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

IOC are Indicator of Compromise which are data that indicate that the security of the network has been compromised or breached. IOC are used to provide information about the perpetrator and includes information such as IP address, domain name, hash and email addresses.

Some enrichments that can facilitate a cyber threat investigation are:

1. Geolocation

This step involves finding the physical location of the IOC by using means such as ip address or domain name. If the ip address or domain name comes from a country where the organization has no presence in, this could be a possibility of a cyber-attack.

1. Increase in incorrect log-ins or access requests

An increase in login attempts may indicate a brute force attack by the perpetrator whereby they may be searching for a vulnerability in the system and preparing for a large scale attack.

1. Historical Analysis

This involve analysing past IOC to determine if the perpetrator was involved in any past attack or have a malicious behavior in general.

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

To uncover unknown IOCs from a list of IOCs, one can do:

* Pattern matching. Pattern matching can be used to discover certain IOC that matches certain patterns. For example, matching IOC to a known malicious email address or ip address.
* Past threat intelligence reports. Study past reports to have an idea of what unknown IOC might appear.
* Machine Learning: Using machine learning involves using past data to train the model. It helps to identify anomalies and learn the pattern of IOC. This model can then be used to identify unknown IOC which may have similar patterns.