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

investigation.

IP addresses can be enriched by retrieving the geolocations of potential attacks. In the case of prevention, we can block certain types of contents depending on the geolocation of the user, as well as blocking any IPs that comes from hotspots for malicious activities. As for the case of investigation of a cyber attack, for example DDoS attacks, the enriched data enables us to identify IP locations of the machines making the attacks which might help in preventing future occurrences of such attacks.

URLs can also be enriched to retrieve the full-length URL as an attacker might shorten it in an attempt to disguise itself. This enriched data can then be used to reduce malware incidents by blocking own users’ access to known malicious sites.

Hashes can also be enriched to retrieve information such as number of times the files were executed and first and last execution time to determine how much damage has been caused by these files.

1. How would you surface potentially unknown IOCs from the list of IOCs in the report?

Geographical irregularities can be surfaced by inspecting the geolocation of the IP addresses as when there are login attempts from countries that have no relations to the business and/or locations that are hotspots for malicious activities, it may be a sign of a security compromise and/or a sign of potential cyber attack.

Upon retrieving the name, email address or phone number, potentially unknown IOCs such as social networks, public records and etc could also be extracted from online sources. Using this information, further analysis could be done such as social network analysis, to identify the person’s social network map to determine if any relationship with malicious personnels exists.

Using the hashes, IOCs such as files behaviour (E.g. how many times the files were executed), potential damage as well as the pattern of traversal can also be derived.

From the domain names, web searches can be done to determine if the domain is of malicious intent.