Mark Lavallee

TelEng\_Skills\_Challenge

Short Description

Fun challenge! I created a simple config file with cli input, and just pasted the log into logstash from the cli.

In the config file I used grok, which I didn’t use last time, and I enjoyed getting a better understanding of grok filters. Once I had things “groked out” the way I wanted, I used a transform plugin to change the severity from an int to a string using predefined values in a dictionary.

My output was to the cli and also to a json file called “output.json” using the json codec. I added a few different fields beyond what was asked, such as and antivirus process or event id (I called it process id), and also differentiated between the metadata timestamp and the event timestamp.

I appreciate the opportunity and your consideration!

Thank you,

Mark