Project Title:

Security Event Investigation & Access Analysis using SQL

Project Overview:

This project involved conducting a comprehensive SQL-driven investigation to support security incident response and access management. By leveraging structured queries on `login_attempts` and `employees` datasets, key activities included:

- **Time-based filtering:** Isolating login events by specific dates, times (e.g., after hours), and event ID ranges to reconstruct attack timelines and detect anomalous access patterns.
- **Location-based anomaly detection:** Filtering login attempts to exclude or target specific geographies (e.g., outside Mexico) to pinpoint suspicious activity sources.
- **User-role and asset association:** Joining employee data with device assignments and login records to map user identities to their machines and authentication history.

The project applied industry best practices for data filtering and correlation aligned with SOC workflows and MITRE ATT&CK techniques (e.g., T1078 Credential Access via brute force). It enhanced visibility into user activity, supported asset accountability, and streamlined audit readiness.

🔍 Query 1: Retrieve Logins After a Specific Date

SQL:

SELECT * FROM login_attempts WHERE login_date >= '2022-05-09';

Description:
Isolated login events occurring on or after May 9, 2022, to support post-incident timeline reconstruction and potential threat actor activity review.

```
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 41
Server version: 10.3.39-MariaDB-0+deb10u2 Debian 10

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

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

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
   | success |
+----------+----------+------------+------------+---------+--------------
---+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.1
2  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.23
2  |       0 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168.3.24
   |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.2
43 |       1 |
|        9 | yappiah  | 2022-05-11 | 13:47:29   | MEX     | 192.168.59.13
6  |       1 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.2
21 |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.8
```

```
8   |        0 |
|       177 | wjaffrey | 2022-05-11 | 00:15:55   | USA     | 192.168.144.1
65 |        0 |
|       179 | jclark   | 2022-05-12 | 04:08:17   | CAN     | 192.168.232.9
3   |        0 |
|       180 | tmitchel | 2022-05-12 | 14:53:21   | MEX     | 192.168.190.2
02 |        1 |
|       181 | abellmas | 2022-05-10 | 13:37:05   | CAN     | 192.168.60.11
1   |        0 |
|       182 | lyamamot | 2022-05-10 | 06:01:31   | USA     | 192.168.106.5
2   |        0 |
|       183 | nmason   | 2022-05-11 | 05:29:36   | CANADA | 192.168.137.1
47 |        0 |
|       185 | jsoto    | 2022-05-10 | 13:34:58   | USA     | 192.168.151.9
1   |        0 |
|       188 | jsoto    | 2022-05-11 | 00:39:09   | USA     | 192.168.21.88
    |        0 |
|       192 | bisles   | 2022-05-10 | 08:32:03   | USA     | 192.168.201.4
0   |        1 |
|       194 | jclark   | 2022-05-12 | 14:11:04   | CAN     | 192.168.197.2
47 |        0 |
|       195 | alevitsk | 2022-05-11 | 06:59:13   | CANADA | 192.168.236.7
8   |        1 |
|       196 | acook    | 2022-05-10 | 09:56:48   | CAN     | 192.168.52.90
    |        0 |
|       198 | yappiah  | 2022-05-12 | 10:37:22   | MEXICO | 192.168.103.1
06 |        1 |
|       199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO | 192.168.44.23
2   |        0 |
|       200 | jclark   | 2022-05-12 | 01:11:45   | CANADA | 192.168.91.10
3   |        1 |
+----------+----------+------------+------------+---------+-------------
---+---------+
125 rows in set (0.088 sec)

MariaDB [organization]>
```

🔍 Query 2: Retrieve After-Hours Failed Logins

SQL:

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

Description:
Retrieved failed login attempts that occurred after 6:00 PM, aligning with after-hours threat detection practices. Useful for identifying brute-force attacks or insider threats (MITRE T1078, T1110).

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date >= '2022-05-09';
+----------+----------+------------+------------+---------+---------------
---+---------+
| event_id | username | login_date | login_time | country | ip_address
   | success |
+----------+----------+------------+------------+---------+---------------
---+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.1
40 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.1
2  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.1
62 |       1 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.23
2  |       0 |
|        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168.3.24
   |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.2
43 |       1 |
|        9 | yappiah  | 2022-05-11 | 13:47:29   | MEX     | 192.168.59.13
6  |       1 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.228.2
21 |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.8
1  |       0 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.1
35 |       1 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US      | 192.168.16.99
   |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.5
1  |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.1
89 |       1 |
```

```
|       181 | abellmas | 2022-05-10 | 13:37:05    | CAN      | 192.168.60.11
1   |        0 |
|       182 | lyamamot | 2022-05-10 | 06:01:31    | USA      | 192.168.106.5
2   |        0 |
|       183 | nmason   | 2022-05-11 | 05:29:36    | CANADA   | 192.168.137.1
47  |        0 |
|       185 | jsoto    | 2022-05-10 | 13:34:58    | USA      | 192.168.151.9
1   |        0 |
|       186 | bisles   | 2022-05-09 | 04:29:17    | USA      | 192.168.40.72
    |        0 |
|       187 | arusso   | 2022-05-09 | 00:36:26    | MEX      | 192.168.77.13
7   |        0 |
|       188 | jsoto    | 2022-05-11 | 00:39:09    | USA      | 192.168.21.88
    |        0 |
|       190 | jsoto    | 2022-05-09 | 05:09:21    | USA      | 192.168.25.60
    |        0 |
|       192 | bisles   | 2022-05-10 | 08:32:03    | USA      | 192.168.201.4
0   |        1 |
|       194 | jclark   | 2022-05-12 | 14:11:04    | CAN      | 192.168.197.2
47  |        0 |
|       195 | alevitsk | 2022-05-11 | 06:59:13    | CANADA   | 192.168.236.7
8   |        1 |
|       196 | acook    | 2022-05-10 | 09:56:48    | CAN      | 192.168.52.90
    |        0 |
|       198 | yappiah  | 2022-05-12 | 10:37:22    | MEXICO   | 192.168.103.1
06  |        1 |
|       199 | yappiah  | 2022-05-11 | 19:34:48    | MEXICO   | 192.168.44.23
2   |        0 |
|       200 | jclark   | 2022-05-12 | 01:11:45    | CANADA   | 192.168.91.10
3   |        1 |
+----------+----------+------------+------------+---------+--------------
---+---------+
165 rows in set (0.001 sec)

MariaDB [organization]>
```

🔍 Query 3: Specific Date Logins

SQL:

SELECT * FROM login_attempts WHERE login_date = '2022-05-09' OR login_date = '2022-05-11';

Description:
Queried all login attempts on May 9-11, 2022, as part of a targeted investigation into suspicious access activity during that time frame.

