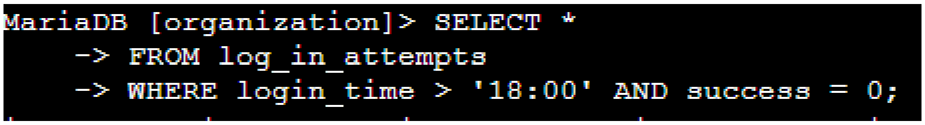
Apply filters to SQL queries

Project description

I used SQL queries with filters (including WHERE, OR, NOT, and LIKE) to investigate potential security issues by retrieving and narrowing down records from the **employees** and **log_in_attempts** tables**.** Specifically, I identified suspicious and policy-relevant login activity by filtering for certain users, dates/times. Locations and outcomes, and I cross-referenced these results with employee details such as department and office location. This allowed me to isolate the most relevant records, determine which employees and machines were involved, and support incident analysis with clear, targeted datesets.

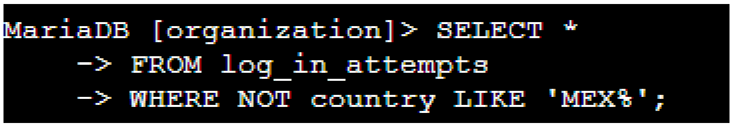
Retrieve after hours failed login attempts



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

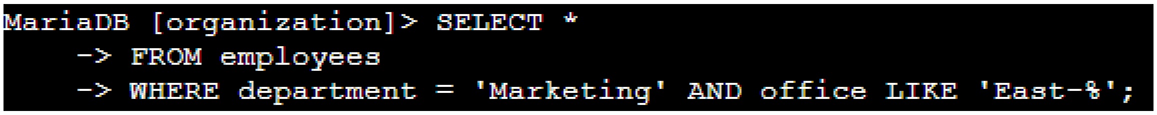
Retrieve login attempts on specific dates

Retrieve login attempts outside of Mexico

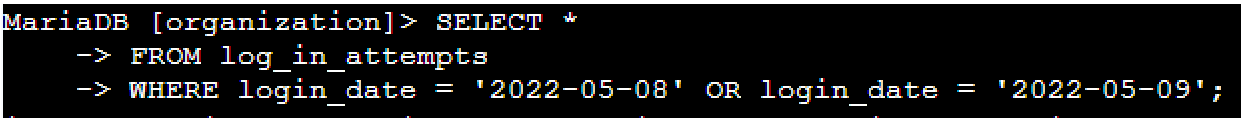


```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
```

Retrieve employees in Marketing

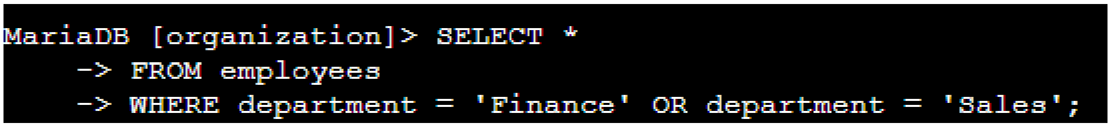


```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office LIKE 'East-%';
```



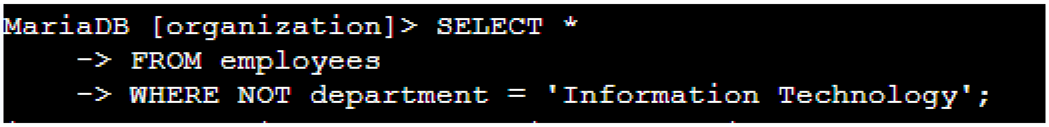
```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-08' OR login_date = '2022-05-09';
```

Retrieve employees in Finance or Sales



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = 'Sales';
```

Retrieve all employees not in IT



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

Summary

In this investigation, I used SQL filtering techniques to isolate relevant records from the **employees** and **log_in_attempts** tables. I identified potentially suspicious activity by querying **after-hours failed logins**, isolating **login attempts on specific dates**, and filtering attempts **outside of Mexico**. I also retrieved targeted employee groups by filtering departments and office locations (Marketing in East offices, Finance/Sales staff, and all employees not in IT). These queries helped narrow large datasets into actionable subsets for security review and incident reporting.