TYPE=Regex rule match timed out. SORC=LogRhythm MPE EVID=2052. MESG=Regex rule match timed out. MsgSourceId = 167, MPERuleRegexID = 1009495, Base MPERuleID = 1489727, Rule Name = USERID Messages, KB Version = 7.1.629.0, Timeout = 100ms, MsgSourceTypeID = 1000134, PolicyID = -1000134, RawLog = 01 20 2022 01:50:03 10.195.1.200 <LOC4:INFO> Jan 20 01:50:03 TIM-bdr-fwl01.bench.com 1,2022/01/20 01:50:03,016201020154,USERID,login,2560,2022/01/20 01:50:03,vsys1,10.1.99.3,bei\sartpn,corp-pa-id01,0,1,2700,0,0,agent,,1244932951,0x0,494,940,0,0,,TIM-bdr-fwl01,1,,2022/01/20 01:50:02,1,0x0,bei\sartpn,,2022-01-20T01:50:03.835-08:00

Next Step

Trim the timeout headers to make manual test samples. I did this by applying the function =right(A2,len(A2)-286 I determined 286 by analyzing the number of characters in the log above.

This provided so each log would start with “RawLog =).

I then ensured that all of these logs indeed started with that.

I then repeated the function above but exchanged the numeric for =right(B2,len(B2)-9

I used 9 because “RawLog = “ is 9 characters. Also notice that I changed the cell to B2 and not A2. The reason is because you are applying a function to the results of a previous function. If you use A2 you will get results just not the ones you are looking for.

The reason for doing this in two steps is to account for character fluctuation in the timeout messages themselves

You will have to cut them out to a new excel sheet. If you use “copy” the reference to the function stays in that cell and you can’t put it on a new sheet.

Once you have it on a new sheet. Save it as a CSV. This is essentially saving the data as it is seen and it will drop the formulas. If you need to filter it more later then you simply load the data via csv in excel.

Line 930: 03/19/2022 10:07:46.216046 [USDFW11AS170V]

=right(A5,len(A5)-52