Filters with AND, OR, and NOT

In the previous lesson, we learned about even more ways to filter queries in SQL to work with some typical security analyst tasks.
However, when working with real security questions, we often have to filter for multiple conditions.
Vulnerabilities, for instance, might depend on more than one factor.
For example, a security vulnerability might be related to machines using a specific email client on a specific operating system.
So, to find the possible vulnerabilities, we need to find machines using both the email client and the operating system.

To make a query with multiple conditions that must be met, we use the AND operator between two separate conditions.
AND is an operator that specifies that both conditions must be met simultaneously.
Bringing this back to our fruit and vegetable analogy, this is the same as asking someone to select apples from the big box where the apples are large and fresh.
This means our results won't include any small apples even if they're fresh, or any rotten apples even if they're large.
They'll only include large fresh apples.
The apples must meet both conditions.

Going back to our database, the machines table lists all operating systems and email clients.
We want a list of machines running Operating System 1 and a list of machines using Email Client 1.
We'll use the left and right circles in the Venn diagram to represent these groups.
We need SQL to select the machines that have both OS 1 and Email Client 1.
The filled-in area at the intersection of these circles represents this condition.
Let's take this and implement it in SQL.

First, we're going to start by building the first lines of the query, telling SQL to SELECT* all columns FROM the machines table.
Then, we'll add the WHERE clause.
Let's examine this more closely.
First, we indicate the first condition that it must meet, that the operating system column has a value of '0S 1'

Then, we use AND to join this to another condition.
And finally, we enter the other condition, in this case that the email client column should have a value of 'Email Client 1'
And this is how you use the AND operator in SQL!
Let's run this to get the query results.
Perfect! All the results match both our conditions!

Let's keep going and explore more ways to combine different conditions by working with the OR operator.

The OR operator is an operator that specifies that either condition can be met.
In a Venn diagram, let's say each circle represents a condition.
When they are joined with OR,
SQL would select all rows that satisfy one of the conditions.
And it's also ok if it meets both conditions.

Let's run another query and use the OR operator.
Let's say that we wanted the filter to identify machines that have either OS 1 or OS 3 because both types need a patch.
We'll type in these conditions.

Let's examine this more closely.
After WHERE, our first condition indicates we want to filter, so that the query selects machines with 'OS 1'
We use the OR operator because we also want to find records that match another condition.
This additional condition is placed after OR and indicates to also select machines running 'OS 3'
Executing the query, our results now include records that have a value of either OS 1 or OS 3 in the operating system column.
Good job, we're running some complex queries.

The last operator we're going to go into is the NOT operator.
NOT negates a condition.
In a diagram, we can show this by selecting every entry that does not match our condition.
The condition is represented by the circle.
The filled-in portion outside the circle represents what gets returned.
This is all data that does not match the condition.
For example, when picking out fruit, you can be looking for any fruit that is not an apple.
That is a lot more efficient than telling your friend you want a banana or an orange or a lime, and so on.

Suppose you wanted to update all of the devices in your company except for the ones using OS 3.
Bringing this into SQL, we can write this query.

We place NOT after WHERE and before the condition of the filter.
Executing these queries gives us the list of all the machines that aren't running OS 3, and now we know which machines to update.

That was a lot of new content that we just looked into, but you're learning more and more SQL that you can use on your journey to become an analyst!
In the next video, we'll be learning how to combine and join two tables together to expand the kinds of queries we can run. I'll meet you there!

Revision #1
Created 2023-07-10 12:24:51 UTC by naruzkurai
Updated 2023-07-10 12:28:18 UTC by naruzkurai