Noah Bergeron

August 17, 2022

Data is ingested into Logstash by inputting a file. We can then take that file and parse the data into specific readable fields. Once the data is parsed we output that information to a file so we can look over the data. For me, I was able to output the data to a JSON file to be able to see the Syslog separated into specific fields and view it as normalized. Taking a log file that is almost unrecognizable and being able to normalize it to a readable report that you can visualize is crucial to a company’s security. From that report, you can analyze the data and add security protection.

A challenge that I ran into was parsing data and getting my code to perform correctly. This was a big setback for me as there are so many ways to parse data. Troubleshooting steps that I took include going to the discussion forums on elastic.co and reviewing filter plugins on GitHub. After numerous attempts, I reached out to the Cyderes team. After receiving feedback from Samuel Johnson, I went back and utilized the GREEDYDATA Grok Pattern. This helped tremendously as I was able to get some data to parse. Within Elastic, Dev-Tools, I got to work with the Grok Debugger which was helpful. I could enter the log and visually see the parsed structured data. Ultimately, I was not able to complete the skills challenge because I could not get the filter section to work. However, I did come close as some of my data was parsing. I learned a lot about Logstash, Elastic, and Kibana while working on this project and hope to be able to use this acquired knowledge moving forward.