Lateral Movement Detection GPO Settings Cheat Sheet

The very basic universal GPO settings v1.1, June 2021
https://blog.compass-security.com/2020/09/101-for-lateral-movement-detection

Pass the Hash (PTH)

`Computer Configuration\Policies\Administrative Templates\`**`SCM: Pass the Hash Mitigations`**

Lsass.exe audit mode	Enabled
LSA Protection	Enabled

Tracking and Security

`Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\`**`Security Options`**

Audit: Force audit policy subcategory settings to override audit policy category settings	Enable

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\`**`DS Access`**

Audit Directory Service Changes	Success

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\`**`Policy Change`**

Audit Audit Policy Change	Success
Audit MPSSVC Rule-Level Policy Change	Success

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\`**`System`**

Audit Security System Extension	Success
Audit System Integrity	Success & Failure

Accounts, Users and Groups

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Account Logon`

Audit Kerberos Authentication Service	Success & Failure
Audit Kerberos Service Ticket Operations	Success & Failure

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\`**`Account Management`**

Audit Computer Account Management	Success
Audit Other Account Management Events	Success
Audit Security Group Management	Success
Audit User Account Management	Success & Failure

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\`**`Logon / Logoff`**

Audit Account Lockout	Failure
Audit Group Membership	Success
Audit Logoff	Success
Audit Logon	Success & Failure
Audit Other Logon/ Logoff Events	Success & Failure
Audit Special Logon	Success

Permissions, Privileges and Access

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\`**`Object Access`**

Audit File Share	Success & Failure
Audit File System	Success & Failure
Audit Handle Manipulation	Success
Audit Kernel Object	Success & Failure
Audit Other Object Access Events	Success & Failure
Audit Registry	Success & Failure
Audit SAM	Success & Failure

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\`**`Privilege Use`**

Audit Non Sensitive Privilege Use	Success
Audit Sensitive Privilege Use	Success

Processes

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\`**`Detailed Tracking`**

Audit Process Creation	Success

`Computer Configuration\Policies\Administrative Templates\System\`**`Audit Process Creation`**

Include command line in process creation events	Enabled

`Computer Configuration\Policies\AdministrativeTemplates\WindowsComponents\`**`WindowsPowerShell`**

Turn on Module Logging	Enabled Add wildcard in Module names: *
Turn on PowerShell script Block Logging	Enabled

BEWARE that "Audit File System" and "Audit Handle Manipulation" are pretty noisy. The daily volume can easily top 100MB. Thus, configure adequate log sizes and mind log rotation to assure you have what you need when it matters!

Digital Forensics and Incident Response
24/7 Emergency Hotline +41 44 505 1337

COMPASS SECURITY