# Apply filters to SQL queries

## Project description

Security analysts can exploit the immense utilities of the SQL tool to probe into relational databases that typically contain data (usually logs) that can be useful for staying in control of the security architecture of the organization. Given that an organization’s network activities generate tons of data every minute, SQL is useful tool to drill through these data and target only needed information at any time. This information may be needed for troubleshooting, detection, audit, response, etc. to security events and/or incidents.

In this project, I demonstrate how SQL was used to perform different security, audit and control functions for a fictional organization. The organization’s database contains the following two tables:

* log\_in\_attempts
* employees

The log\_in\_attempts table has the following columns:

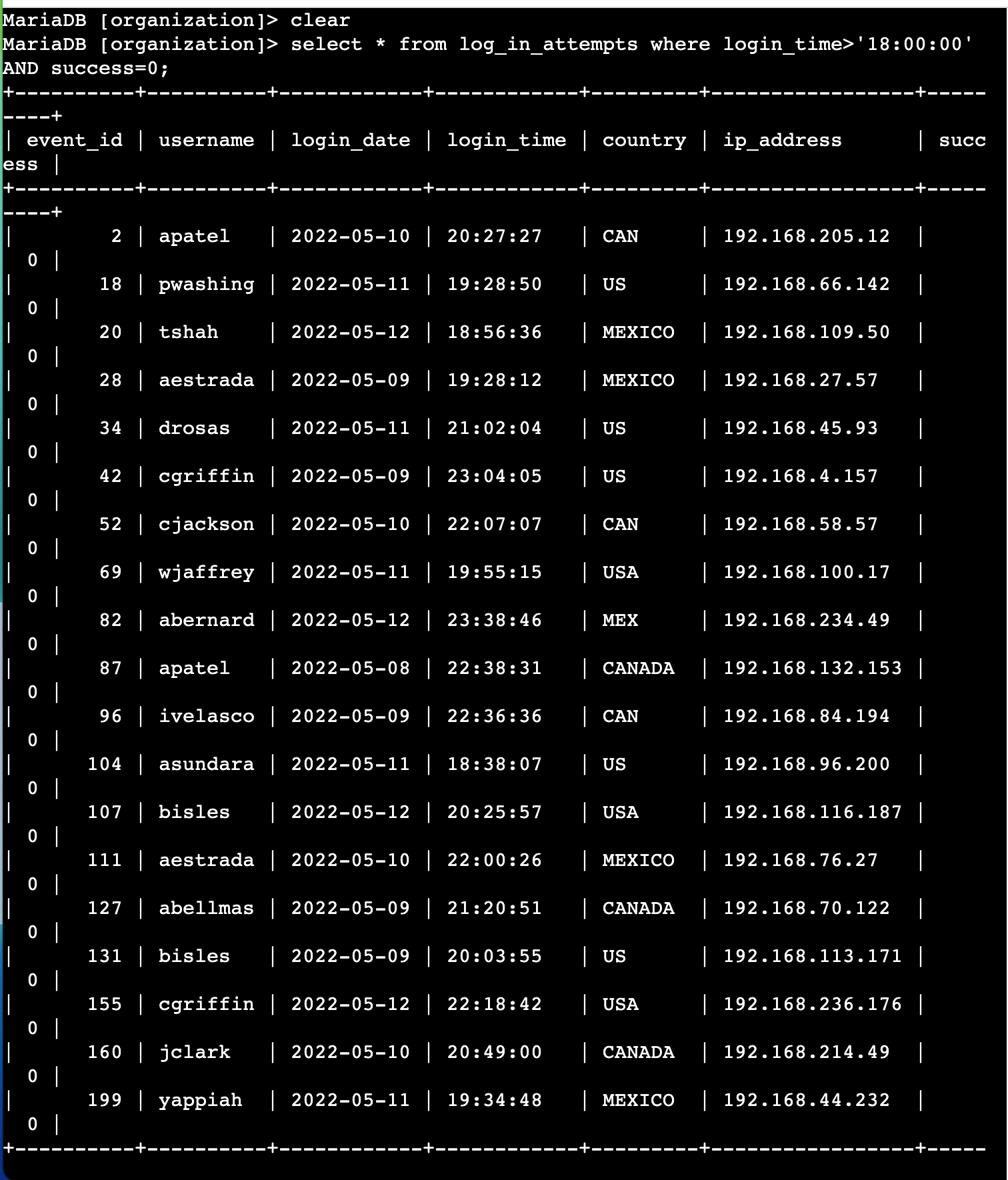
* event\_id: The identification number assigned to each login event
* username: The username of the employee
* login\_date: The date the login attempt was recorded
* login\_time: The time the login attempt was recorded
* country: The country where the login attempt occurred
* ip\_address: The IP address of that employee’s machine
* success: The success of the login attempt; FALSE indicates a failed attempt