```
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
   | success |
+----------+----------+------------+------------+---------+--------------
---+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.1
40 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.1
2  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.1
62 |       1 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.23
2  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.2
43 |       1 |
|        9 | yappiah  | 2022-05-11 | 13:47:29   | MEX     | 192.168.59.13
6  |       1 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.140.8
1  |       0 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.1
35 |       1 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US      | 192.168.16.99
   |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.5
1  |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.1
89 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89
   |       1 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.14
2  |       0 |
|       21 | iuduike  | 2022-05-11 | 17:50:00   | US      | 192.168.131.1
```

```
22 |        0 |
|       175 | jhill    | 2022-05-10 | 00:17:09   | USA     | 192.168.130.2
18 |        0 |
|       176 | cward    | 2022-05-11 | 12:00:02   | MEX     | 192.168.133.8
8  |        0 |
|       177 | wjaffrey | 2022-05-11 | 00:15:55   | USA     | 192.168.144.1
65 |        0 |
|       181 | abellmas | 2022-05-10 | 13:37:05   | CAN     | 192.168.60.11
1  |        0 |
|       182 | lyamamot | 2022-05-10 | 06:01:31   | USA     | 192.168.106.5
2  |        0 |
|       183 | nmason   | 2022-05-11 | 05:29:36   | CANADA  | 192.168.137.1
47 |        0 |
|       185 | jsoto    | 2022-05-10 | 13:34:58   | USA     | 192.168.151.9
1  |        0 |
|       186 | bisles   | 2022-05-09 | 04:29:17   | USA     | 192.168.40.72
   |        0 |
|       187 | arusso   | 2022-05-09 | 00:36:26   | MEX     | 192.168.77.13
7  |        0 |
|       188 | jsoto    | 2022-05-11 | 00:39:09   | USA     | 192.168.21.88
   |        0 |
|       190 | jsoto    | 2022-05-09 | 05:09:21   | USA     | 192.168.25.60
   |        0 |
|       192 | bisles   | 2022-05-10 | 08:32:03   | USA     | 192.168.201.4
0  |        1 |
|       195 | alevitsk | 2022-05-11 | 06:59:13   | CANADA  | 192.168.236.7
8  |        1 |
|       196 | acook    | 2022-05-10 | 09:56:48   | CAN     | 192.168.52.90
   |        0 |
|       199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.168.44.23
2  |        0 |
+----------+----------+------------+------------+---------+--------------
---+---------+
123 rows in set (0.001 sec)

MariaDB [organization]>
```

🔍 Query 4: Early-Morning Logins

SELECT * FROM login_attempts WHERE login_time < '07:00:00';

Purpose: Isolated pre-7 AM login attempts to detect abnormal access times, aiding in anomaly detection and threat hunting.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time < '07:00:00';
+----------+----------+------------+------------+---------+--------------
---+---------+
| event_id | username | login_date | login_time | country | ip_address
   | success |
+----------+----------+------------+------------+---------+--------------
---+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.1
40 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.1
62 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.7
1  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.23
2  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.2
43 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.1
73 |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.1
89 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89
   |       1 |
|       22 | rjensen  | 2022-05-11 | 00:59:26   | MEX     | 192.168.213.1
28 |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.1
92 |       1 |
|       27 | aalonso  | 2022-05-10 | 01:55:35   | MEX     | 192.168.103.2
10 |       0 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.18
6  |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.4
8  |       1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.2
```

```
00 |       0 |
|      166 | tmitchel | 2022-05-10 | 05:45:16   | MEX      | 192.168.80.12
9  |       0 |
|      175 | jhill    | 2022-05-10 | 00:17:09   | USA      | 192.168.130.2
18 |       0 |
|      177 | wjaffrey | 2022-05-11 | 00:15:55   | USA      | 192.168.144.1
65 |       0 |
|      179 | jclark   | 2022-05-12 | 04:08:17   | CAN      | 192.168.232.9
3  |       0 |
|      182 | lyamamot | 2022-05-10 | 06:01:31   | USA      | 192.168.106.5
2  |       0 |
|      183 | nmason   | 2022-05-11 | 05:29:36   | CANADA   | 192.168.137.1
47 |       0 |
|      184 | alevitsk | 2022-05-08 | 03:09:48   | CAN      | 192.168.33.70
   |       0 |
|      186 | bisles   | 2022-05-09 | 04:29:17   | USA      | 192.168.40.72
   |       0 |
|      187 | arusso   | 2022-05-09 | 00:36:26   | MEX      | 192.168.77.13
7  |       0 |
|      188 | jsoto    | 2022-05-11 | 00:39:09   | USA      | 192.168.21.88
   |       0 |
|      189 | nmason   | 2022-05-08 | 05:37:24   | CANADA   | 192.168.168.1
17 |       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 |
|      195 | alevitsk | 2022-05-11 | 06:59:13   | CANADA   | 192.168.236.7
8  |       1 |
|      200 | jclark   | 2022-05-12 | 01:11:45   | CANADA   | 192.168.91.10
3  |       1 |
+----------+----------+------------+------------+---------+--------------
---+---------+
67 rows in set (0.001 sec)

MariaDB [organization]>
```

