Scenario 2:

Date: July 26 2024.	**Entry:** # 1
Description	During the Detection and Analysis phase, I investigated a suspicious SHA-256 file hash flagged by the organization's intrusion detection system. The file hash, `54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`, was linked to an email attachment received by an employee. Utilizing VirusTotal, I analyzed the hash to determine the file's legitimacy and potential malicious nature. The VirusTotal report confirmed that the file was flagged as malicious by multiple cybersecurity vendors. This analysis validated the alert and provided actionable insights into the nature of the threat. My findings prompted me to escalate the incident to a Level 2 SOC Analyst for further investigation and containment.
Tool(s) used	**VirusTotal:** An online threat analysis platform that identifies known malicious files and URLs. It was used to verify the file hash and its associated risks. **Security Information and Event Management (SIEM):** The organization's SIEM system flagged the suspicious file hash and generated an alert.
The 5 W's	● **Who:** A malicious cybercriminal targeting the organization via phishing. ● **What:** A phishing email containing a malicious attachment

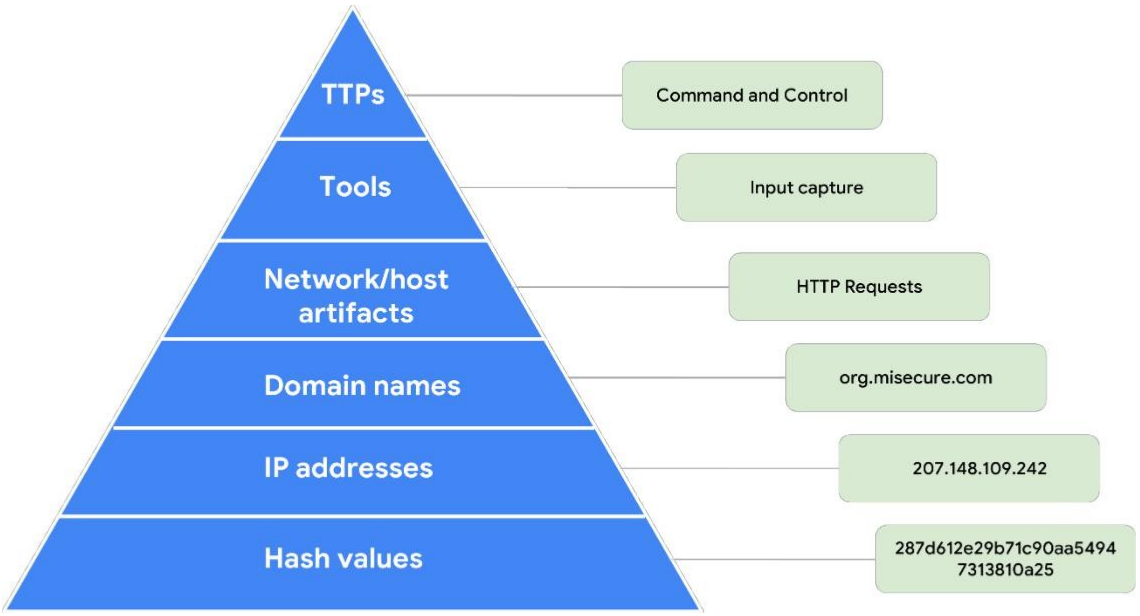
	identified by the SHA-256 hash. ● **Where**: The incident occurred on an employee’s computer at a financial services company. ● **When**: The alert was triggered at 1:20 p.m. and reported to the SOC. ● **Why**: The employee executed a malicious file attachment delivered via a phishing email, enabling the attacker to gain access to the system.
Additional notes	**Preventative Measures:** • **Employee Training:** Conduct phishing awareness training to help employees identify and avoid suspicious email attachments. • **Technical Safeguards:** Implement advanced email filtering solutions to detect and block malicious attachments before they reach employees. • **Endpoint Protection:** Deploy endpoint detection and response tools to identify and contain malicious activity on user devices. • **Incident Escalation:** Escalate similar incidents to higher-level SOC analysts for comprehensive analysis and response.

Reflections for Scenario 2	This incident highlights the critical role of phishing awareness and the importance of layered security measures. While VirusTotal provided valuable insights into the malicious nature of the file, the root cause remains a lack of employee awareness and inadequate email filtering solutions. Key takeaways include:

	• The need to proactively train employees to identify phishing attempts and report suspicious emails. • Enhancing technical controls to reduce reliance on user awareness alone. • Establishing a robust incident response playbook that outlines escalation paths and containment measures for similar incidents.

Follow-Up Actions	1. **Escalation**: Ensure the incident is thoroughly reviewed by a Level 2 SOC Analyst to assess the broader impact and potential compromise. **2. Threat Hunting:** Conduct a thorough threat-hunting exercise across the network to identify any additional indicators of compromise related to this incident. 3. **Post-Incident Review:** Hold a review meeting to document lessons learned and update the organization’s incident response playbook accordingly. **4. Policy Updates**: Implement stricter policies for email attachment handling, such as disallowing executable files unless explicitly approved.

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.