Skill Assessment Test for Cyber Analytic Engineer

A. Automation Scripting

1. Provide a script to automate the extraction of IP addresses, URLs and hashes from the following cyber threat report.

   “Win32/INDUSTROYER A new threat for industrial control system”
   (https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf)

   You can use any open source tools and library to help with the extraction.

2. With the IP addresses extracted from the pdf document, develop a python script to resolve the autonomous system number (ASN) and Country code for each IP address. The output should be in a CSV file. You can use any open source library to develop the python script.

B. Cyber Threat Analysis

Provide a write-up for the following.

1. From the extracted IOCs, outline the type of enrichments that can facilitate cyber threat investigation.

2. How would you surface potential additional unknown IOCs from this list of IOCs from the report?

C. Analytics Development

1. Design an algorithm to shortlist IPs that could be running reconnaissance activities against an enterprise web server. State any assumption you make in your design. Use the dataset in the following link to develop a prototype of the algorithm.

   https://www.secrepo.com/maccdc2012/http.log.gz