SQL Log & Employee Data Analysis for Security Operations

Overview

This project demonstrates hands-on SQL skills used by security analysts to investigate authentication activity and retrieve employee system information during security incidents and system maintenance efforts.

Across two lab exercises, I analyzed login attempt data and employee records using SQL filtering techniques. The focus was on extracting precise datasets using comparison operators, date and time filtering, and compound logic (`AND`, `OR`, `NOT`)—core skills used in SOC, GRC, and incident response roles.

Scenario

A simulated organization experienced security concerns involving authentication activity and required system updates across departments. I was tasked with retrieving relevant login and employee data from a MariaDB database to support:

- Security incident investigations
- Identification of abnormal login behavior
- Department-based system update planning

The analysis was conducted using the `log_in_attempts` and `employees` tables within the organization database.

Skills Demonstrated

- SQL querying for security analysis

- Filtering with `WHERE` clauses
- Date and time-based filtering
- Comparison operators (`=`, `>`, `<`, `>=`, `<=`, `<>`)
- Logical operators (`AND`, `OR`, `NOT`)
- Pattern matching with `LIKE`
- Authentication log analysis
- Employee and department data filtering

Part 1: Login Attempt Analysis

1. Login Attempts by Date

Retrieved login attempts:

- After a specific date
- On or after a given date
- Within a defined date range

Use case: Narrowing investigation scope during a security incident.

---

2. Login Attempts by Time

Analyzed logins occurring:

- Outside normal business hours
- Within specific early-morning time windows

Use case: Identifying abnormal or suspicious login behavior.

3. Login Attempts by Event ID

Filtered login attempts based on numeric event ID thresholds and ranges.

Use case: Isolating relevant authentication events during log reviews.

Part 2: Advanced Filtering with AND, OR, and NOT

4. After-Hours Failed Login Attempts

Retrieved failed login attempts that occurred after business hours using compound conditions.

Use case: Detecting potential brute-force or unauthorized access attempts.

5. Login Attempts on Specific Dates

Retrieved login attempts occurring on two specific dates using logical OR conditions.

Use case: Investigating activity around a known incident date.

6. Login Attempts Outside of Mexico

Filtered login attempts that did not originate from Mexico using `NOT` and `LIKE`.

Use case: Identifying geographically unusual login activity.

Employee Data Analysis

7. Employees in Marketing (East Building)

Retrieved employee records for:

- Marketing department

- Offices located in the East building

Use case: Coordinating department-specific system updates.

---

8. Employees in Finance or Sales

Retrieved employees belonging to either Finance or Sales departments.

Use case: Targeted maintenance and access reviews.

---

9. Employees Not in IT

Filtered all employees not in the Information Technology department.

Use case: Identifying systems requiring updates not already applied by IT.

Tools & Technologies

- SQL
- MariaDB
- Command-line database environment

Why This Matters

Security analysts frequently rely on SQL to:

- Investigate authentication logs
- Detect anomalous access patterns
- Support incident response decisions

- Coordinate secure system updates across departments

This project reflects real-world analyst workflows by combining log analysis with employee and department data filtering using precise SQL logic.

Next Steps

- Correlate login activity with IP addresses and user roles
- Automate recurring security queries
- Expand analysis into full incident response reports
- Integrate findings into SIEM-style workflows