Section B

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

There are 3 main types of IOCs extracted – Domain name, IP address and hashes.

To facilitate cyber threat investigation, WHOIS lookup can be performed on the IP addresses or domain names to obtain the registered owner along with contact and address information. In addition, from the IP address, the geographical location of the IOC can be determined.

Making use of the IP address, reverse IP lookup can be performed to find all the suspicious hostnames linked to a particular IP address. In addition, reverse DNS lookup may be performed to obtain further information for cyber threat investigation.

The file hashes could also be enriched for cyber threat investigation. From historical log files, the hash of files in the system can be compared to the IOC hashes to determine whether the enterprise has been attacked by this particular threat and determine the extent of damage. From this, other IOCs such as IP addresses that sent the file into the system can be uncovered and further investigated. Furthermore, by comparing the hash with threat intelligence feeds, further information about the type of file and what potential malicious activities that the file may perform can be obtained.

Question 2 How would you surface potentially unknown IOCs from the list of IOCs in the report?

Using the enrichment as mentioned in the previous question, potential IOCs can be surfaced.

Using WHOIS lookup, potential IOCs can be surfaced by investigating more about the registered owner or organisation and domains or IP addresses associated with this registered entity. Through reverse IP lookup, suspicious hostnames can be surfaced.

From historical log files, the trace of how a particular malicious file with hash similar to a hash IOC can be determined. This allows for the surfacing of related IP addresses or hostnames that have handled the file, potentially surfacing unknown IOCs. This is further complemented by looking at DNS logs if present.

References

1. *Reverse IP Lookup, find hosts sharing an IP*. HackerTarget.com. (2022, February 1). https://hackertarget.com/reverse-ip-lookup/
2. ManageEngine Log360. (n.d.). Threat hunting: MD5 hash IoCs. https://www.manageengine.com/products/eventlog/cyber-security/md5-hash-iocs.html
3. Hogg, S. (2020, May 6). *Improved security through DNS inspection (part 1)*. Infoblox Blog. https://blogs.infoblox.com/ipv6-coe/improved-security-through-dns-inspection-part-1/