Jacob Cannamela

CSD310

11/16/2024

Module 5.2 Assignment

**Go out to the W3Schools links above, and select at least three functions to experiment with.**

I chose the functions *as*, *group by*, and *case*.

The *as* function is used to create an alias for the duration of the query. I use this all the time for my job as a threat detection engineer while working in splunk. Often a log will contain a field that I do not think has the best naming convention. So, I rename the field using the *as* function to ensure the table output looks the way I want. The field may be called “dstip” and I would use dstip *as* destination\_ip. The *group by* function will group results by one or more columns. I use this function all the time when I create detections in splunk for work. I will often do a *group by* IP address, computer name, or username to see all the different things per user/ip/computer that I am interested in. Example would be, if I know there is a malicious file that ran in our company, I could *group by* computername to find the unique computernames that executed my file. The *case* function is another function I use often for my job. The *case* function is treated as an “if this then that” operator. I use this on the job when writing queries against a data set often. One of the prime examples is when computername ran file xyz then value=infected. This is a very simplified version of how I use this command for work.

**I am confused about this instruction “Provide an appropriate alias for the column header in the results.”**

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated