# SOC Analyst Level 1

## The Pyramid of Pain

Prepared by: Abdullah Akram

# ■ Introduction

The Pyramid of Pain, introduced by David Bianco, is a strategic model in cybersecurity that demonstrates the impact of different types of indicators of compromise (IOCs) on adversaries. It highlights how defenders can increase the difficulty for attackers by focusing on higher levels of the pyramid.

## ■ Hash Values

Definition: Unique digital fingerprints of files (e.g., MD5, SHA1).
Example: Malware file hash identified by antivirus.
Impact: Very low. Attackers can easily change file content to generate new hashes.

## ■ IP Addresses

Definition: Numerical addresses used for communication.
Example: Malicious IP used for command-and-control (C2).
Impact: Low to medium. Attackers rotate IPs quickly using proxies or botnets.

## ■■ Domain Names

Definition: Human-readable names mapped to IP addresses.
Example: phishing-login[.]com.
Impact: Medium. Requires time and money to register and configure new domains.

## ■■ Network/Host Artifacts

Definition: Indicators within systems, like file paths, registry keys, or log entries.
Example: Malware creating persistence in Windows registry.
Impact: High. Attackers must re-engineer malware or infrastructure.

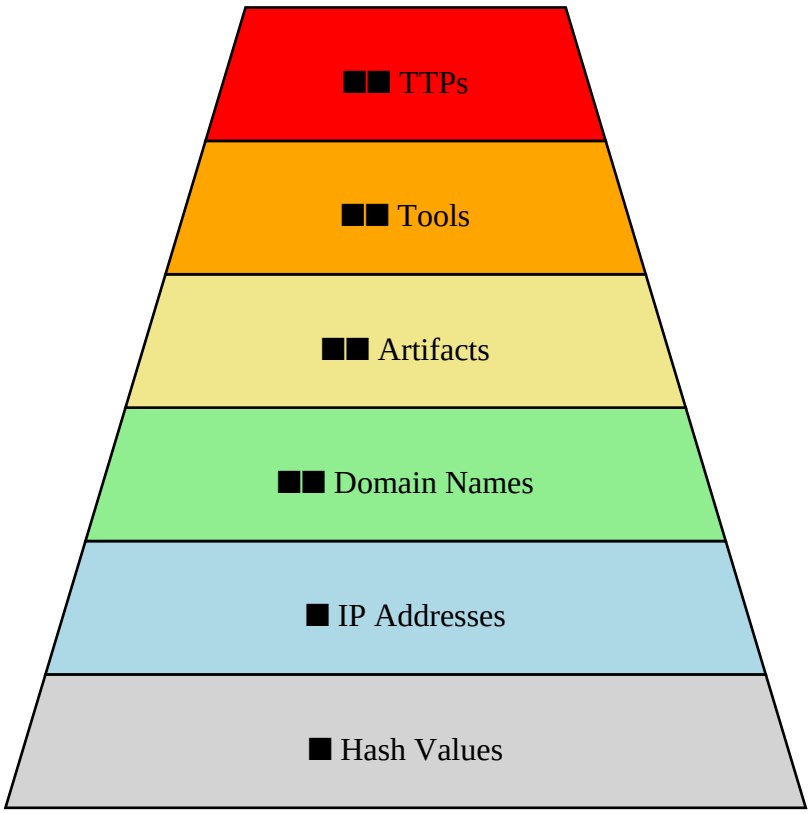
## ■■ Tools

Definition: Software and frameworks used by attackers.
Example: Mimikatz for credential dumping.
Impact: Very high. Losing tools forces attackers to find or build alternatives.

## ■■ TTPs (Tactics, Techniques, and Procedures)

Definition: Overall strategies and methods attackers use.
Example: Use of spear phishing + privilege escalation chain.
Impact: Maximum. Adversaries must completely rethink their approach when TTPs are countered.

# ■ Pyramid of Pain Diagram


■■ TTPs
■■ Tools
■■ Artifacts
■■ Domain Names
■ IP Addresses
■ Hash Values

## ■ Why It’s Important for SOC Analysts

The Pyramid of Pain serves as a guide for SOC analysts in their daily operations. By prioritizing detection and blocking of higher-level indicators, analysts can effectively increase the operational cost for attackers. This not only reduces the success rate of attacks but also buys defenders more time to prepare countermeasures.

## ■ Key Takeaways

| |
|---|
| • Hash values are weak indicators; attackers can change them easily. |
| • Blocking domains and IPs causes moderate pain but attackers adapt fast. |
| • Targeting artifacts, tools, and TTPs has the greatest defensive impact. |
| • SOC analysts should focus on higher layers to maximize adversary disruption. |

## ■ Conclusion

The Pyramid of Pain emphasizes the importance of targeting adversaries at higher levels to inflict maximum disruption. By focusing on TTPs and tools rather than simple indicators, SOC analysts can significantly hinder adversaries' ability to operate, ultimately making defense stronger and attacks less successful.