Below you will find the technical CYDERES Telemetry Skills challenge. We hope you find this to be challenging, rewarding, and it is enjoyable discovering some of these tools if you haven’t used them already!

Please provide a public Git repository with the finished challenge by March 8th , 2023.

**Summary:**

We would like to see your ability to learn new technologies quickly as well as your ability to execute in a timely manner. The skills we would like to see from you:

* Install Logstash. This can be on a PC/laptop or in a virtual machine.
* Create a Logstash configuration file. The Logstash configuration file should do the following:
* Allow for ingestion of the **Security Log Data** below via a “Logstash Input Plugin”, your choice.
* Allow for output of data via a “Logstash Output Plugin”, your choice.
* Utilizing any number of “Logstash Filter Plugins”, transform data from the **Security Log Data** from its original format to a normalized structure described below.
* Design your solution so that a different piece of **Security Log Data** structured the same, but containing different data in the log message, could be ingested and achieve a similar output based on the data contained within the log.
* Send the **Security Log Data** example to Logstash and capture the output from Logstash in some form (text, screenshot, etc). Include this in the Git repo.
* Save the Logstash configuration created above in a public Git repo.
* Write a short description of how data is ingested and output from Logstash based on your solution. Include this write-up in the Git repo.

**Security Log Data:**

<14>1 2016-12-25T09:03:52.754646-06:00 contosohost1 antivirus 2496 - - alertname="Virus Found" computername="contosopc42" computerip="216.58.194.142" severity="1"

**Output as JSON formatted data containing (but not exclusively) the following fields:**

description: "Virus Found"

hostname: "contosopc42"

source\_ip: "216.58.194.142"

severity: "High"

**What we are mainly looking for:**

* Using Logstash to ingest and output data
* Understanding of how data can be normalized before storage, related to in SIEM products in this challenge
* Preferences for methodology in completing the tasks
* Communication of the solution designed
* Ability to use Git

**When you are finished:** 

Provide a link to the Git repo which will include:

* The Logstash configuration file
* Short paragraph write up of the solution
* Any relevant information showing successful output from Logstash

**Run into issues?**   
   
If there is a part of the instructions that are not clear, please email [Jonas.harris@cyderes.com](mailto:Jonas.harris@cyderes.com) or [Matt.mcginnis@cyderes.com](mailto:Matt.mcginnis@cyderes.com) for clarification. This skills challenge can be accepted incomplete, however, please outline any difficulties encountered and troubleshooting steps taken to overcome those issues in your final write up of the solution.