Apply filters to SQL queries

Project description

In this scenario, I am a security professional at a large organization. Part of my job is to investigate security issues to help keep the system secure. Recently we discovered some potential security issues that involve login attempts and employee machines.

Retrieve after hours failed login attempts

This type of query uses the 'AND' operator to return information that must satisfy both of the criteria listed. This is useful when you want to narrow your query down for more efficient investigative searches.

```
MariaDB [organization]> SELECT*
    -> FROM log_in_attempts
    -> WHERE login_time > '18:00' AND success = 0;
```

Individuals do not usually log-in to an organization's system outside of work hours. This can be seen as an attempt to conduct malicious activities that are otherwise easy to detect during working hours.

Retrieve login attempts on specific dates

This type of query uses the 'OR' operator to return information that meets either or all of the criteria listed. This is useful when trying to investigate different categories of information simultaneously, without having to run a separate query.

```
MariaDB [organization]> SELECT*
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
```

Narrowing the date range of a search query can produce results faster than if you searched without a date range, saving you minutes, which can be vital when conducting time-sensitive