WHITEPAPER

The pyramid of pain – Insider risk & NetClean ProActive

www.netclean.com

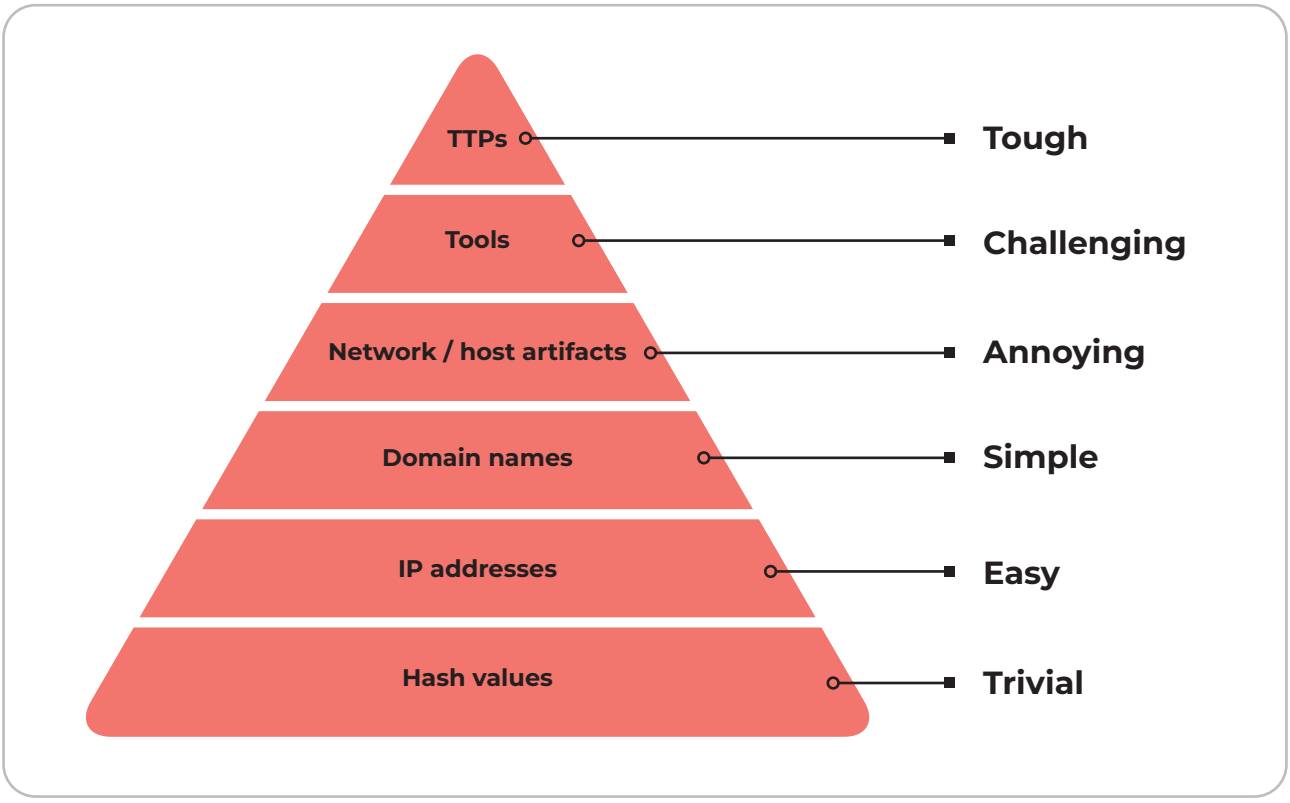
NetClean.

The Pyramid of pain – Insider risk & NetClean ProActive.

The Pyramid of Pain is a cybersecurity concept that illustrates the increasing difficulty attackers face when defenders disrupt different types of indicators in an attack. It categorizes these indicators from easiest to hardest to change, starting with hash values (easy) and moving up to TTPs (Tactics, Techniques, and Procedures) (hardest).

The Pyramid of Pain is highly applicable to insider risk because it helps security teams understand how difficult it is to detect and disrupt malicious insiders based on different types of forensic indicators. **While the framework is traditionally used in external threat intelligence, its principles can be applied to insider threat detection and response by mapping insider behaviors to the pyramid's layers**.

Each layer of the pyramid represents a different type of forensic indicator that security teams can use to detect malicious, negligent, or compromised insiders. The higher up the pyramid an organization can operate, the more effective it will be in disrupting insider threats.



How NetClean ProActive fits In

NetClean ProActive operates at the hash level—the base of the pyramid—by detecting known CSAM (Child Sexual Abuse Material) hashes on corporate endpoints. While hash-based detection is traditionally considered easy for attackers to evade (since they can slightly alter files to change hashes), CSAM hashes operate differently from conventional malware hashes because:

- Legality & Investigative Value – CSAM hashes represent illegal material rather than generic malware, making them high-risk indicators that organizations must act on immediately when detected.
- High-Confidence Indicators – Unlike malware, where hash detection alone is sometimes insufficient, CSAM hashes are definitive evidence of contraband, providing zero false positives when properly sourced.
- Behavioral & Insider Threat Insights – NetClean ProActive goes beyond hash detection by making it possible to correlating user activity and providing intelligence on potential insider threats, tying into higher levels of the pyramid (Tools and TTPs).

Aligning with higher pyramid layers

While NetClean ProActive primarily operates at the hash level, its real strength comes when combined with broader security measures, including:

- Integration with Threat Intelligence & Insider Risk Platforms – Moving from Indicators of Compromise (IOCs) to Indicators of Behavior (IOBs).
- In a platform agnostic way aiding in contextualizing detections to identify behavioral patterns – Helping organizations trace back activity to tools, accounts, and actions taken by users.
- Triggering deeper investigations and enforcement actions – Leading to policy changes and strengthening organizational security postures.