Portfolio Activity: Apply filters to SQL queries

Activity Overview

In this activity, you will create a new portfolio document to demonstrate your experience using SQL. You can add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, read Create a cybersecurity portfolio.

To create your portfolio document, you will review a scenario and follow a series of steps. This scenario is connected to the lab you have just completed about using the AND, OR, and NOT operators in SQL to filter for information. You will explain the queries you performed in that lab, and this will help you prepare for future job interviews and other steps in the hiring process.

Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the scenario below. Then complete the step-by-step instructions.

You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines.

Your task is to examine the organization's data in their **employees** and **log_in_attempts** tables. You'll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

Note: *This scenario involves the same queries as the ones the* ***Filter with AND, OR, and NOT*** *lab. You can revisit the lab to get screenshots to include in your portfolio document. If you choose, it's also possible to complete this activity without revisiting the lab by typing your queries in the template*

Instructions:

1. Retrieve after hours failed login attempts

You recently discovered a potential security incident that occurred after business hours. To investigate this, you need to query the **log_in_attempts** table and review after hours login activity. Use filters in SQL to create a query that identifies all failed login attempts that occurred after 18:00. (The time of the login attempt is found in the **login_time** column. The **success** column contains a value of **0** when a login attempt failed; you can use either a value of **0** or **FALSE** in your query to identify failed login attempts.)

Describe your query and how it works in the Retrieve after hours failed login attempts section of the Apply filters to SQL queries template.

In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template.

2. Retrieve login attempts on specific dates

A suspicious event occurred on 2022-05-09. To investigate this event, you want to review all login attempts which occurred on this day and the day before. Use filters in SQL to create a query that identifies all login attempts that occurred on 2022-05-09 or 2022-05-08. (The date of the login attempt is found in the **login_date** column.)

Describe your query and how it works in the Retrieve login attempts on specific dates section of the Apply filters to SQL queries template.

In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template.

3. Retrieve login attempts outside of Mexico

There's been suspicious activity with login attempts, but the team has determined that this activity didn't originate in Mexico. Now, you need to investigate login attempts that occurred outside of Mexico. Use filters in SQL to create a query that identifies all login attempts that occurred outside of Mexico. (When referring to Mexico, the **country** column contains values of both **MEX** and **MEXICO**, and you need to use the **LIKE** keyword with **%** to make sure your query reflects this.)

Describe your query and how it works in the Retrieve login attempts on specific dates section of the Apply filters to SQL queries template.

In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template.

4. Retrieve employees in Marketing

Your team wants to perform security updates on specific employee machines in the Marketing department. You're responsible for getting information on these employee machines and will need to query the **employees** table. Use filters in SQL to create a query that identifies all employees in the Marketing department for all offices in the East building.

(The department of the employee is found in the **department** column, which contains values that include **Marketing**. The office is found in the office column. Some examples of values in this column are **East-170**, **East-320**, and **North-434**. You'll need to use the **LIKE** keyword with **%** to filter for the East building.)

Describe your query and how it works in the Retrieve employees in Marketing section of the Apply filters to SQL queries template.

In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template.

5. Retrieve employees in Finance or Sales

Your team now needs to perform a different security update on machines for employees in the Sales and Finance departments. Use filters in SQL to create a query that identifies all employees in the Sales or Finance departments. (The department of the employee is found in the **department** column, which contains values that include **Sales** and **Finance**.)

Describe your query and how it works in the Retrieve employees in Finance or Sales section of the Apply filters to SQL queries template.

In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template.

6. Retrieve all employees not in IT

Your team needs to make one more update to employee machines. The employees who are in the Information Technology department already had this update, but employees in all other departments need it. Use filters in SQL to create a query which identifies all employees not in the IT department. (The department of the employee is found in the **department** column, which contains values that include **Information Technology**.)

Describe your query and how it works in the Retrieve all employees not in IT section of the Apply filters to SQL queries template.

In the **Filter with AND, OR, and NOT** lab, take a screenshot of the SQL query you used and copy it into the template. Or, type this query directly into the template.

7. Finalize your document

To finalize the document and make its purpose clear to potential employers, be sure to complete the Project description and Summary sections of the Apply filters to SQL queries template.

In the Project description section, give a general overview of the scenario and what you accomplish through SQL. Write two to four sentences.

In the Summary section, provide a short summary of the previous tasks and connect them to the scenario. Write approximately two to four sentences.

What to Include in Your Response

Be sure to include the following in your completed activity:

- Screenshots of your queries or typed versions of the queries
- Explanations of your queries
- A project description at the beginning
- A summary at the end
- Details on using **LIKE** to search for a pattern
- Details on filtering for dates and times
- Details on using **AND** and **OR** to filter on multiple conditions

Details on using **NOT** in filters