Apply filters to SQL queries

Project description

In this activity, I utilized SQL queries to investigate potential security issues involving login attempts and employee machines at a large organization. By applying filters to the organization's data in the log_in_attempts and employees tables, I retrieved relevant records and gained insights to ensure system security.

Retrieve after hours failed login attempts

To investigate a potential security incident that occurred after business hours, I executed the following SQL query to identify all failed login attempts that took place after 18:00:

```
SELECT event_id, username, login_date, login_time, country, ip_address
FROM log_in_attempts
WHERE success = FALSE AND login_time > '18:00';
```

Retrieve login attempts on specific dates

To examine a suspicious event that occurred on 2022-05-09, I created an SQL query to retrieve all login attempts on that specific date and the day before:

```
SELECT event_id, username, login_date, login_time, country, ip_address
FROM log_in_attempts
WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

Retrieve login attempts outside of Mexico

To investigate suspicious login attempts that did not originate in Mexico, I used the following SQL query with the LIKE keyword to account for variations in country values:

```
SELECT event_id, username, login_date, login_time, country, ip_address
FROM log_in_attempts
WHERE country NOT LIKE 'MEX%';
```

Retrieve employees in Marketing

To obtain information on employees in the Marketing department located in the East building, I executed the following SQL query, utilizing the LIKE keyword to filter for the East building:

```
SELECT employee_id, device_id, username, department, office
FROM employees
WHERE department = 'Marketing' AND office LIKE 'East-%';
```

Retrieve employees in Finance or Sales

To gather details about employees in either the Finance or Sales departments, I used the following SQL query:

```
SELECT employee_id, device_id, username, department, office
FROM employees
WHERE department = 'Finance' OR department = 'Sales';
```

Retrieve all employees not in IT

To identify all employees who are not part of the Information Technology (IT) department, I executed this SQL query:

```
SELECT employee_id, device_id, username, department, office
FROM employees
WHERE department != 'Information Technology';
```

Summary

In this activity, I successfully used SQL queries to investigate potential security issues related to login attempts and employee machines in the organization. By filtering data based on specific criteria, I retrieved valuable information to help maintain system security. These queries showcased my ability to leverage SQL for security investigations, a crucial skill for a security professional.