Filter dates and numbers

In this video, we're going to continue using SQL queries and filters, but now we're going to apply them to new data types.
First, let's explore the three common data types that you will find in databases:
string, numeric, and date and time.
String data is data consisting of an ordered sequence of characters.
These characters could be numbers, letters, or symbols.
For example, you'll encounter string data in user names, such as a user name: analyst10.
Numeric data is data consisting of numbers, such as a count of log-in attempts.
Unlike strings, mathematical operations can be used on numeric data, like multiplication or addition.
Date and time data refers to data representing a date and/or time.

Previously, we applied filters using string data, but now let's work with numeric and date and time data.
As a security analyst, you'll often need to query numbers and dates.
For example, we could filter patch dates to find machines that need an update, or we could filter log-in attempts to return only
those made in a certain period of time.
We learned about operators in the last video, and we're going to use them again for numbers and dates.

Common operators for working with numeric or date and time data types include: equals, greater than, less than, not equal to, greater than or equal to, and less than or equal to.
Let's say you want to find the log-in attempts made after 6 pm.
Because this is past normal business hours, you want to look for suspicious patterns.
You can identify these attempts by using the greater than operator in your filter.
We'll start writing our query in SQL.
We begin by indicating that we want to select all columns FROM the log_in_attempts table.
Then we'll add our filter with WHERE.

Our condition indicates that the value in the time column must be greater than, or for dates and times, later than '18:00', which is how 6 pm is written in SQL.
Let's run this and examine the output.
Perfect! Now we have a list of log-in attempts made after 6 pm.

We can also filter for numbers and dates by using the BETWEEN operator.
BETWEEN is an operator that filters for numbers or dates within a range.
An example of this would be when looking for all patches installed within a certain range.
Let's do this! Let's find all the patches installed between March 1st, 2021 and September 1st, 2021.
In our query, we start with selecting all records FROM the machines table.

And we add the BETWEEN operator in the WHERE statement.

Let's break down the statement.
First, after WHERE, we indicate which column to filter, in our case, OS_patch_date.
Next, comes our operator BETWEEN.
We then add the beginning of our range, type AND, then finish by adding the end of our range and a semicolon.
Now, let's run this and explore the output.
And now we have a list of all machines patched between those two dates!

Before we wrap up, an important thing to note is that when we filter for strings,
dates, and times, we use quotation marks to specify what we're looking for.
However, for numbers, we don't use quotation marks.
With this new knowledge, you're now ready to work on all sorts of interesting filters for numbers and dates.
In the next video, we'll be able to expand our filtering even further by using multiple conditions in one query.

Revision #1
Created 10 July 2023 11:27:38 by naruzkurai
Updated 10 July 2023 12:09:51 by naruzkurai