This document will outline the possible enrichment steps that can be taken for IP addresses, URLs and hashes.

1. For hashes, using sites like VirusTotal, AlienVault OTX or Joe Sandbox (malware sandbox) will provide additional information on the sample. For example, using VirusTotal we can obtain SSDeep, Imphash and TLSH hashes. These can be used for similarity analysis with other samples. It could also be used to threat hunt for existence of samples within the same family.  
     
   Additionally, it also provides additional information such as the different names the files may appear under from previous analysis, the IP address and the domain names that the file may connect to, as well as files that were dropped from the execution of the application. This could be useful as it is computationally intensive to obtain the hash for every file on the system, and other attributes such as the file name could be used as an alternative to perform threat hunting on systems.  
     
   Furthermore, if the site further reveals that the application is signed with a valid Authenticode signature (Windows), it could also indicate a potential supply chain attack and could help to identify the user/organisation that had the certificate compromised, helpful in an investigation. This could tie in with the enrichment of domains in bullet point 3.  
     
   Virustotal also provides additional enrichment information that tells us about the file itself. If it is an application, it provides information such as entropy, an indicator of whether a packer could have been used to obfuscate data/payloads.
2. For IP addresses, we can gather information on the domains that are hosted on that IP address. To do so, we can perform a reverse IP lookup. Additionally, we can check the reputation of the IP address to see if it is a known IP address that has been known to be a phishing site or delivering malware by using sites such as AbuseIPDB.  
     
   For domains obtained through reverse IP lookup, we can perform further analysis from information in bullet point 3.  
     
   We can also check what applications are running on those IP addresses using services such as Shodan. This gives us additional information on the infrastructure of the threat actor. For example, if TCP port 50050 is open then there is a possible indication that Cobalt Strike is running.
3. For URLs, the main focus is the domain. In addition to checking the reputation of the IP address using AbuseIPDB, VirusTotal, we can perform an additional check that gives us information on the person/organisation that registered the domain (assuming domain privacy is not enabled). This gives us information on the contact details of the user/organisation, the registrar that registered the domain, the nameservers, whether the domain is protected by a loud balancer (such as Cloudflare), the country and several other details. Using this, we can also perform a reverse whois lookup to determine whether the user/organisation is affiliated with any other domains, useful in potentially locating other compromised domains.