This is a brief documentation on my thought process on how I completed this project. My first step was to make a list of steps that would need to be taken to complete this project. This list included the following: Find the appropriate documentation necessary to install and configure Logstash, Install Logstash, Create the filter necessary to parse the data and Document my findings on Github. After finding the documentation, I attempted to install Logstash on a Windows machine and then a Linux Debian 11 machine as I did not have experience installing this program. I quickly learned that Debian 11 would be the best choice for me. I adopted a trail and error testing methodology as I did not have any experience with Logstash. I started with creating a list of standardized keywords that would become the anchor points in my configuration file. These words are as follows: alertname, computername, computerip and severity. The values that followed these words are the values that need to be returned in the output. I is my assumption that regardless of the values that needed to be returned these keywords would not change. While I started my project with the use of the JSON filter that is default with Logstash, I was not having much success parsing this log completely. I continued to work with this filter until I realized that the issue was with my computer. It crashed and I lost all my testing data. I rebuilt another Debian 11 box on Monday and installed Logstash. I also realized that while JSON would be the ideal filter, I needed to switch to using GROK to parse my log statement. I used the trail and error methodology with pointed knowledge of what I wanted returned and what I did not want hidden.