The employees table has the following columns:

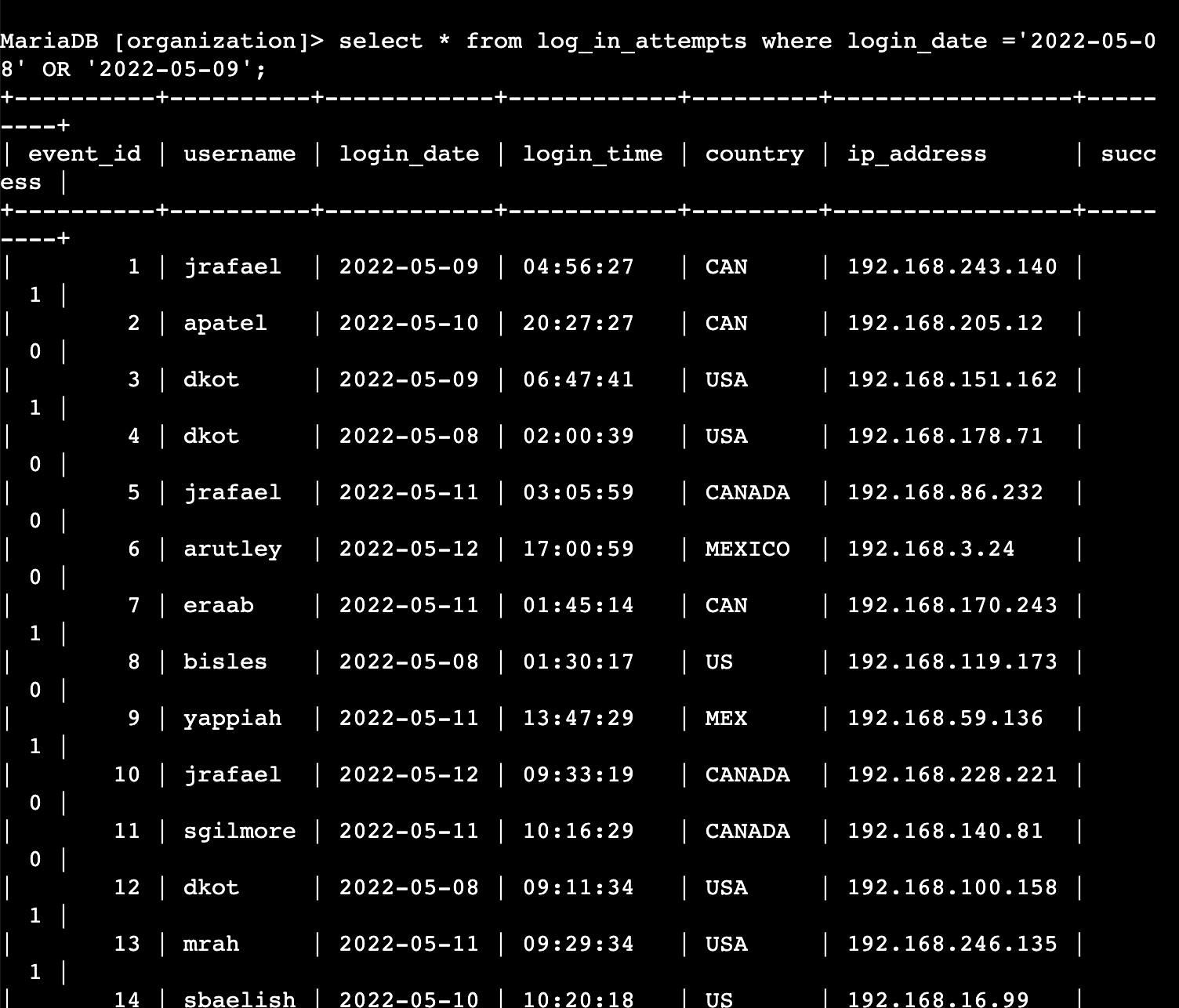
* employee\_id: The identification number assigned to each employee
* device\_id: The identification number assigned to each device used by the employee
* username: The username of the employee
* department: The department the employee is in
* office: The office the employee is located in

