Provide a write-up for the following.

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

**Indicators of compromise** or **IOCs** as commonly provides some form evidence on a computing device that the security of the network has been breached or compromised. By monitoring for indicators of compromise, organizations can detect attacks and act quickly to prevent breaches from occurring or limiting damages by stopping attacks at the onset.

From my understanding of the question and the Pyramid-of-Pain (PoP), the extracted IOCs are from the lowest level of the structure which means they are generally easy for defenders to gather and protect the infrastructure. However, cyber threat investigators shouldn’t take too much pride in this as attackers just needs to only recompile code with some trivial changes, thereby changing the hash to form a new attack strategy.

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

From the perspective of uncovering additional unknown IOCs, I would utilise an up-to-date IOCs in my network defender setup in conjunction with historic data, such as logged DNS queries or email attachment hashes, to hunt for signs of past compromise. Not only can this technique help to build up a clear picture of past attacks, but it also allows for retrospective mitigation of the effects of any previous intrusion.

Through this approach, I am able to analyse patterns of specific IOCs or discover recurrence and update my security tools and policies to protect against future attacks.

From the perspective of helping the wider IT community, I would also share these results in a consistent, well-structured manner (i.e. Structured Threat Information Expression STIX)) to help other companies and IT professionals in improving their incident response and computer forensics.