# The Subtractive Top 10 (Draft Standard)

This list prioritizes high-impact, low-friction endpoint and network subtractions:

• S01: Process Tree Integrity: Preventing browsers and office productivity suites from launching system shells ( cmd , powershell ).

• S02: Protocol Extinction: The systematic removal of legacy discovery protocols (NTLM, LLMNR, NetBIOS).

• S03: Execution Locality: Blocking unsigned binary execution from user-writable directories (%AppData% , %Temp% ).

• S04: Lateral Path Erasure: Disabling peer-to-peer administrative protocols (RDP, SMB) between non-server endpoints.

• S05: Credential Guardrails: Enforcing LSA protection and disabling legacy credential caching (WDigest).

• S06: Scripting Host Lockdown: Disabling environment-wide access to wscript.exe and cscript.exe for non-administrative users.

• S07: Surface Area Pruning: Decommissioning non-essential OS features (XPS, SMBv1, Fax, Printing services, etc) by default.

• S08: Identity Path Silencing: Restricting the use of local "Administrator" accounts and removing them from network-accessible groups.

• S09: Shell Contextualization: Enforcing Constrained Language Mode for PowerShell to prevent "Living off the Land" (LotL) techniques.

• S10: Egress Determinism: Transitioning from "Allow-All" outbound traffic to authenticated, proxy-only egress for endpoints.

## Strategic Objective: Non-Conductivity

The goal of these subtractions is to establish **deterministic boundaries** within a network. By collapsing these specific attack paths, an environment becomes architecturally **non-conductive**. In this model, vulnerabilities are viewed as "sparks," while architecture defines whether those sparks can turn into a breach or go nowhere because the "oxygen" (the attack path) has been removed.

## Measuring Efficacy

The efficacy of these subtractions is measured by the **Path Erasure Rate (PER)**, a leading metric designed to capture structural risk removal and the reduction in attacker optionality.

$$PER = \left( \frac{\sum(TTPs\ Erased\ X\ Impacted\ Assets)}{\sum(Total\ TTP\ Baseline\ X\ Total\ Assets)} \right) X100$$

According to the **Law of Subtractive Risk**, structural risk (Rs) is inversely proportional to the PER score. This demonstrates that security improves most effectively by erasing attack paths rather than adding reactive tools, as one architectural change can remove thousands of exploit possibilities.