## Retrieve after hours failed login attempts

*You recently discovered a potential security incident that occurred after business hours. To investigate this, you need to query the log\_in\_attempts table and review after hours login activity. Use filters in SQL to create a query that identifies all failed login attempts that occurred after 18:00. Retrieve login attempts on specific dates.*

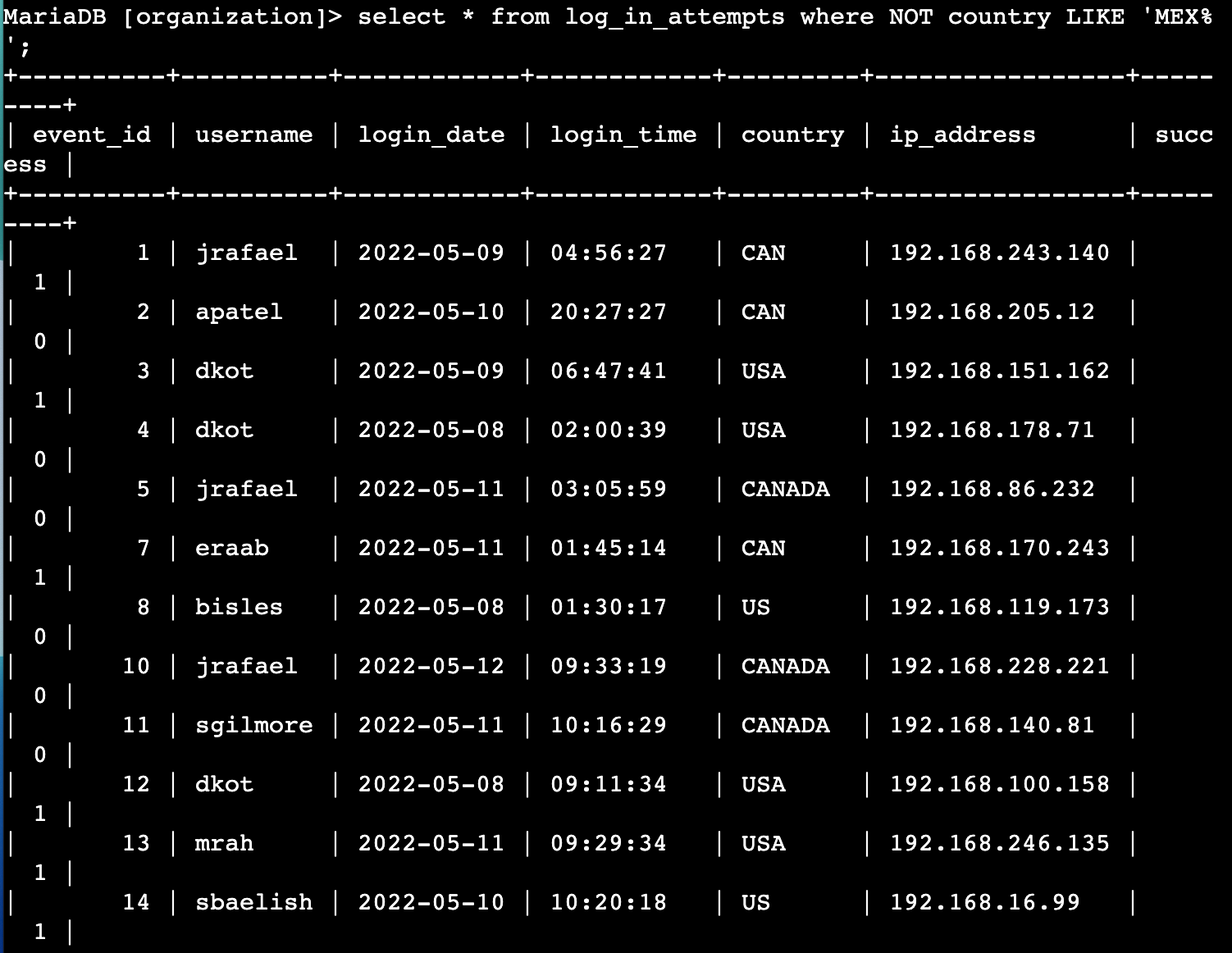


*A suspicious event occurred on 2022-05-09. To investigate this event, you want to review