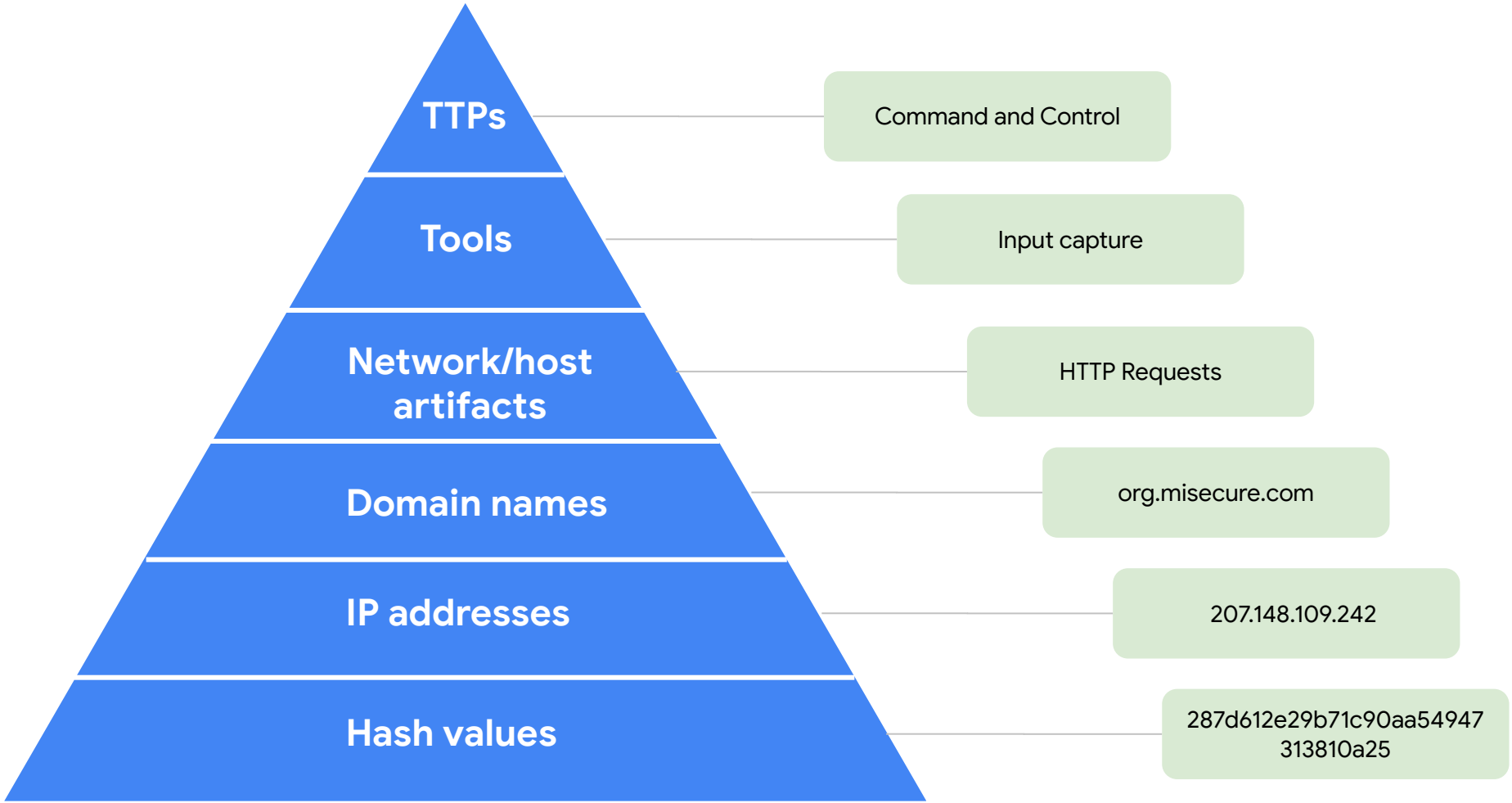
We received an alert about a suspicious file being downloaded on an employee's computer.

I retrieved the malicious file and create a SHA256 hash of the file. And uses VirusTotal to uncover additional IoCs that are associated with the file.

The file hash has been reported as malicious by over 50 vendors. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor 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