1. **<u>From the extracted IOCs, outline the type of enrichments that can facilitate cyber threat investigations.</u>**

Different cyber threat investigations would require different sets of IOCs depending on their individual motivation and aim.
If the aim is to investigate if a breach has occurred, or to blacklist a compromised network or host, we can enrich the data with network/host artifacts like the internet provider or datacenter hosting the IP address and the domain name will help us better understand typical host information to look for.
However if the aim is to generate higher forms of cyber intelligence to defend against future attacks, it might not be sufficient as such information is often volatile and easy to change. Instead, we should focus on tactics, tools and procedures. Information like how the typical initial compromise occurs, how privileges were escalated, or even related CVE vulnerabilities would provide a better view of the typical behaviour and attack vector used by the adversary. A database of such information can be built and enhanced with other intelligence feed, to enhance the IDS or threat hunting capabilities.

2. **<u>How would you surface potential additional unknown IOCs from this list of IOCs from the report?</u>**

For domain name or host information, a simple lookup is often enough. IP addresses could be used to search for the related domain name or internet provider. Simple scripts could be used to automate such processes.
However if we are looking for information regarding TTPs, then a simple script is often insufficient as such data spans across files of different formats, often in an unstructured way. Published papers or articles need to be parsed and normalized before it can be aggregated and stored. Such often require the use of Natural language processing modules. Such information could be passed to machine learning algorithms to generate intelligence which traditional methods are not able to.