all login attempts which occurred on this day and the day before. Use filters in SQL to create a query that identifies all login attempts that occurred on 2022-05-09 or 2022-05-08.*



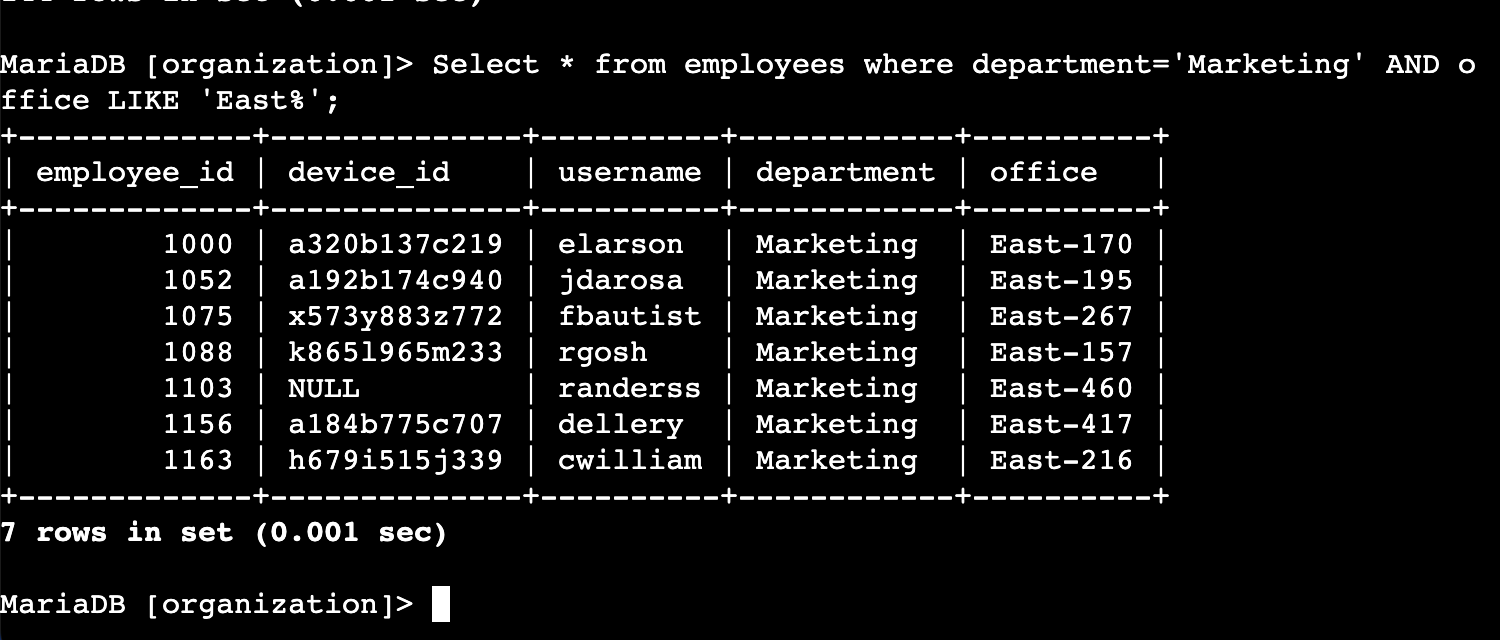
## Retrieve login attempts outside of Mexico

*There’s been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. Now, you need to investigate login attempts that occurred outside of Mexico. Use filters in SQL to create a query that identifies all login attempts that occurred outside of Mexico.*



