262r945 | jsoto    | Finance    | Nor
th-271   |
|        1017 | r550s824t230 | jclark   | Finance    | Nor
th-188   |
|        1018 | s310t540u653 | abellmas | Finance    | Nor
th-403   |
|        1022 | w237x430y567 | arusso   | Finance    | Wes
t-465    |
|        1024 | y976z753a267 | iuduike  | Sales      | Sou
th-215   |
|        1025 | z381a365b233 | jhill    | Sales      | Nor
th-115   |
```

Image 5.1: Truncated list of employees in Finance or Sales.

SELECT *
FROM employees
WHERE department = ‘Finance’ OR department = ‘Sales’

6. Retrieve All Employees Not in IT

A security scan is to be run on computers outside the IT department. I list the systems concerned using the database.

```
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   |
|        1009 | NULL         | lrodriqu | Sales
| South-134   |
|        1010 | k2421212m542 | jlansky  | Finance
| South-109   |
|        1011 | l748m120n401 | drosas   | Sales
| South-292   |
|        1015 | p611q262r945 | jsoto    | Finance
| North-271   |
|        1016 | q793r736s288 | sbaelish | Human Resources
| North-229   |
```

Image 6.1: Truncated list of employees not in the IT department.

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

Summary

This lab portfolio shows the knowledge of SQL filters AND, OR, NOT to retrieve information selectively from the log_in_attempts and employees databases. I also make use of the LIKE and % wildcard operator to make similar matches.