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time < '07:00:00';
+----------+----------+------------+------------+---------+--------------
---+---------+
| event_id | username | login_date | login_time | country | ip_address
   | success |
+----------+----------+------------+------------+---------+--------------
---+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.243.1
40 |       1 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.1
62 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.178.7
1  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.86.23
2  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.170.2
43 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.119.1
73 |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.1
89 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.89
   |       1 |
|       22 | rjensen  | 2022-05-11 | 00:59:26   | MEX     | 192.168.213.1
28 |       0 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.1
92 |       1 |
|       27 | aalonso  | 2022-05-10 | 01:55:35   | MEX     | 192.168.103.2
10 |       0 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.18
6  |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.4
8  |       1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.2
```

🔍 Query 5: Between 6:00 and 7:00 AM

SELECT * FROM login_attempts WHERE login_time >= '06:00:00' AND login_time < '07:00:00';

Purpose: Targeted login events within a 1-hour window to identify brute-force patterns or batch login scripts executed pre-business hours.

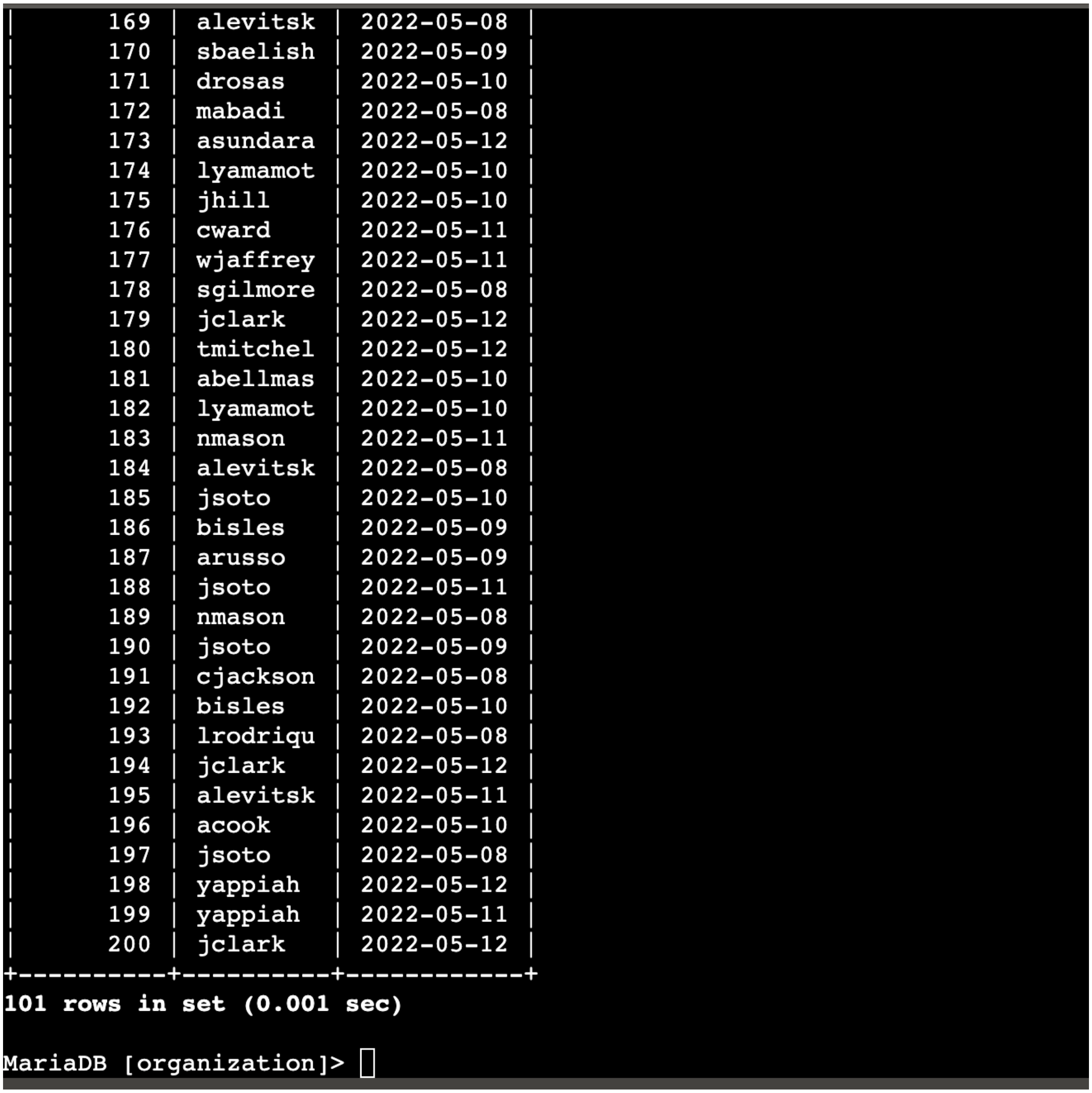
```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE log_in_attempts BETWEEN '06:00:00' and '07:00:00';
ERROR 1054 (42S22): Unknown column 'log_in_attempts' in 'where clause'
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time >= '06:00:00' AND login_time < '07:00:00';
+----------+----------+------------+------------+---------+--------------
---+---------+
| event_id | username | login_date | login_time | country | ip_address
   | success |
+----------+----------+------------+------------+---------+--------------
---+---------+
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.151.1
62 |       1 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.1
89 |       1 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.1
92 |       1 |
|       37 | eraab    | 2022-05-10 | 06:03:41   | CANADA  | 192.168.152.1
48 |       0 |
|       71 | mcouliba | 2022-05-09 | 06:57:42   | CAN     | 192.168.55.16
9  |       0 |
|       98 | gesparza | 2022-05-11 | 06:30:14   | CANADA  | 192.168.148.8
0  |       0 |
|      106 | tmitchel | 2022-05-12 | 06:15:41   | MEXICO  | 192.168.3.252
   |       1 |
|      134 | iuduike  | 2022-05-09 | 06:46:40   | USA     | 192.168.22.11
5  |       1 |
|      136 | mabadi   | 2022-05-10 | 06:56:44   | US      | 192.168.214.2
34 |       1 |
|      142 | gesparza | 2022-05-11 | 06:31:14   | CANADA  | 192.168.117.5
6  |       1 |
|      147 | yappiah  | 2022-05-08 | 06:04:34   | MEX     | 192.168.65.24
5  |       0 |
|      148 | daquino  | 2022-05-08 | 06:15:55   | CANADA  | 192.168.135.6
```

🔍 Query 6: Event IDs Greater Than or Equal to 100

SELECT eventId, username, loginDate FROM login_attempts WHERE eventId >= 100;

Purpose: Queried high-priority or post-deployment login events to support log review during incident response.

```
MariaDB [organization]> SELECT event_id, username, login_date
    -> FROM log_in_attempts
    -> WHERE event_id >= 100;
+----------+----------+------------+
| 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 |
|      110 | mabadi   | 2022-05-09 |
|      111 | aestrada | 2022-05-10 |
|      112 | rjensen  | 2022-05-09 |
|      113 | gesparza | 2022-05-10 |
|      114 | smartell | 2022-05-10 |
|      115 | ivelasco | 2022-05-10 |
|      116 | tmitchel | 2022-05-10 |
|      117 | bsand    | 2022-05-08 |
|      118 | smartell | 2022-05-12 |
|      119 | tmitchel | 2022-05-11 |
|      120 | tmitchel | 2022-05-09 |
|      121 | btang    | 2022-05-10 |
|      122 | yappiah  | 2022-05-11 |
|      123 | bmoreno  | 2022-05-10 |
|      124 | asundara | 2022-05-12 |
|      125 | bisles   | 2022-05-11 |
|      126 | jrafael  | 2022-05-12 |
|      127 | abellmas | 2022-05-09 |
|      128 | jclark   | 2022-05-09 |
|      129 | drosas   | 2022-05-12 |
```



