# **Apply filters to SQL queries**

## **Project description**

In this scenario, I’m responsible for identifying potential security threats by examining data from the "log\_in\_attempts" and "employees" tables. By writing SQL queries, I gather targeted information to evaluate suspicious activity—such as logins outside regular hours, access attempts on certain dates, unauthorized access from locations outside Mexico, and employee details filtered by department and location.

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

To examine possible security incidents happening outside of business hours, I plan to use SQL to filter data from the "log\_in\_attempts" table. The focus will be on extracting all failed login attempts that took place after 6:00 PM (18:00).

SELECT \*

FROM log\_in\_attempts

WHERE success = 0 AND TIME(login\_time) > '18:00:00';

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

To look into a particular incident, I’ll run a SQL query on the "log\_in\_attempts" table to pull all login attempts that happened on May 8 or May 9, 2022.

SELECT \*

FROM log\_in\_attempts

WHERE login\_date IN ('2022-05-08', '2022-05-09');

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

To analyze unusual login activity from outside Mexico, I’ll use SQL filters to extract entries from the "log\_in\_attempts" table where the country is listed as anything other than "MEX" or "MEXICO".

SELECT \*

FROM log\_in\_attempts

WHERE country NOT LIKE 'MEX%';

## **Retrieve employees in Marketing**

To collect details on employees working in the Marketing department and based in the East building, I’ll query the "employees" table using specific SQL filters.

SELECT \*

FROM employees

WHERE department = 'Marketing' AND office LIKE 'East%';

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

To find employees who belong to either the Finance or Sales departments, I’ll use SQL filters on the "employees" table to retrieve the relevant records.

SELECT \*

FROM employees

WHERE department IN ('Finance', 'Sales');

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

To retrieve a list of employees outside the IT department, I’ll apply SQL filters to the "employees" table to exclude those associated with IT.

SELECT \*

FROM employees

WHERE department != 'Information Technology';

## **Summary**

Through SQL queries, I've conducted a comprehensive investigation into potential security issues, including after-hours login attempts, suspicious login attempts on specific dates, login attempts from outside Mexico, and employee details based on department and location. These queries assist in enhancing the organization's security by identifying and addressing potential vulnerabilities and risks.