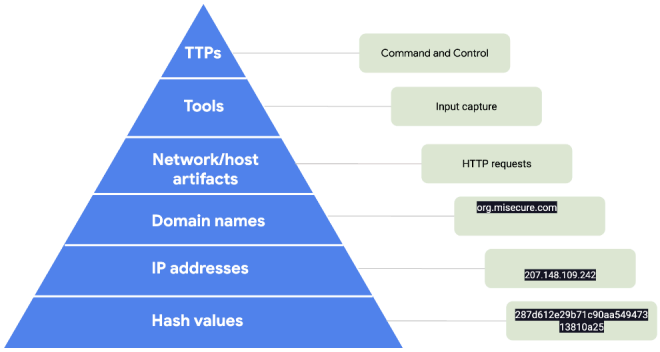
Date: 02/09/2025	**Entry:** Investigate a suspicious file hash
Description	You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer. You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file, password was provided in the email. The employee downloaded the file, entered password, which opened the file. When the employee opened the file, a malicious payload was then executed on their computer. You retrieve the malicious file and create a SHA256 hash of the file (hash function is an algorithm that produces a code that can't be decrypted). Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint. A level-one SOC analyst at a financial services company investigates a phishing attack. An employee downloaded a password-protected spreadsheet, triggering a malicious payload. Using VirusTotal, the analyst verifies the SHA256 hash, confirming malware (59/72 detection score). Key IoCs include the hash value, IP address, and domain name. The incident falls under **Detection & Analysis**, identifying malware via VirusTotal, and potentially **Containment** if mitigation steps followed.

Date: 02/09/2025	**Entry:** Investigate a suspicious file hash
Tool(s) used	Google Chrome Pyramid of Pain VirusTotal-service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content. Through crowdsourcing, VirusTotal gathers and reports on threat intelligence from the global cybersecurity community. This helps security analysts determine which IoCs have been reported as malicious. Pyramid of Pain- Powerpoint

The 5 W's	• **Who**: level one security operations center (SOC) analyst at a financial services company -Employee
	• **What**: pyramid of pain-attached below (PHISHING via email)
	  ○ The SHA256 file hash which we will be verifying
	• **Where**:VirusTotal
	• **When:**
	  ○ 1:11 p.m.: An employee receives an email containing a file attachment.
	  ○ 1:13 p.m.: The employee successfully downloads and opens the file.
	  ○ 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer.
	  ○ 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC.
	• **Why:** Determining whether the file is malicious, which gurns out to be. Score of 59/72, as well as a -226 community score that verifies malware detections and flagpro malware.

Date: 02/09/2025	**Entry:** Investigate a suspicious file hash
Additional notes	**Has this file been identified as malicious? Explain why or why not.** YES. 59/72 Vendors Score -226 Community Score Malware Detections -Security Vendors' Analysis: Flagpro malware This file has been identified as malicious after confirming with the help of VirusTotal. Once accessing the file, we can see that there is a score of 59/72 which causes concerns as the higher the number is the more likely it is a malicious virus. Furthermore, the file as a community score of -226 indicating there is a maliciousness malware within the file. The last identifier is that we can see the flagpro malware within the links of multiple files therefore we can confirm, it is malicious.  3 IoCs = Hash Value, IP address, domain name