SQL for Security Data Analysis

Project Overview/Purpose: This project demonstrates the use of **SQL queries** with various filtering techniques to perform security-related data analysis. Working with simulated `log_in_attempts` and `employees` tables, I conducted investigations into potential security incidents and retrieved targeted employee information to support system updates and hardening initiatives.

Skills Demonstrated:

- **SQL Querying & Filtering:** Proficiency in using `SELECT`, `FROM`, and `WHERE` clauses.
- **Logical Operators:** Applied `AND`, `OR`, and `NOT` operators for complex data segmentation.
- **Pattern Matching:** Utilized `LIKE` with the wildcard (`%`) for flexible data searches (e.g., partial string matching for locations/offices).
- **Security Incident Investigation:** Identified suspicious login patterns (after-hours, specific dates, unusual locations).
- **Data Retrieval for Security Operations:** Extracted targeted employee data for specific departmental or location-based security updates.
- **Analytical Thinking:** Interpreted data requirements to construct effective queries for security insights.

Tools Used:

- **SQL (Structured Query Language)**
- **Relational Database Management System (Conceptual)**

Key Outcomes:

- Successfully identified **failed login attempts** occurring outside business hours, crucial for immediate security incident response.
- Pinpointed all login activity on specific **suspicious dates** and from **unauthorized geographic locations**, aiding in broader security investigations.
- Efficiently retrieved segmented lists of employees (e.g., Marketing, Finance, Sales, non-IT, specific buildings) to facilitate **targeted security updates** and system hardening measures.
- Demonstrated ability to transform raw log and employee data into actionable security intelligence.

Files Included:

- `after_hours_failed_logins.sql`
- `specific_date_logins.sql`

- `logins_outside_mexico.sql`
- `employees_marketing_east_building.sql`
- `employees_finance_or_sales.sql`
- `employees_not_in_IT.sql`
- `screenshots_of_query_outputs/` (Folder containing relevant screenshots)