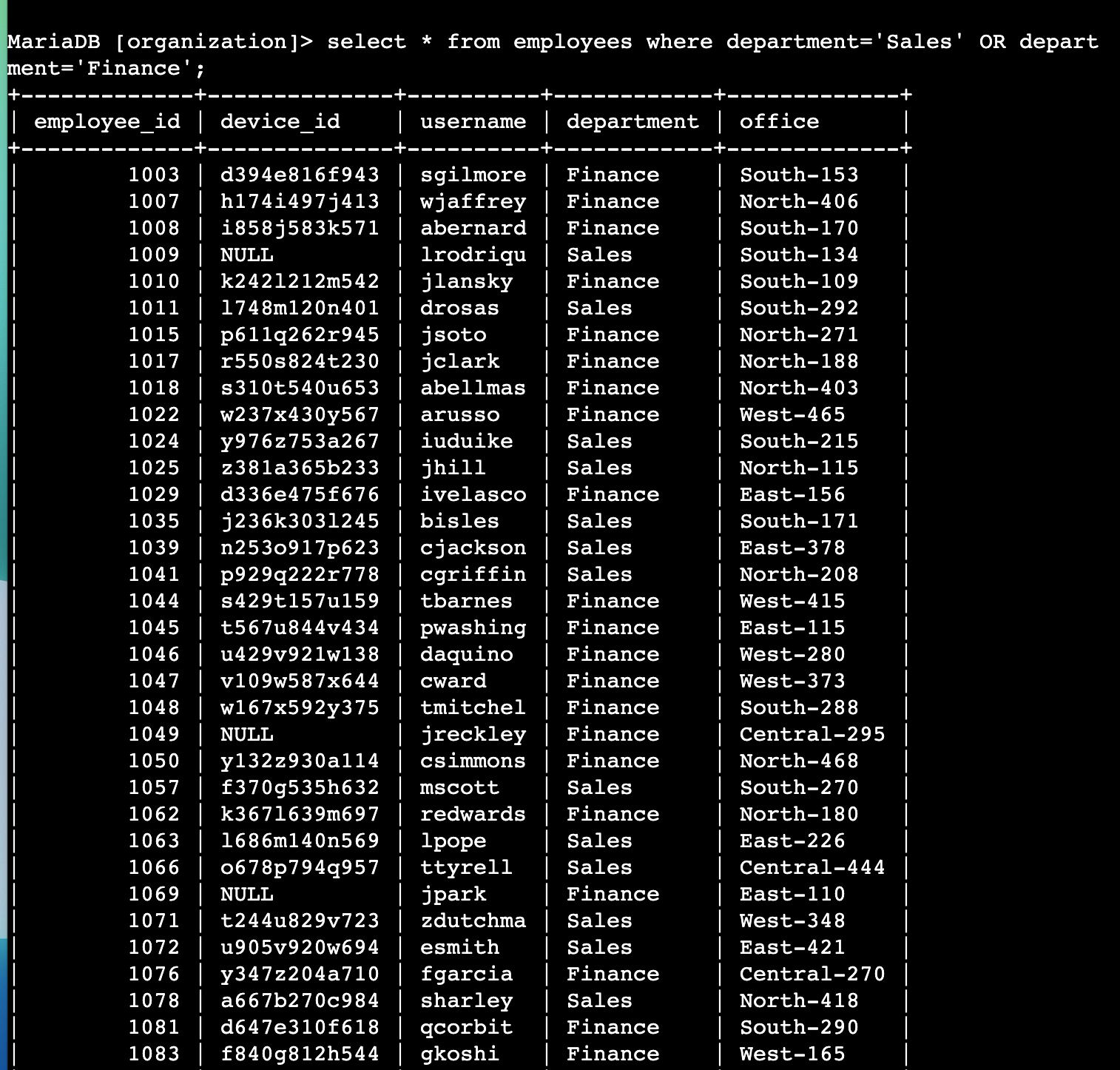
## Retrieve employees in Marketing

Your team wants to perform security updates on specific employee machines in the Marketing department. You’re responsible for getting information on these employee machines and will need to query the employees table. Use filters in SQL to create a query that identifies all employees in the Marketing department for all offices in the East building.