```
|       169 | alevitsk | 2022-05-08 |
|       170 | sbaelish | 2022-05-09 |
|       171 | drosas   | 2022-05-10 |
|       172 | mabadi   | 2022-05-08 |
|       173 | asundara | 2022-05-12 |
|       174 | lyamamot | 2022-05-10 |
|       175 | jhill    | 2022-05-10 |
|       176 | cward    | 2022-05-11 |
|       177 | wjaffrey | 2022-05-11 |
|       178 | sgilmore | 2022-05-08 |
|       179 | jclark   | 2022-05-12 |
|       180 | tmitchel | 2022-05-12 |
|       181 | abellmas | 2022-05-10 |
|       182 | lyamamot | 2022-05-10 |
|       183 | nmason   | 2022-05-11 |
|       184 | alevitsk | 2022-05-08 |
|       185 | jsoto    | 2022-05-10 |
|       186 | bisles   | 2022-05-09 |
|       187 | arusso   | 2022-05-09 |
|       188 | jsoto    | 2022-05-11 |
|       189 | nmason   | 2022-05-08 |
|       190 | jsoto    | 2022-05-09 |
|       191 | cjackson | 2022-05-08 |
|       192 | bisles   | 2022-05-10 |
|       193 | lrodriqu | 2022-05-08 |
|       194 | jclark   | 2022-05-12 |
|       195 | alevitsk | 2022-05-11 |
|       196 | acook    | 2022-05-10 |
|       197 | jsoto    | 2022-05-08 |
|       198 | yappiah  | 2022-05-12 |
|       199 | yappiah  | 2022-05-11 |
|       200 | jclark   | 2022-05-12 |
+----------+----------+------------+
101 rows in set (0.001 sec)

MariaDB [organization]>
```

🔍 Query 7: Login Attempts Between 100–150

SELECT username FROM login_attempts WHERE eventId BETWEEN 100 AND 150;

SELECT username FROM login_attempts WHERE eventId BETWEEN 100 AND 150;

Purpose: Filtered usernames tied to login attempts within a specific event ID range to narrow investigation focus.

```
MariaDB [organization]> SELECT username
    -> FROM log_in_attempts
    -> WHERE event_id BETWEEN '100' and '150';
+----------+
| username |
+----------+
| tmitchel |
| sbaelish |
| jreckley |
| jhill    |
| asundara |
| cjackson |
| tmitchel |
| bisles   |
| daquino  |
| mcouliba |
| mabadi   |
| aestrada |
| rjensen  |
| gesparza |
| smartell |
| ivelasco |
| tmitchel |
| bsand    |
| smartell |
| tmitchel |
| tmitchel |
| btang    |
| yappiah  |
| bmoreno  |
| asundara |
| bisles   |
| jrafael  |
| abellmas |
| jclark   |
| drosas   |
```

```
| tmitchel |
| tmitchel |
| btang    |
| yappiah  |
| bmoreno  |
| asundara |
| bisles   |
| jrafael  |
| abellmas |
| jclark   |
| drosas   |
| mrah     |
| bisles   |
| rjensen  |
| asundara |
| iuduike  |
| bsand    |
| mabadi   |
| jrafael  |
| tmitchel |
| apatel   |
| btang    |
| btang    |
| gesparza |
| jhill    |
| daquino  |
| ivelasco |
| nmason   |
| yappiah  |
| daquino  |
| jlansky  |
| nmason   |
+----------+
51 rows in set (0.001 sec)

MariaDB [organization]>
```

🔍 Query 8: Row Numbering Within a Subset

```
SELECT
  ROW_NUMBER() OVER (ORDER BY eventId) AS row_num,
  username
FROM login_attempts
WHERE eventId BETWEEN 100 AND 150;
```

Purpose: Ranked users by login event ID using `ROW_NUMBER()` to visualize sequential activity, enhancing report quality and analysis structure.

```
MariaDB [organization]> SELECT
    ->     ROW_NUMBER() OVER () AS '#',
    ->     username
    -> FROM log_in_attempts
    -> WHERE event_id BETWEEN '100' AND '150';
+----+----------+
| #  | username |
+----+----------+
|  1 | tmitchel |
|  2 | yappiah  |
|  3 | tmitchel |
|  4 | jhill    |
|  5 | tmitchel |
|  6 | bsand    |
|  7 | tmitchel |
|  8 | tmitchel |
|  9 | rjensen  |
| 10 | daquino  |
| 11 | gesparza |
| 12 | drosas   |
| 13 | ivelasco |
| 14 | mabadi   |
| 15 | jrafael  |
| 16 | gesparza |
| 17 | bisles   |
| 18 | bmoreno  |
| 19 | apatel   |
| 20 | asundara |
| 21 | tmitchel |
| 22 | mabadi   |
| 23 | sbaelish |
| 24 | bsand    |
| 25 | asundara |
| 26 | jlansky  |
| 27 | smartell |
| 28 | mrah     |
```

🔍 **Query 9 :** Retrieve After-Hours Failed Login Attempts

SELECT * FROM login_attempts

WHERE login_time > '18:00:00'

AND success = 0;

Description / Purpose:
This query retrieves all failed login attempts (`success = 0`) that occurred after business hours (after 6:00 PM). It is useful in identifying potential unauthorized access attempts outside standard working times. These logs can indicate early stages of brute-force attacks, credential misuse, or policy violations that should be reviewed by the SOC team.

```
MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = '1';
+----------+----------+------------+------------+---------+----
-------------+---------+
| event_id | username | login_date | login_time | country | ip_
address      | success |
+----------+----------+------------+------------+---------+----
-------------+---------+
|       23 | yappiah  | 2022-05-10 | 18:11:53   | MEXICO  | 192
.168.200.48  |       1 |
|       51 | jrafael  | 2022-05-10 | 22:40:01   | CANADA  | 192
.168.148.115 |       1 |
|       54 | jreckley | 2022-05-10 | 19:31:19   | MEXICO  | 192
.168.167.152 |       1 |
|       57 | asundara | 2022-05-12 | 21:13:02   | US      | 192
.168.211.201 |       1 |
|       60 | acook    | 2022-05-11 | 21:46:00   | CAN     | 192
.168.54.45   |       1 |
```

```
|        65 | aalonso  | 2022-05-09 | 23:42:12   | MEX     | 192
.168.52.37   |        1 |
|        66 | aestrada | 2022-05-08 | 21:58:32   | MEX     | 192
.168.67.223  |        1 |
|       105 | cjackson | 2022-05-12 | 19:36:42   | CAN     | 192
.168.247.153 |        1 |
|       108 | daquino  | 2022-05-09 | 21:30:48   | CANADA  | 192
.168.15.110  |        1 |
|       115 | ivelasco | 2022-05-10 | 23:06:01   | CAN     | 192
.168.154.1   |        1 |
|       116 | tmitchel | 2022-05-10 | 20:33:27   | MEXICO  | 192
.168.119.26  |        1 |
|       118 | smartell | 2022-05-12 | 23:21:31   | MEXICO  | 192
.168.173.196 |        1 |
|       119 | tmitchel | 2022-05-11 | 23:07:13   | MEXICO  | 192
.168.110.175 |        1 |
|       121 | btang    | 2022-05-10 | 22:00:36   | US      | 192
.168.80.143  |        1 |
|       126 | jrafael  | 2022-05-12 | 18:47:52   | CAN     | 192
.168.22.16   |        1 |
|       132 | rjensen  | 2022-05-12 | 23:26:03   | MEX     | 192
.168.9.166   |        1 |
|       158 | smartell | 2022-05-09 | 19:30:32   | MEXICO  | 192
.168.190.178 |        1 |
|       164 | jclark   | 2022-05-12 | 21:15:52   | CAN     | 192
.168.18.34   |        1 |
|       173 | asundara | 2022-05-12 | 23:17:52   | US      | 192
.168.58.217  |        1 |
+-----------+----------+------------+------------+---------+----
-------------+---------+
20 rows in set (0.146 sec)
```

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = '0';
+----------+----------+------------+------------+---------+----
------------+---------+
| 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 |
```

```
.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   |        0 |
|       199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO   | 192
.168.44.232   |        0 |
+----------+----------+------------+------------+---------+----
-------------+---------+
19 rows in set (0.001 sec)

MariaDB [organization]>
```

