**Project description**

In this project, I investigated potential security incidents by using SQL queries to retrieve filtered information from the log\_in\_attempts and employees tables in the organization database. I applied SQL filters using WHERE, AND, OR, NOT, LIKE, and BETWEEN to isolate data such as failed logins after business hours, login events on specific dates, and employee machine details for security updates.

**Retrieve after hours failed login attempts**

To find failed login attempts after working hours (after 18:00), I wrote the following SQL query:

SELECT \*

FROM log\_in\_attempts

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

A screen shot of a computer

AI-generated content may be incorrect.

This query uses the AND operator to combine two conditions: login time is after 6 PM, and the attempt was unsuccessful (represented by 0 in the success column).

**Retrieve login attempts on specific dates**

To find login attempts during and before a specific suspicious day (May 9, 2022), I used the following query:

SELECT \*

FROM log\_in\_attempts

WHERE login\_date = '2022-05-09' OR login\_date = '2022-05-08';

A screenshot of a computer

AI-generated content may be incorrect.

This query filters the results to include only records from May 8 and May 9 using the OR operator between two date matches.

**Retrieve login attempts outside of Mexico**

To exclude login attempts from Mexico (values such as 'MEX' or 'MEXICO'), I used the following SQL query:

SELECT \*

FROM log\_in\_attempts

WHERE country NOT LIKE 'MEX%';

A screen shot of a computer

AI-generated content may be incorrect.

The NOT LIKE 'MEX%' clause filters out any country name that starts with "MEX", ensuring we only get login attempts from outside of Mexico.

**Retrieve employees in Marketing**

To get employees in the Marketing department who are located in any East office, I used:

SELECT \*

FROM employees

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

A screenshot of a computer program

AI-generated content may be incorrect.

This query combines an exact match for the department with a pattern match for any office that starts with "East-", using the LIKE keyword with %.

**Retrieve employees in Finance or Sales**

To get employees from either the Finance or Sales departments, I used this query:

SELECT \*

FROM employees

WHERE department = 'Finance' OR department = 'Sales';

A screenshot of a computer

AI-generated content may be incorrect.

This filters the results to show all employees who work in either of the two departments using the OR operator.

**Retrieve all employees not in IT**

To find employees who are **not** part of the Information Technology department, I used the following query:

SELECT \*

FROM employees

WHERE department <> 'Information Technology';

Or

SELECT \*

FROM employees

WHERE NOT department = 'Information Technology';

This uses the <> operator (not equal to) to exclude anyone working in IT from the result set.

A screenshot of a computer screen

AI-generated content may be incorrect.

**Summary**

Using SQL, I effectively filtered data to investigate login patterns and employee details in the organization. I retrieved failed login attempts outside business hours, login activity on specific dates, and excluded certain countries and departments. I also retrieved specific employee information based on department and office location to support security update procedures. These SQL skills are crucial for real-world cybersecurity investigations.