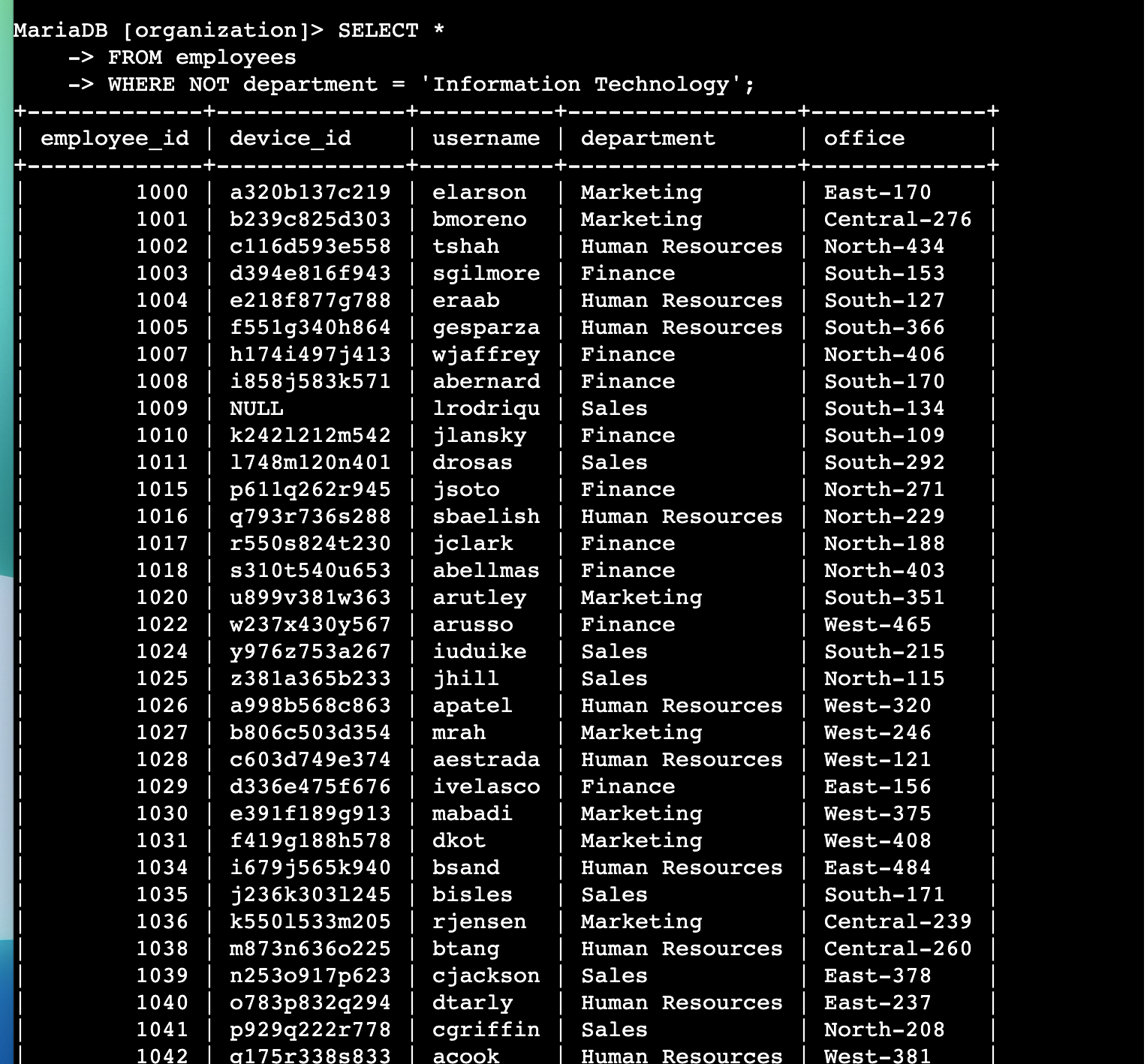
## Retrieve employees in Finance or Sales

Your team now needs to perform a different security update on machines for employees in the Sales and Finance departments. Use filters in SQL to create a query that identifies all employees in the Sales or Finance departments.



## Retrieve all employees not in IT

*Your team needs to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it. Use filters in SQL to create a query which identifies all employees not in the IT department.*



## Summary

SQL is an important tool for security analysts in their line of work. It is useful for different reasons, all of which are important for maintaining security and reducing risk vulnerabilities. In this exercise, I was able to use SQL to probe different tables as part of activities such as audit trail, compliance activities and network updates.