🔍 Query 10: **Retrieve Login Attempts on 2022-05-08 and 2022-05-09**

SQL Code:

SELECT * FROM login_attempts

WHERE login_date = '2022-05-09'

  OR login_date = '2022-05-08';

Description / Purpose:

This query retrieves all login attempts that occurred on May 9 and May 8, 2022. It supports incident response investigations by filtering for user authentication events that happened on or immediately before a known security event. Analysts use this query to identify suspicious logins, detect patterns, and correlate findings with system alerts and threat intelligence.

```
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       | 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 |
```

```
|       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 |
|       169 | alevitsk | 2022-05-08 | 08:10:43   | CANADA   | 192
.168.210.228 |        0 |
|       170 | sbaelish | 2022-05-09 | 16:43:18   | USA      | 192
.168.65.113  |        0 |
|       172 | mabadi   | 2022-05-08 | 08:06:50   | US       | 192
.168.180.41  |        1 |
|       178 | sgilmore | 2022-05-08 | 12:27:22   | CAN      | 192
.168.52.216  |        0 |
|       184 | alevitsk | 2022-05-08 | 03:09:48   | CAN      | 192
.168.33.70   |        0 |
|       186 | bisles   | 2022-05-09 | 04:29:17   | USA      | 192
.168.40.72   |        0 |
|       187 | arusso   | 2022-05-09 | 00:36:26   | MEX      | 192
.168.77.137  |        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]>
```

🔍 Query 11 : **Retrieve Login Attempts Outside of Mexico**

SQL Code:

SELECT * FROM login_attempts

WHERE country NOT LIKE '%MEX%';

Description / Purpose:
This query filters login attempts to exclude any records from Mexico, including those labeled `MEX` or `MEXICO`. It is designed for geolocation-based investigation when suspicious login activity is known **not** to have originated from Mexico. SOC analysts use this filter to isolate potentially malicious login attempts from foreign IPs or unknown countries during an incident response effort.

```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE  country NOT 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 |
```

```
|       183 | nmason   | 2022-05-11 | 05:29:36   | CANADA  | 192
.168.137.147 |        0 |
|       184 | alevitsk | 2022-05-08 | 03:09:48   | CAN     | 192
.168.33.70   |        0 |
|       185 | jsoto    | 2022-05-10 | 13:34:58   | USA     | 192
.168.151.91  |        0 |
|       186 | bisles   | 2022-05-09 | 04:29:17   | USA     | 192
.168.40.72   |        0 |
|       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 (0.002 sec)

MariaDB [organization]> 
```

```
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 |
```

```
|       185 | jsoto    | 2022-05-10 | 13:34:58   | USA     | 192
.168.151.91  |        0 |
|       186 | bisles   | 2022-05-09 | 04:29:17   | USA     | 192
.168.40.72   |        0 |
|       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 (0.001 sec)

MariaDB [organization]>
```

🔍 Query 12: **Retrieve Marketing Employees in East Building**

SQL Code:

SELECT * FROM employees

WHERE department LIKE '%Marketing%'

AND office LIKE 'East%';

Purpose / Description:

This query identifies employees who work in the **Marketing department** and are located in

any office within the East building. It uses `LIKE` filtering to handle flexible text matching for both the `department` (e.g., "Marketing" or "Digital Marketing") and `office` (e.g., "East-170", "East-320") fields. It’s typically used during **targeted security update rollouts** or **asset inventory scoping** based on department and location.

```
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 Technolog
y | East-320    |
|        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   |
|        1012 | m756n668o146 | nmason   | Information Technolog
y | North-160   |
```

```
|         1185 | d790e839f461 | revens   | Sales
  | North-330    |
|         1186 | e281f433g404 | sacosta  | Sales
  | North-460    |
|         1187 | f963g637h851 | bbode    | Finance
  | East-351     |
|         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 |
|         1192 | k570l183m949 | rlaghari | Information Technolog
y | East-138     |
|         1193 | l186m618n319 | esantiag | Information Technolog
y | Central-300 |
|         1194 | m340n287o441 | zwarren  | Human Resources
  | West-212     |
|         1195 | n516o853p957 | orainier | Finance
  | East-346     |
|         1196 | o225p357q829 | sshah2   | Information Technolog
y | South-385    |
|         1197 | p791q114r509 | aabara   | Information Technolog
y | North-159    |
|         1198 | q308r573s459 | jmartine | Marketing
  | South-117    |
|         1199 | r520s571t459 | areyes   | Human Resources
  | East-100     |
+-------------+--------------+----------+---------------------
--+-------------+
200 rows in set (0.001 sec)

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 |
|        1156 | a184b775c707 | dellery  | Marketing  | East-417 |
|        1163 | h679i515j339 | cwilliam | Marketing  | East-216 |
+-------------+-------------+----------+------------+----------+
7 rows in set (0.027 sec)
```

🔍 Query 13: Retrieve Employees in Sales or Finance Departments

SQL Code:

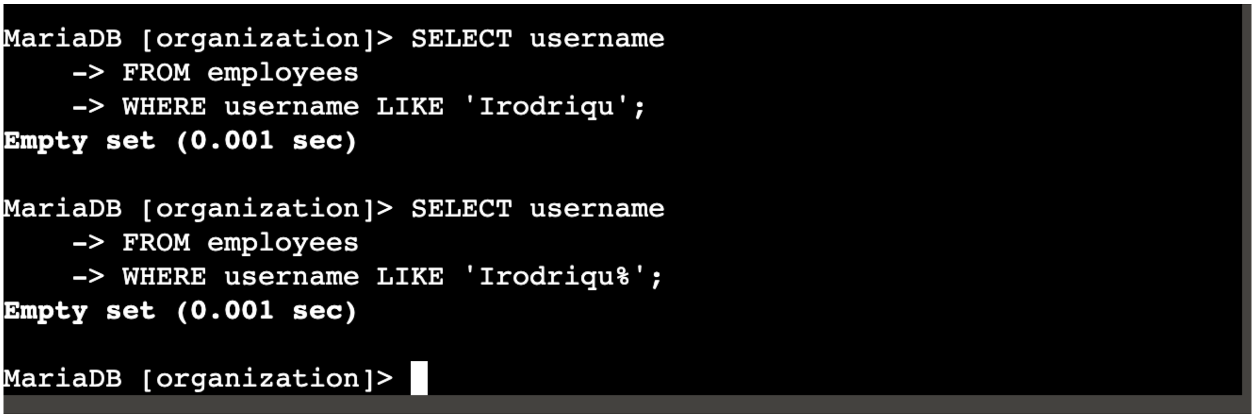
```
SELECT * FROM employees

WHERE department LIKE '%Finance%'

   OR department LIKE '%Sales%';
```

Purpose / Description:
This query filters the `employees` table to retrieve all records for employees working in either the **Sales** or **Finance** departments. It uses `LIKE` with wildcards to account for possible variations in department names (e.g., “Global Finance”, “Sales-West”). This query is useful for **targeted security updates**, **access audits**, or **patch rollouts** for users in financially sensitive roles.

```
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   |
|        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    |
|        1035 | j236k303l245 | bisles   | Sales      | South-171   |
|        1039 | n253o917p623 | cjackson | Sales      | East-378    |
|        1041 | p929q222r778 | cgriffin | Sales      | North-208   |
|        1044 | s429t157u159 | tbarnes  | Finance    | West-415    |
|        1045 | t567u844v434 | pwashing | Finance    | East-115    |
|        1046 | u429v921w138 | daquino  | Finance    | West-280    |
|        1047 | v109w587x644 | cward    | Finance    | West-373    |
|        1048 | w167x592y375 | tmitchel | Finance    | South-288   |
|        1049 | NULL         | jreckley | Finance    | Central-295 |
|        1050 | y132z930a114 | csimmons | Finance    | North-468   |
|        1057 | f370g535h632 | mscott   | Sales      | South-270   |
|        1062 | k367l639m697 | redwards | Finance    | North-180   |
|        1063 | l686m140n569 | lpope    | Sales      | East-226    |
|        1066 | o678p794q957 | ttyrell  | Sales      | Central-444 |
|        1069 | NULL         | jpark    | Finance    | East-110    |
```



🔍 Query 14: Retrieve All Employees Not in IT

SQL Code:

SELECT * FROM employees

WHERE department NOT LIKE 'Information Technology';

Purpose / Description:
This query retrieves all employees **excluding** those in the **Information Technology** department. It uses the `NOT LIKE` clause with wildcards to ensure flexible filtering, accounting for partial department names like "Information Technology Team" or "IT Support". This allows targeted deployment of a final security update to all other teams.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department LIKE '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 | 1748m120n401  | drosas   | Sales           | South-292   |
|        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   |
|        1020 | u899v381w363  | arutley  | Marketing       | South-351   |
|        1022 | w237x430y567  | arusso   | Finance         | West-465    |
|        1024 | y976z753a267  | iuduike  | Sales           | South-215   |
|        1025 | z381a365b233  | jhill    | Sales           | North-115   |
|        1026 | a998b568c863  | apatel   | Human Resources | West-320    |
|        1027 | b806c503d354  | mrah     | Marketing       | West-246    |
|        1028 | c603d749e374  | aestrada | Human Resources | West-121    |
|        1029 | d336e475f676  | ivelasco | Finance         | East-156    |
|        1030 | e391f189g913  | mabadi   | Marketing       | West-375    |
|        1031 | f419g188h578  | dkot     | Marketing       | West-408    |
|        1034 | i679j565k940  | bsand    | Human Resources | East-484    |
|        1035 | j236k3031245  | bisles   | Sales           | South-171   |
|        1036 | k5501533m205  | rjensen  | Marketing       | Central-239 |
|        1038 | m873n636o225  | btang    | Human Resources | Central-260 |
```

```
|       1174 | s371t911u987 | eortiz    | Finance         | North-428   |
|       1175 | t959u687v394 | jclark2   | Finance         | North-194   |
|       1176 | u849v569w521 | nliu      | Sales           | West-220    |
|       1177 | v691w183x928 | aezra     | Human Resources | East-190    |
|       1178 | w986x187y885 | nlannist  | Marketing       | North-196   |
|       1179 | x174y934z376 | asalas    | Human Resources | North-445   |
|       1180 | y131z211a578 | medwards  | Human Resources | Central-340 |
|       1181 | z803a233b718 | sessa     | Finance         | South-207   |
|       1183 | b566c710d544 | lquraish  | Human Resources | East-400    |
|       1184 | c986d200e170 | ptsosie   | Human Resources | Central-247 |
|       1185 | d790e839f461 | revens    | Sales           | North-330   |
|       1186 | e281f433g404 | sacosta   | Sales           | North-460   |
|       1187 | f963g637h851 | bbode     | Finance         | East-351    |
|       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]>
```

🔍 Query 15: Match Employees to Their Machines

SQL Code:

SELECT employees.*, machines.*

FROM employees

INNER JOIN machines

ON employees.device_id = machines.device_id;

Purpose / Description:
This query uses an `INNER JOIN` on the `device_id` field to match each employee with their corresponding machine. It returns all columns from both the `employees` and `machines` tables, making it useful for tracking user-device relationships, verifying assignments, or preparing for endpoint security operations. Only records with a valid match in both tables are shown, ensuring accurate identity-to-asset correlation.

```
MariaDB [organization]> clear
MariaDB [organization]> SELECT *
    -> FROM machines;
+--------------+------------------+----------------+---------------+-----
--------+
| device_id    | operating_system | email_client   | OS_patch_date | empl
oyee_id |
+--------------+------------------+----------------+---------------+-----
--------+
| a184b775c707 | OS 1             | Email Client 1 | 2021-09-01    |
   1156 |
| a192b174c940 | OS 2             | Email Client 1 | 2021-06-01    |
   1052 |
| a305b818c708 | OS 3             | Email Client 2 | 2021-06-01    |
   1182 |
| a317b635c465 | OS 1             | Email Client 2 | 2021-03-01    |
   1130 |
| a320b137c219 | OS 2             | Email Client 2 | 2021-03-01    |
   1000 |
| a398b471c573 | OS 3             | Email Client 2 | 2021-12-01    |
      0 |
| a667b270c984 | OS 1             | Email Client 1 | 2021-03-01    |
   1078 |
| a821b452c176 | OS 2             | Email Client 2 | 2021-12-01    |
   1104 |
| a998b568c863 | OS 3             | Email Client 1 | 2021-12-01    |
   1026 |
| b157c491d493 | OS 2             | Email Client 1 | 2021-03-01    |
      0 |
| b239c825d303 | OS 1             | Email Client 1 | 2021-03-01    |
   1001 |
| b264c773d977 | OS 2             | Email Client 2 | 2021-03-01    |
   1157 |
| b265c937d713 | OS 2             | Email Client 1 | 2021-09-01    |
   1131 |
| b433c245d868 | OS 1             | Email Client 1 | 2021-06-01    |
```

