Short write up of solution for Teleng\_challenge – Mark Lavallee

This was fun!

My solution is pretty simple, it take the input via CLI and then filters it, outputting both to the screen and a file. I used filters to devide the log into two sections – a syslog section and a “foo=bar” section. For the syslog I used grok to separate the sections but also grab some extra data and set them to variables I felt would be good to have. For the foo=bar section I used the KV filter to parse the event fields in the post grok message, the mutate filter to do some house cleaning and renaming of fields, and finally, the translate filter to translate the severity from an integer to a string with defined values. I sued the stdout and file output plugins to view the results and write to a file.