# **SQL Security Investigation Project**

## **Project description**

In this project, I used SQL queries to investigate potential security issues related to login attempts and employee data. By applying filters with AND, OR, and NOT operators, I was able to identify suspicious activity, such as failed logins occurring outside normal working hours or from unexpected locations.

## **Retrieve after hours failed login attempts**

This query retrieves all login attempts that failed and occurred outside of normal business hours (8 AM–6 PM):

SELECT \*  
 FROM log\_in\_attempts  
 WHERE success = FALSE  
 AND (hour < 8 OR hour > 18);

## **Retrieve login attempts on specific dates**

This query filters login attempts that occurred on specific dates of interest, such as days when suspicious activity was reported:

SELECT \*  
 FROM log\_in\_attempts  
 WHERE date IN ('2025-10-10', '2025-10-11');

## **Retrieve login attempts outside of Mexico**

This query identifies login attempts made from IP addresses not located in Mexico, which could indicate unauthorized access attempts:

SELECT \*  
 FROM log\_in\_attempts  
 WHERE NOT country = 'Mexico';

## **Retrieve employees in Marketing**

This query retrieves a list of all employees who work in the Marketing department:

SELECT \*  
 FROM employees  
 WHERE department = 'Marketing';

## **Retrieve employees in Finance or Sales**

This query retrieves all employees who are part of either the Finance or Sales departments:

SELECT \*  
 FROM employees  
 WHERE department = 'Finance'  
 OR department = 'Sales';

## **Retrieve all employees not in IT**

This query retrieves all employees who are not part of the IT department, using the NOT operator:

SELECT \*  
 FROM employees  
 WHERE NOT department = 'IT';

## **Summary**

Through these SQL queries, I demonstrated the ability to use filtering conditions to investigate and analyze data for security monitoring. These queries can help identify failed login attempts during unusual hours, logins from outside approved regions, and employee data by department. Together, they support a proactive approach to securing organizational systems and detecting potential threats.