```
| y103z561a649 | OS 2            | Email Client 1 | 2021-03-01    |
  1128 |
| y131z211a578 | OS 2            | Email Client 1 | 2021-03-01    |
  1180 |
| y132z930a114 | OS 2            | Email Client 2 | 2021-06-01    |
  1050 |
| y246z508a775 | OS 2            | Email Client 1 | 2021-12-01    |
     0 |
| y347z204a710 | OS 2            | Email Client 2 | 2021-12-01    |
  1076 |
| y765z123a548 | OS 2            | Email Client 2 | 2021-06-01    |
  1154 |
| y943z930a241 | OS 1            | Email Client 2 | 2021-09-01    |
  1102 |
| y976z753a267 | OS 2            | Email Client 2 | 2021-06-01    |
  1024 |
| z381a365b233 | OS 3            | Email Client 2 | 2021-12-01    |
  1025 |
| z451a308b518 | OS 2            | Email Client 1 | 2021-03-01    |
  1051 |
| z566a147b347 | OS 1            | Email Client 1 | 2021-12-01    |
  1129 |
| z654a154b259 | OS 2            | Email Client 2 | 2021-12-01    |
  1077 |
| z803a233b718 | OS 1            | Email Client 2 | 2021-12-01    |
  1181 |
| z821a946b264 | OS 3            | Email Client 2 | 2021-06-01    |
     0 |
| z942a966b589 | OS 3            | Email Client 1 | 2021-09-01    |
  1155 |
+--------------+-----------------+----------------+---------------+-----
--------+
200 rows in set (0.122 sec)

MariaDB [organization]>
```

🔍 **Query 16: Join Machines to Employees**

SQL Code:

SELECT *

FROM machines

INNER JOIN employees

ON machines.device_id = employees.device_id;

Purpose / Description:

This query performs an `INNER JOIN` between the `machines` and `employees` tables using the shared `device_id` column. It returns all records where both tables have a matching device ID, effectively mapping each machine to its assigned employee. This is essential for endpoint inventory, monitoring, and accountability in a SOC or IT environment.

```
MariaDB [organization]> SELECT *
    -> FROM machines
    -> INNER JOIN employees ON machines.device_id = employees.device_id;
+--------------+------------------+----------------+---------------+-----
--------+-------------+--------------+----------+-----------------------
+-------------+
| device_id    | operating_system | email_client   | OS_patch_date | empl
oyee_id | employee_id | device_id    | username | department
| office      |
+--------------+------------------+----------------+---------------+-----
--------+-------------+--------------+----------+-----------------------
+-------------+
| a320b137c219 | OS 2             | Email Client 2 | 2021-03-01    |
  1000 |        1000 | a320b137c219 | elarson  | Marketing
| East-170    |
| b239c825d303 | OS 1             | Email Client 1 | 2021-03-01    |
  1001 |        1001 | b239c825d303 | bmoreno  | Marketing
| Central-276 |
| c116d593e558 | OS 3             | Email Client 1 | 2021-09-01    |
  1002 |        1002 | c116d593e558 | tshah    | Human Resources
| North-434   |
| d394e816f943 | OS 3             | Email Client 2 | 2021-03-01    |
  1003 |        1003 | d394e816f943 | sgilmore | Finance
| South-153   |
| e218f877g788 | OS 2             | Email Client 1 | 2021-09-01    |
  1004 |        1004 | e218f877g788 | eraab    | Human Resources
| South-127   |
| f551g340h864 | OS 3             | Email Client 2 | 2021-12-01    |
  1005 |        1005 | f551g340h864 | gesparza | Human Resources
| South-366   |
| g329h357i597 | OS 1             | Email Client 2 | 2021-06-01    |
  1006 |        1006 | g329h357i597 | alevitsk | Information Technology
| East-320    |
| h174i497j413 | OS 2             | Email Client 1 | 2021-03-01    |
  1007 |        1007 | h174i497j413 | wjaffrey | Finance
| North-406   |
```

Query 17: Return All Employees and Matching Machines (RIGHT JOIN)

SELECT *

FROM machines

RIGHT JOIN employees

ON machines.device_id = employees.device_id;

Description:
This query uses a `RIGHT JOIN` to retrieve **all employees**, even if they **don't have a machine** assigned. It joins `machines` and `employees` via `device_id`, ensuring visibility into every user's asset status. This helps uncover **employees without devices**, useful for identifying provisioning or HR-system sync gaps.

```
MariaDB [organization]> SELECT *
    -> FROM machines
    -> RIGHT JOIN employees ON machines.device_id = employees.device_id;
+--------------+------------------+----------------+---------------+-----
--------+-------------+--------------+----------+-----------------------
+-------------+
| device_id    | operating_system | email_client   | OS_patch_date | empl
oyee_id | employee_id | device_id    | username | department
| office      |
+--------------+------------------+----------------+---------------+-----
--------+-------------+--------------+----------+-----------------------
+-------------+
| a320b137c219 | OS 2             | Email Client 2 | 2021-03-01    |
  1000 |        1000 | a320b137c219 | elarson  | Marketing
| East-170    |
| b239c825d303 | OS 1             | Email Client 1 | 2021-03-01    |
  1001 |        1001 | b239c825d303 | bmoreno  | Marketing
| Central-276 |
| c116d593e558 | OS 3             | Email Client 1 | 2021-09-01    |
  1002 |        1002 | c116d593e558 | tshah    | Human Resources
| North-434   |
| d394e816f943 | OS 3             | Email Client 2 | 2021-03-01    |
  1003 |        1003 | d394e816f943 | sgilmore | Finance
| South-153   |
| e218f877g788 | OS 2             | Email Client 1 | 2021-09-01    |
  1004 |        1004 | e218f877g788 | eraab    | Human Resources
| South-127   |
| f551g340h864 | OS 3             | Email Client 2 | 2021-12-01    |
  1005 |        1005 | f551g340h864 | gesparza | Human Resources
| South-366   |
| g329h357i597 | OS 1             | Email Client 2 | 2021-06-01    |
  1006 |        1006 | g329h357i597 | alevitsk | Information Technology
| East-320    |
| h174i497j413 | OS 2             | Email Client 1 | 2021-03-01    |
  1007 |        1007 | h174i497j413 | wjaffrey | Finance
```

