# Background Info

The following information contains details about the alert that will help you complete this activity. The details include a file hash and a timeline of the event. Keep these details for reference as you proceed to the next steps.

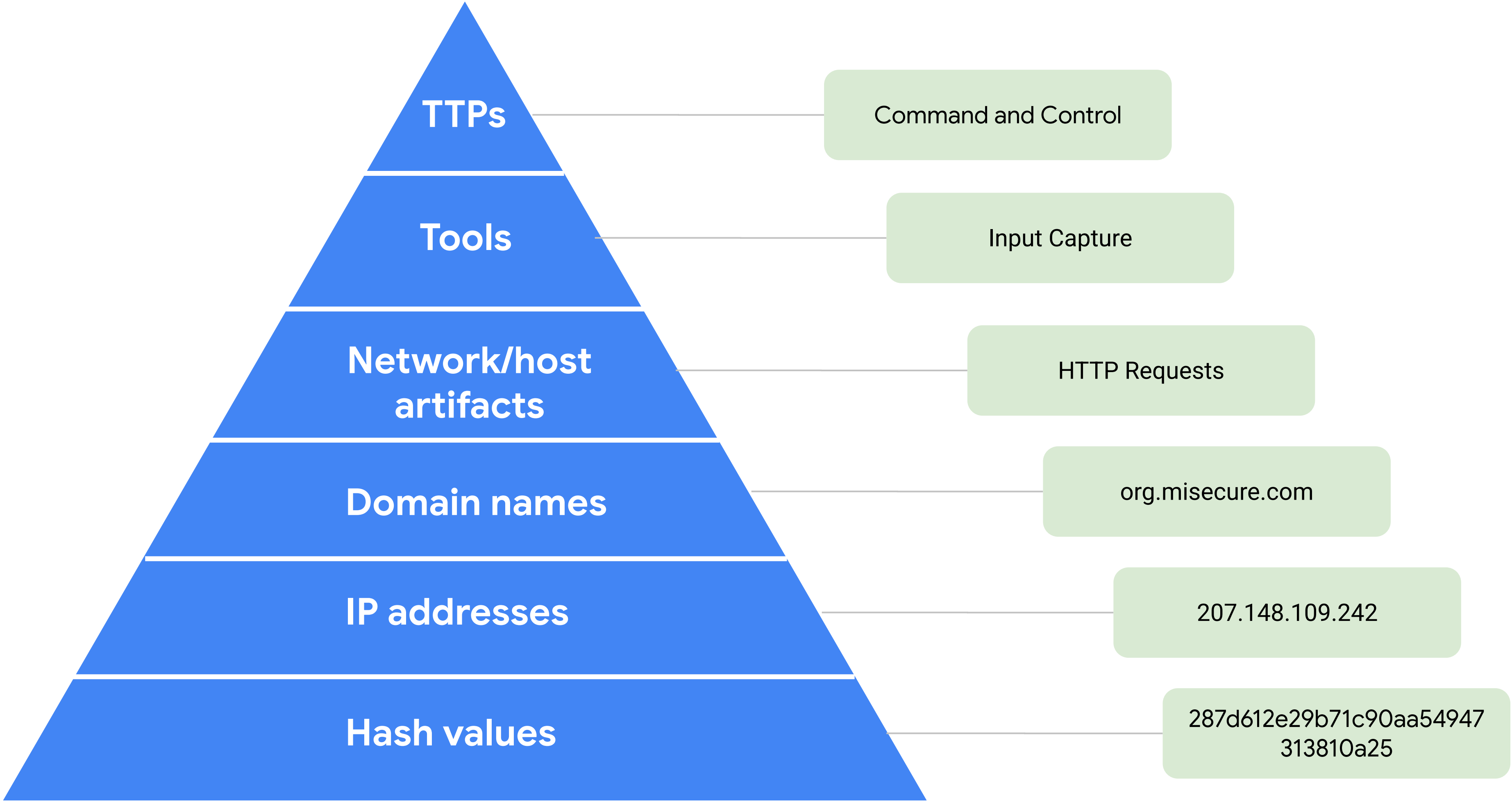
**SHA256 file hash:** 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Here is a timeline of the events leading up to this alert:

- **1:11 p.m.:** An employee receives an email containing a file attachment.
- **1:13 p.m.:** The employee successfully downloads and opens the file.
- **1:15 p.m.:** Multiple unauthorized executable files are created on the employee's computer.
- **1:20 p.m.:** An intrusion detection system detects the executable files and sends out an alert to the SOC.

## Has this file been identified as malicious? Explain why or why not.

The file has been reported by at least 50 different vendors. The file hash is known as “Flagpro,” which is a commonly used malware by the 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