**Apply filters to SQL queries**

**Project description**

In this project, SQL queries were used to investigate potential security incidents and apply security updates to employee devices. By using SQL filters, suspicious login attempts outside working hours, on specific dates, and from locations outside Mexico were identified. Additionally, employee lists from specific departments were retrieved to facilitate security updates.

**Retrieve after-hours failed login attempts**

**SQL Query:**

SELECT \*

FROM log\_in\_attempts

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

**Description:**

This query retrieves all failed login attempts that occurred after 6:00 PM. It uses the filter login\_time > '18:00:00' to select attempts occurring after 6:00 PM and success = FALSE to identify failed attempts. This helps investigate potential security incidents outside of working hours.

**Retrieve login attempts on specific dates**

**SQL Query:**

SELECT \*

FROM log\_in\_attempts

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

**Description:**

This query retrieves all login attempts that occurred on 2022-05-09 or 2022-05-08. It uses the filter login\_date = '2022-05-09' OR login\_date = '2022-05-08' to select attempts from these specific dates. This is useful for investigating suspicious events on certain days.

**Retrieve login attempts outside of Mexico**

**SQL Query:**

SELECT \*

FROM log\_in\_attempts

WHERE country NOT LIKE 'MEX%' AND country NOT LIKE 'MEXICO%';

**Description:**

This query retrieves all login attempts that occurred outside of Mexico. It uses the filter country NOT LIKE 'MEX%' AND country NOT LIKE 'MEXICO%' to exclude login attempts originating in Mexico. This is helpful for detecting suspicious activity from foreign locations.

**Retrieve employees in Marketing**

**SQL Query:**

SELECT \*

FROM employees

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

**Description:**

This query retrieves all employees in the Marketing department who work in the East building. It uses the filter department = 'Marketing' to select Marketing employees and office LIKE 'Este%' to filter offices in the East building. This is useful for applying security updates to specific machines.

**Retrieve employees in Finance or Sales**

**SQL Query:**

SELECT \*

FROM employees

WHERE department = 'Finanzas' OR department = 'Ventas';

**Description:**

This query retrieves all employees in the Finance or Sales departments. It uses the filter department = 'Finanzas' OR department = 'Ventas' to select employees from these departments. This is useful for applying security updates to the devices of these employees.

**Retrieve all employees not in IT**

**SQL Query:**

SELECT \*

FROM employees

WHERE department != 'Tecnología de la información';

**Description:**

This query retrieves all employees who do not belong to the IT department. It uses the filter department != 'Tecnología de la información' to exclude IT employees. This helps ensure that security updates are applied to employees who have not yet received them.

**Summary**

In summary, SQL filters were applied to identify suspicious login attempts and apply security updates to employee devices. The queries retrieved specific information about failed login attempts, activity outside of Mexico, and employees in departments such as Marketing, Finance, and Sales. These tasks helped strengthen the organization's security and investigate potential security incidents.