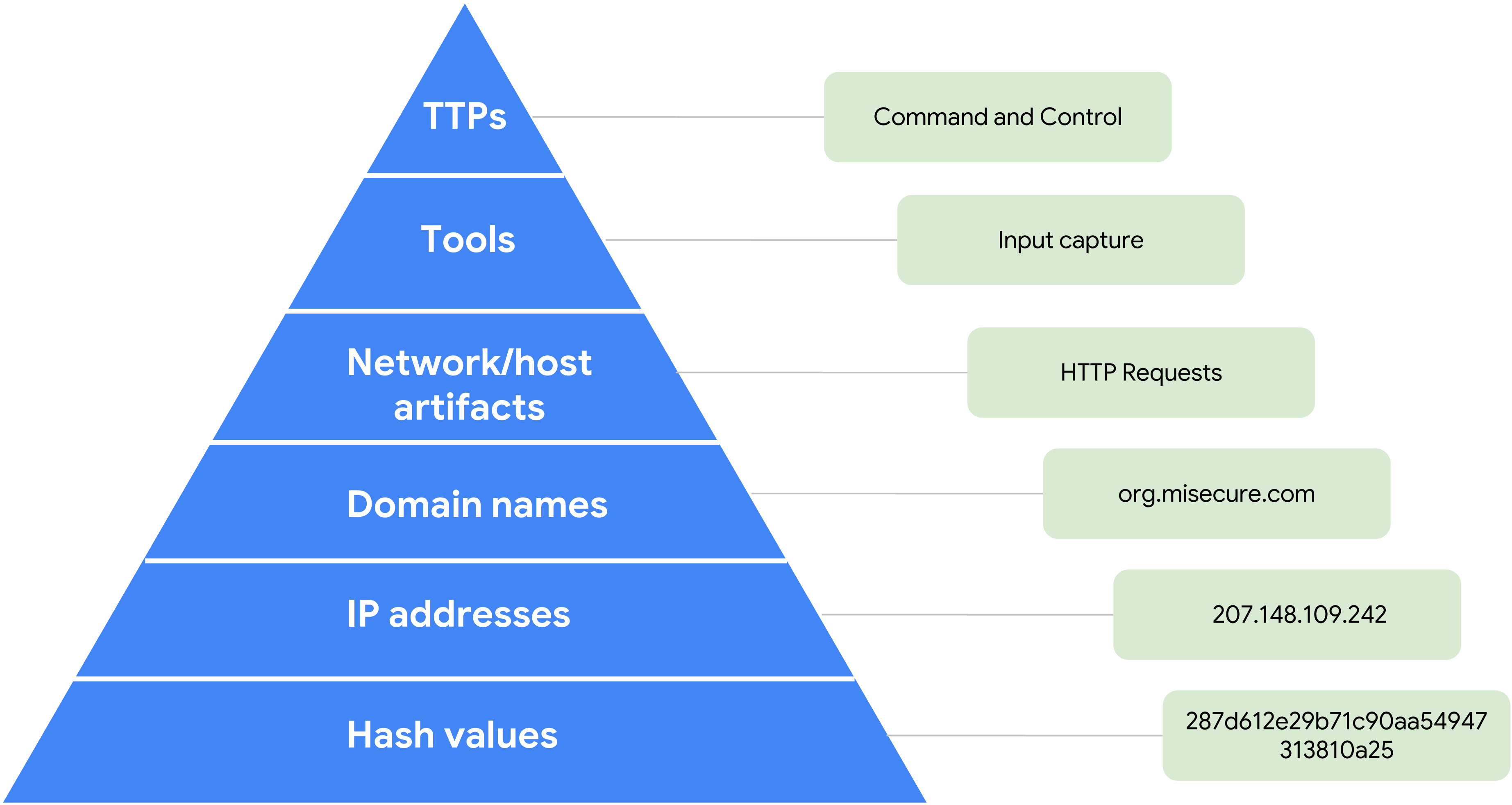
Investigation of suspicious hash file

Problem Statement

You have been tasked with investigating a security alert related to a suspicious file hash. Your objective is to conduct a thorough investigation to determine if the hash is malicious and, based on your findings, produce a report outlining the details of the threat, including the associated malware, threat actor, and any identified Tactics, Techniques, and Procedures (TTPs).

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

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

Command and Control

Tools

Input capture

Network/host artifacts

HTTP Requests

Domain names

org.misecure.com

IP addresses

207.148.109.242

Hash values

287d612e29b71c90aa54947
313810a25