```
| NULL          | NULL                | NULL            | NULL           |
   NULL |        1190 | NULL           | kcarter  | Marketing
| Central-270 |
| NULL          | NULL                | NULL            | NULL           |
   NULL |        1191 | NULL           | shakimi  | Marketing
| Central-366 |
| k570l183m949 | OS 3                | Email Client 1 | 2021-12-01     |
   1192 |        1192 | k570l183m949 | rlaghari | Information Technology
| East-138    |
| l186m618n319 | OS 1                | Email Client 2 | 2021-12-01     |
   1193 |        1193 | l186m618n319 | esantiag | Information Technology
| Central-300 |
| m340n287o441 | OS 2                | Email Client 2 | 2021-09-01     |
   1194 |        1194 | m340n287o441 | zwarren  | Human Resources
| West-212    |
| n516o853p957 | OS 1                | Email Client 1 | 2021-09-01     |
   1195 |        1195 | n516o853p957 | orainier | Finance
| East-346    |
| o225p357q829 | OS 3                | Email Client 1 | 2021-12-01     |
   1196 |        1196 | o225p357q829 | sshah2   | Information Technology
| South-385   |
| p791q114r509 | OS 2                | Email Client 1 | 2021-09-01     |
   1197 |        1197 | p791q114r509 | aabara   | Information Technology
| North-159   |
| q308r573s459 | OS 3                | Email Client 1 | 2021-03-01     |
   1198 |        1198 | q308r573s459 | jmartine | Marketing
| South-117   |
| r520s571t459 | OS 2                | Email Client 2 | 2021-03-01     |
   1199 |        1199 | r520s571t459 | areyes   | Human Resources
| East-100    |
+--------------+-------------------+-----------------+----------------+-----
--------+------------+-------------+----------+----------------------
+-------------+
200 rows in set (0.002 sec)

MariaDB [organization]>
```

🔍 Query 18: **Retrieve Employees with Login Attempts**

SQL Code:

SELECT employees.*, log_in_attempts.*

FROM employees

INNER JOIN log_in_attempts

ON employees.username = log_in_attempts.username;

Purpose / Description:

This query uses an inner join on the `username` column to combine employee information with their login attempt records. It returns data only for employees who have login entries, providing a full view of user authentication activity for use in security incident investigations, auditing, and monitoring. The comprehensive result set supports effective correlation between identity and login behavior.

```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> INNER JOIN log_in_attempts ON employees.username = log_in_attempts
.username;
+-------------+--------------+----------+------------------------+-------
------+----------+----------+------------+------------+---------+--------
---------+---------+
| employee_id | device_id    | username | department             | office
      | event_id | username | login_date | login_time | country | ip_addr
ess       | success |
+-------------+--------------+----------+------------------------+-------
------+----------+----------+------------+------------+---------+--------
---------+---------+
|        1032 | g773h303i639 | jrafael  | Information Technology | Centra
l-309 |        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168
.243.140 |       0 |
|        1026 | a998b568c863 | apatel   | Human Resources        | West-3
20    |        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168
.205.12  |       0 |
|        1031 | f419g188h578 | dkot     | Marketing              | West-4
08    |        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168
.151.162 |       0 |
|        1031 | f419g188h578 | dkot     | Marketing              | West-4
08    |        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168
.178.71  |       0 |
|        1032 | g773h303i639 | jrafael  | Information Technology | Centra
l-309 |        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168
.86.232  |       0 |
|        1020 | u899v381w363 | arutley  | Marketing              | South-
351   |        6 | arutley  | 2022-05-12 | 17:00:59   | MEXICO  | 192.168
.3.24    |       0 |
|        1004 | e218f877g788 | eraab    | Human Resources        | South-
127   |        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168
.170.243 |       0 |
|        1035 | j236k303l245 | bisles   | Sales                  | South-
171   |        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168
```

```
|        1039 | n253o917p623 | cjackson | Sales                  | East-3
78    |      191 | cjackson | 2022-05-08 | 06:46:07   | CANADA  | 192.168
.7.187   |       0 |
|        1035 | j236k303l245 | bisles   | Sales                  | South-
171   |      192 | bisles   | 2022-05-10 | 08:32:03   | USA     | 192.168
.201.40  |       0 |
|        1009 | NULL         | lrodriqu | Sales                  | South-
134   |      193 | lrodriqu | 2022-05-08 | 07:11:29   | US      | 192.168
.125.240 |       0 |
|        1017 | r550s824t230 | jclark   | Finance                | North-
188   |      194 | jclark   | 2022-05-12 | 14:11:04   | CAN     | 192.168
.197.247 |       0 |
|        1006 | g329h357i597 | alevitsk | Information Technology | East-3
20    |      195 | alevitsk | 2022-05-11 | 06:59:13   | CANADA  | 192.168
.236.78  |       0 |
|        1042 | q175r338s833 | acook    | Human Resources        | West-3
81    |      196 | acook    | 2022-05-10 | 09:56:48   | CAN     | 192.168
.52.90   |       0 |
|        1015 | p611q262r945 | jsoto    | Finance                | North-
271   |      197 | jsoto    | 2022-05-08 | 09:05:09   | US      | 192.168
.36.21   |       0 |
|        1033 | NULL         | yappiah  | Information Technology | West-3
87    |      198 | yappiah  | 2022-05-12 | 10:37:22   | MEXICO  | 192.168
.103.106 |       0 |
|        1033 | NULL         | yappiah  | Information Technology | West-3
87    |      199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.168
.44.232  |       0 |
|        1017 | r550s824t230 | jclark   | Finance                | North-
188   |      200 | jclark   | 2022-05-12 | 01:11:45   | CANADA  | 192.168
.91.103  |       0 |
+-------------+--------------+----------+------------------------+-------
------+----------+----------+------------+------------+---------+--------
---------+---------+
200 rows in set (0.010 sec)

MariaDB [organization]>
```

Final Conclusion:

This SQL investigation framework demonstrates the ability to systematically query and analyze security-relevant data to inform SOC analysts and incident responders. By integrating multiple join types (`INNER JOIN`, `LEFT JOIN`, `RIGHT JOIN`) and advanced filtering, the project enables:

- Rapid identification of failed and successful login attempts, especially during high-risk windows (e.g., after hours).
- Focused reviews of user login behavior around critical incident dates.
- Effective geo-fencing of login sources to isolate suspicious activity origins.

- Accurate mapping of employees to their machines to facilitate endpoint management and incident triage.
- Clear and maintainable query documentation that enhances reproducibility and communication within security teams.

The output is a well-rounded toolkit for access monitoring and investigation that any mature SOC or cybersecurity team would value, bridging the gap between raw data and actionable insights.