# B. Cyber Threat Analysis

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

In part A, we extracted IP addresses, URLs and hashes from the PDF. For the IP addresses, we resolved the ASN and Country code. From the ASN and Country code, we can figure out where the IP address came from and possibly identify who launch the attack. However, we also need to be mindful that the IP addresses can be spoofed. From the ASN and Country code found, we can also flag out other potential unknown IOCs by linking IP addresses that falls in the same ASN as the extracted IOCs, or they come from countries that we have no relation to.

With reference to Anton Chuvakin’s article[[1]](#footnote-1), we can enrich the data through

1. Linking

* Store data in the way each enables easy searching.
* Fast retrieval and organised data can help in analysis.

1. Enriching

* To get Whois data, geographical location, file reputation, etc.
* We did this in part A, but we can extract more information such as whether there are reports of malicious activity from the IOCs

1. Relating

* Linking IP to domain to URL to malware
* Instead of focusing on the IOC obtained, we look into its chain of occurrences.

1. Validating

* Using known malware list to validate if an information obtained is useful.
* Reduces the need for the team to go through redundant data.

1. Contextualising

* Cross referencing data with observations and event that happened
* Flag out data that is linked to a threat actor

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

According to Recorded Future[[2]](#footnote-2), they explored three ways of assessing IP address risk.

1. Ranking ASNs and associated countries based on the total number of risky IP addresses in the ASN

* This is not the best way to accesses the riskiness as it depends on the size of the ASNs in each country. Countries with more and larger ASNs are able to distribute the risk across the country.

1. Ranking ASNs based on the percentage of risky IP addresses it contains

* We are assuming that IP addresses from the same ASN are generally in the same area and hence could be from the same attacker.

1. Ranking ASNs based on IP addresses explicitly associated with malware

* This is a stricter assessment, but it depends on how updated the list of IP addresses associated with malwares.

The list of IOCs from the report has a small sample size so we would not be able to get an accurate analysis as what Record Future did. However, we can still surface potential unknown IOC’s by flagging out IP addresses which have the same ASN as the IOCs in the report. We can also reference potential unknown IOCs with by checking if they have the same ASN as those in the list of IP addresses associated with malware.

For this report I only extracted IOC from readable text in the PDF. I can also look into the metadata of the PDF to check for embedded IOCs.

1. <https://blogs.gartner.com/anton-chuvakin/2014/02/19/how-to-make-better-threat-intelligence-out-of-threat-intelligence-data/> [↑](#footnote-ref-1)
2. <https://www.itproportal.com/features/from-chasing-risk-lists-to-asn-policies-large-scale-analysis-of-risky-internet-activity/> [↑](#footnote-ref-2)