**B. Cyber Threat Analysis**

**Provide a write-up for the following.**

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

The extracted IOCs include IP addresses, URLs, and hashes.

Some methods to enrich IP addresses include:

* Resolving IP to Hostname or domain name system (DNS)
* Separate between internal and external IP addresses
  + For internal IP addresses, get host information
  + For external IP addresses, get IP reputation
* Compare IP to a constantly updated list of blacklisted IPs

Some outputs from enriching IP addresses include:

* Endpoint hostname
* Endpoint domain name
* Endpoint operating system (OS)
* A list of Endpoint IP addresses
* A list of Endpoint MAC addresses
* IP reliability
* Type of host
* Risk level
* IP country of origin
* IP city of origin
* Geolocated latitude and longitude of the IP (GeoIP)
* Shodan data
* VirusTotal data
* PassiveTotal data

Some methods to enrich URLs include:

* Verify URL Secure Sockets Layer (SSL)
* Provide URL reputation
* Rasterize URL
* Automating phishing detection and remediation

Some outputs from enriching URLs include:

* Whether the URL was detected as malicious or not
* Name of vendor who labeled the URL as malicious
* Additional information on the URL
* GeoIP
* Screenshots
* HTML and text

Some methods to enrich hashes include:

* Search Endpoints by Hash
* Analyse file by Hash
* Retrieving file paths by Hash

Some outputs from enriching hashes include:

* Whether the hash was found in the approved hash list or not
* Endpoint device hostname
* Description of the malicious file
* MD5, SHA1, and SHA256 of the file
* File size
* Name of vendor who labeled the file as malicious
* Count the number of devices the hash ran on
* Path of the requested file
* Processes executed by such malicious files
* Command and control (C2) servers and IP addresses the files are associated with
* Type of attack carried out by these files

1. **How would you surface potentially unknown IOCs from the list of IOCs in the report?**

By disseminating the IOCs across the community of cyber threat analysts, potentially unknown IOCs can be discovered from a list of IOCs. Such a culture of knowledge sharing can enhance an organization's incident response and remediation strategies.

Another way is to make use of artificial intelligence (AI) and machine learning methods to detect suspicious activities that security tools may miss. These techniques will serve to be effective as data grows. In the area of network traffic analysis, abnormal or outlier traffic patterns can be detected using clustering approach and raise an alert. Thus, the security team can flag out the IOCs even though they are initially unknown. According to <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9448097>, machine learning can be used to predict vulnerabilities and IOCs, such as unknown attacks, alteration, deletions, exfiltration and redirections that the threat actor could deploy on the system, using cyber threat analysis and input features such as the threat actors’ capability and attack vector, and tools.