Scenario 2:

You are a level one security operations centre (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. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open 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. You might recall from a previous course that a **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.

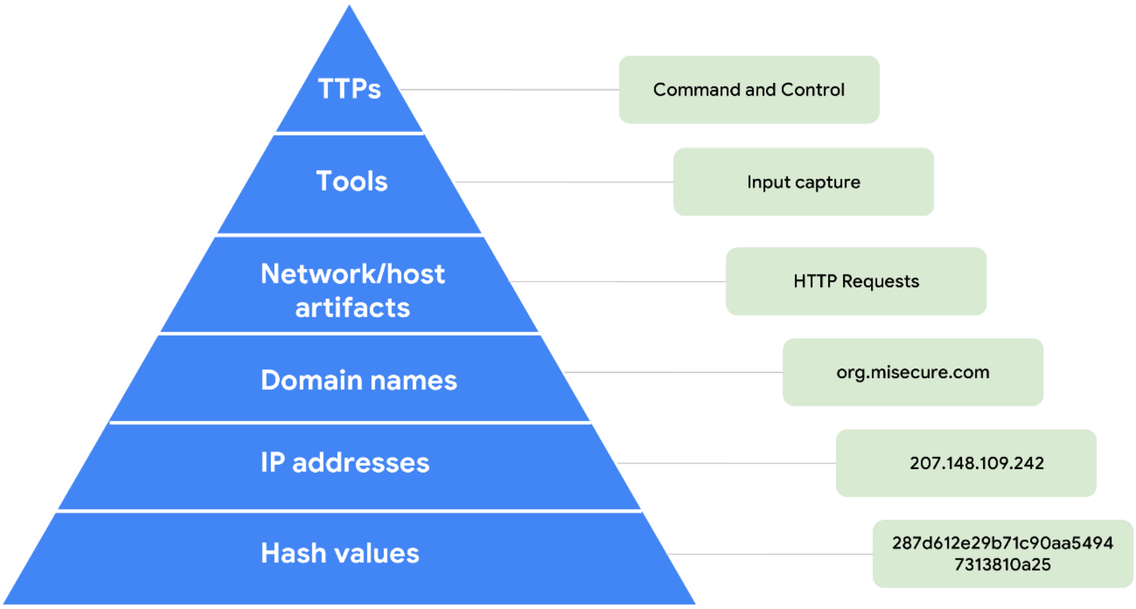
Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.

Date: **July 27 2024**.	**Entry:** # 1
Description	This incident took place during the Detection and Analysis phase. In this scenario, I investigated a suspicious file hash to determine whether it represented a legitimate threat. By analyzing the SHA256 file hash, 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b, I evaluated its characteristics to confirm if the alert warranted further action. This analysis helped identify the presence of potential malicious activity.

Tool(s) used	For this activity, I utilized VirusTotal, an investigative tool used to analyze files and URLs for malicious content, including viruses, worms, and trojans. VirusTotal is particularly helpful for quickly checking if an indicator of compromise, such as a website or file, has been flagged as malicious by others in the cybersecurity community. In this scenario, I acted as a security analyst within a Security Operations Centre (SOC) during the Detection and Analysis phase. After a suspicious file hash was flagged by the organization's security systems, I used VirusTotal to analyze the hash. The analysis revealed that the file was reported as malicious. This deeper investigation allowed me to confirm the nature of the threat and determine the necessary next steps.
The 5 W's	● **Who** caused the incident? A malicious cybercriminal initiated the attack. ● **What** happened? The incident involved an email sent to an employee that contained a malicious file attachment. The file was identified by the SHA-256 hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **Where** did the incident happen? The incident occurred on an employee's computer at a financial service company ● **When** did the incident occur? At 1:20 p.m., the organization's intrusion detection system detected the malicious file and sent an alert to the Security Operations Centre (SOC). ● **Why** did the incident happen? The incident happened because the employee received an email with a malicious attachment, downloaded it, and executed the file, enabling the threat actor's access.

Additional notes	**Preventative Measures:** • Employees should be trained to never download or open suspicious file attachments from emails. • Enhancing security awareness training is critical to ensure that employees are better equipped to recognize and avoid potential phishing attacks. • Additionally, this incident should be escalated to a Level 2 SOC Analyst for further investigation and response. • Depending on the organization's playbook, the process for handling such incidents may vary, but involving higher-level analysts ensures a thorough assessment and mitigation plan.

Pyramid of Pain



Has this file hash been reported as malicious? Explain why or why not.

The file hash has been flagged as malicious by numerous third-party vendors, with over 50 vendors reporting it as such. This raises significant concern about its legitimacy. Additionally, the community score is highly indicative of its malicious nature, with a -216 score, further supporting the analysis. According to the malware detection results in the security vendors' analysis section, this file has been identified as a known threat. Specifically, it matches the characteristics of Flagpro malware, which is frequently associated with the advanced threat actor BlackTech. Given these findings, it is strongly advised not to open this file.