Scenario

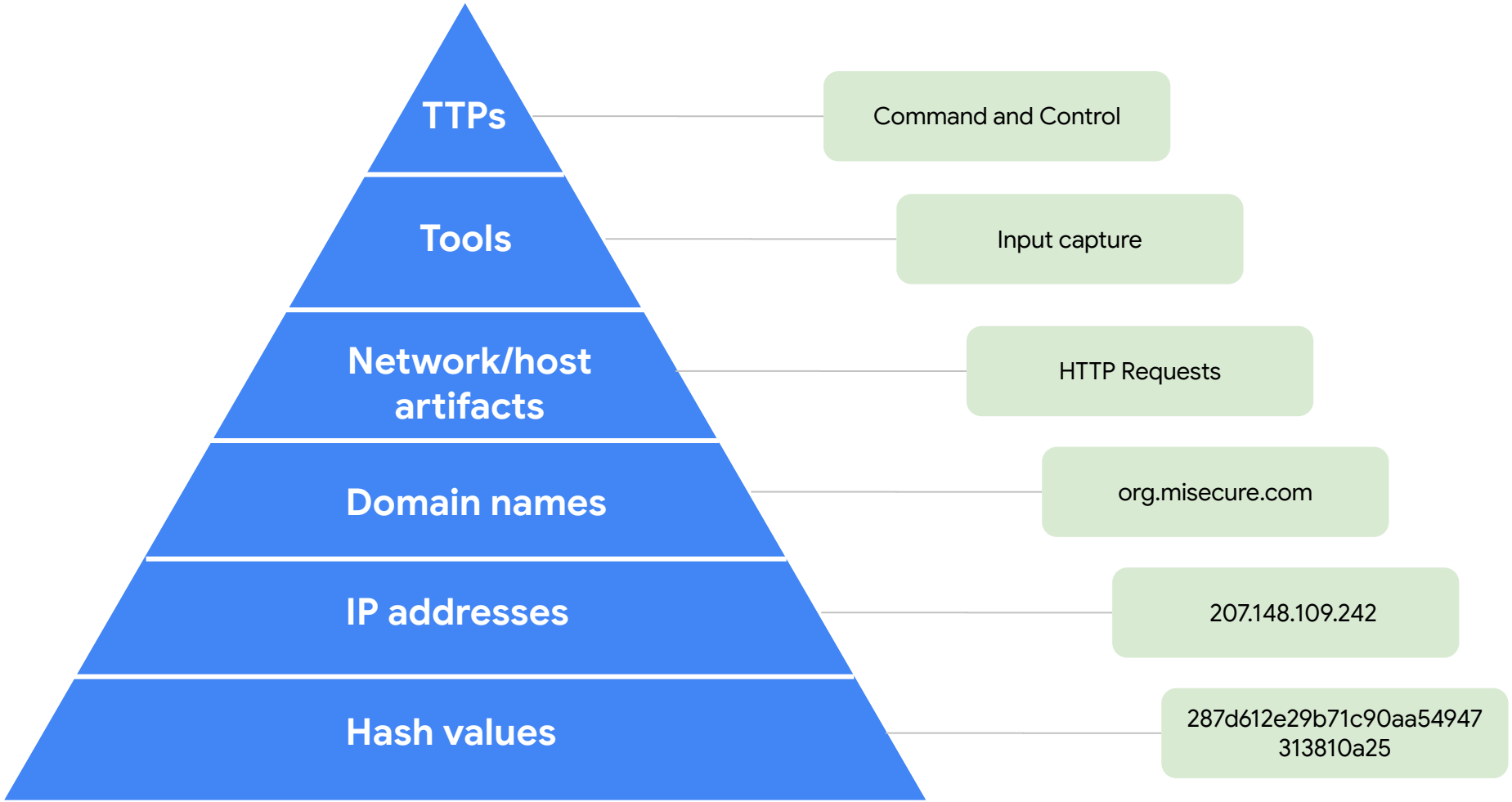
You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.

You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. 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.

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

The file hash has been flagged as malicious by more than 50 vendors. Further investigation reveals that this hash corresponds to the Flagpro malware, which is commonly associated with the advanced threat group BlackTech.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Command and Control
Input capture
HTTP Requests
org.misecure.com
207.148.109.242
287d612e29b71c90aa54947313810a25