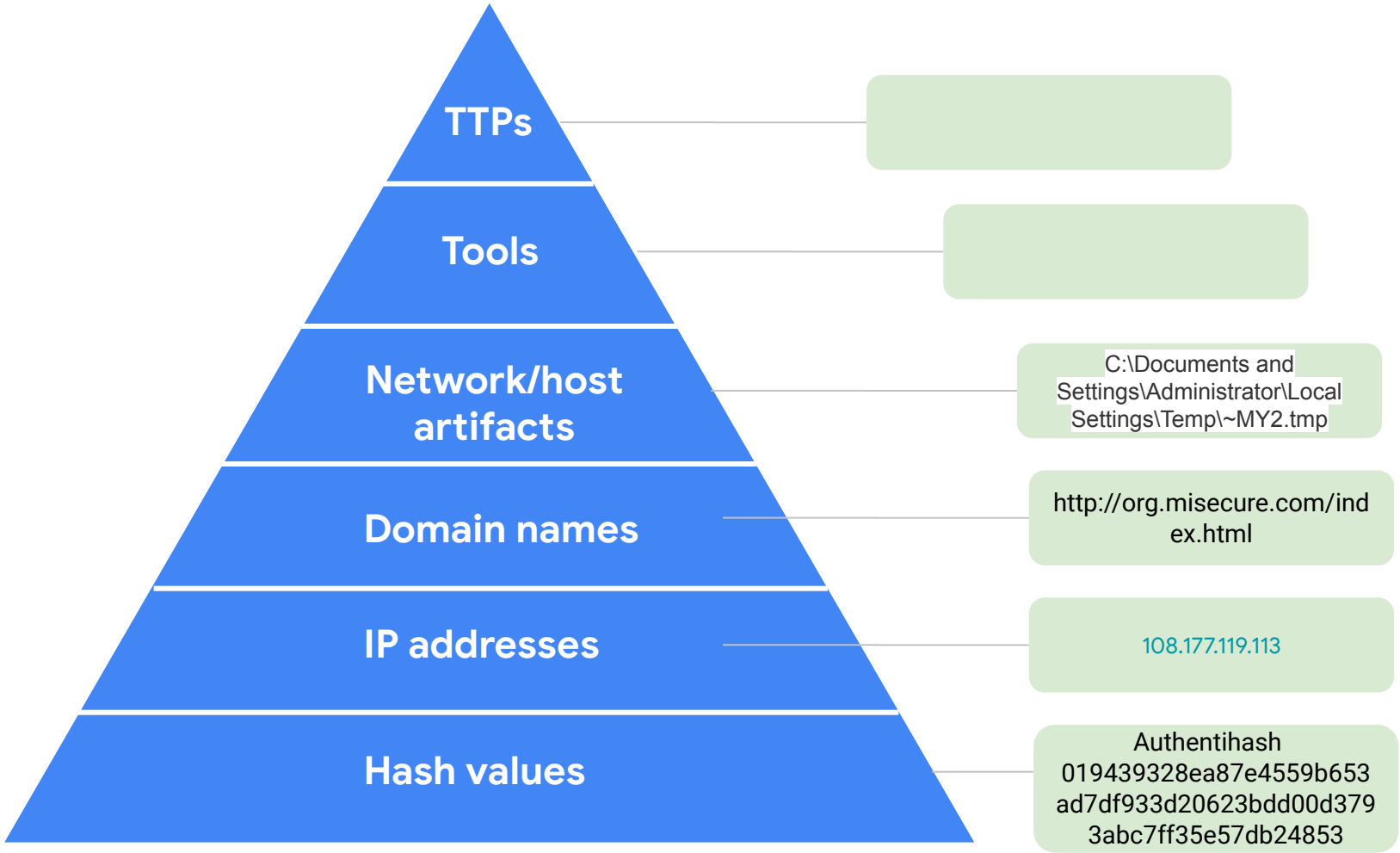
SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

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.

Yes. It seems that this file is malicious. Most of the file scanners reported that this file is indeed harmful. Community score was also quite severe and 55 out of 71 scanners reported this file as malicious.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
C:\Documents and Settings\Administrator\Local Settings\Temp\~MY2.tmp
http://org.misecure.com/index.html
108.177.119.113
Authentihash 019439328ea87e4559b653ad7df933d20623bdd00d3793abc7ff35e57db24853