Apply filters to SQL queries

Project description

There was a potential security incident that occurred after business hours (after 18:00). All after hours login attempts that failed need to be investigates.

The following code shows how I created a SQL query to filter for failed login attemtps that occurred after business hours.

Retrieve after hours failed login attempts

In response to a security incident that took place after business hours (after 18:00), all failed login attempts during that time require investigation. To filter for these attempts, I created a SQL query, the code for which is presented below.



Retrieve login attempts on specific dates

To investigate any login activity that occurred on 2022-05-09 or the day before due to a suspicious event, I utilized SQL query creation. The following code demonstrates how I filtered for these login attempts.(screenshot cropped due to 75 rows returned).



Retrieve login attempts outside of Mexico

Based on my investigation of the organization's login attempts data, I suspect that there is an issue with login attempts outside of Mexico. As such, it is necessary to investigate these attempts. To filter for login attempts that occurred outside of Mexico, I created a SQL query, the code of which is demonstrated below. (screenshot cropped due to 144 lines returned)



Retrieve employees in Marketing

Updating the computers of specific employees in the Marketing department requires identifying which employee machines to update. To filter for employee machines from employees in the Marketing department in the East building, I utilized SQL query creation, as demonstrated in the following code.



Retrieve employees in Finance or Sales

Obtaining information on which employee machines to update for the Finance and Sales departments requires filtering for employee machines from only these two departments. To do this, I utilized SQL query creation and filtered for employee machines from employees in the Finance or Sales departments, as shown in the following code. (screenshot cropped due to 71 rows returned)



Retrieve all employees not in IT

To perform a security update on employees who are not in the Information Technology department, it is necessary to identify which employee machines require updating. To accomplish this, I created a SQL query to filter for employee machines from employees not in the Information Technology department, as demonstrated by the following code. (screenshot cropped due to 161 rows returned)



Summary

By utilizing SQL queries with filters on the log\_in\_attempts and employees tables, I obtained specific information on login attempts and employee machines. I employed the AND, OR, and NOT operators to filter for the necessary data, and used the LIKE operator and the percentage sign (%) wildcard to search for patterns in the data.