

Active Directory Security

K-12 hardening playbook

Jim Tyler, Director of Technology, Niles Community Schools · MAEDS 2026

A plain-language guide to locking down a K-12 Active Directory domain: admin accounts that cannot be stolen, servers that cannot be reached from a classroom PC, Group Policy that cannot be abused, and backups that actually run, with separate rules for domain controllers, servers and workstations.

Every item answers four questions: **What to set**, **Why it matters**, **Where it lives** (Group Policy path, PowerShell, or console), and **Who catches it** if you skip it. Rows are meant to be scanned during a presentation or used as a working checklist. The "Who catches it" tag is the point of this handout: a large share of the rows that matter most are tagged MANUAL, because no scanner reads them.

CONTENTS

- | | |
|--|---|
| 1. Scanner legend | 10. Phase 7: Directory hygiene |
| 2. Before you start | 11. Phase 8: Cloud sync boundaries (Entra Connect, Google sync) |
| 3. Phase 0: Inventory (what to read before changing anything) | 12. Phase 9: Detection |
| 4. Phase 1: Privileged accounts and tiering | 13. Phase 9a: Seams the review surfaced |
| 5. Phase 2: Authentication protocols | 14. Phase 10: Keep it that way |
| 6. Phase 3: Group Policy and SYSVOL | 15. Recipes |
| 7. Phase 4: Tier 0 servers, hypervisors and backups | 16. Gotchas: what breaks when you turn things on |
| 8. Phase 5: Workstations | 17. Rollout order |
| 9. Phase 6: Service accounts, scheduled tasks and applications | 18. DCs vs. servers vs. workstations at a glance |

Scanner legend

TAG	MEANING
PINGCASTLE	PingCastle (free, single EXE, five-minute run) reports it. Rule names are given where stable; they drift between versions. Purple Knight covers most of the same ground.
GUERRILLA	Guerrilla (free, CC BY 4.0, written by the author of this handout, PowerShell 7 module, agentless and read-only) reports it. Check IDs are given (ADPRIV-028, ADSCRIPT-004 and so on); 211 AD checks across privileged accounts, ACLs, Kerberos, AD CS, GPO contents, logon scripts, NTLM-relay preconditions, Tier 0 hygiene and logging, plus Entra ID and Google Workspace modules. Every verdict is PASS, FAIL, WARN or an explicit Not Assessed.
BLOODHOUND	BloodHound / SharpHound (or an equivalent Get-Acl sweep) shows it as an edge in the attack graph: ACLs, group nesting, sessions, delegation, and in the CE edition AD CS.
ADELEG	ADEleg (free, single EXE, GUI or CSV) lists every delegation in the directory that is not a Windows default, per container, and names the trustee and the right. Built for the "who was ever given what, and is it still needed" question; diff two exports to see what changed.
LOCKSMITH	Locksmith (free PowerShell module) audits Active Directory Certificate Services for the ESC1 to ESC8 (and newer) template and CA misconfigurations and in Mode 4 offers to fix each issue after warning about its impact. Only relevant if a CA exists.
SCRIPTSENTRY	ScriptSentry (free PowerShell script, Invoke-ScriptSentry.ps1) reads every logon script, GPO script and NETLOGON file and reports hard-coded credentials, unsafe permissions on scripts, NETLOGON/SYSVOL and referenced shares, non-existent shares, and admins with logon scripts. GPP passwords are a PingCastle finding.
MANUAL	No scanner reads it. It lives inside a GPO's user-rights section, on a member server's file system, in Task Scheduler, in a service's logon account, in a sync tool's config, in patch state, or outside AD entirely. You have to go look.
BUILT-IN	A Windows default or a Defender/Security Baseline item; your job is to confirm nobody turned it off.
PAID	Needs a licensed product (Defender for Identity, Entra ID P1/P2, a SIEM). Listed so nobody budgets for it by accident. Everything else in this handout, every scanner above included, is free.

Quick rule: the scanners see AD objects, ACLs, GPO *existence and permissions*, SYSVOL scripts, and (Guerrilla) a good share of GPO *contents* and relay preconditions. None of them sees user-rights assignments as they land on a DC, which servers inherit which GPOs because of where they sit, stored task passwords, service logon accounts, NTFS ACLs on script folders on member servers, missing updates, or anything in Google. Phases 4, 6 and 8 are mostly MANUAL; run every scanner anyway, because the rows they do cover are the ones that are easiest to miss by hand.

What each scanner reads

TOOL	RUN IT WITH	READS	DOES NOT READ
PingCastle	<code>PingCastle.exe --healthcheck</code> from any domain-joined PC	AD objects, group membership, password ages, trusts, DC settings reachable over LDAP/SMB, GPO passwords and permissions, SYSVOL script ACLs	GPO contents beyond a fixed list, member-server configuration, tasks, services, patch state
Guerrilla	<code>Install-Module Guerrilla</code> ; AD assessment from a domain-joined PowerShell 7 session (catalog at guerrilla.army)	Everything PingCastle reads plus GPO contents (Restricted Groups, scripts, scheduled tasks, audit, firewall, PowerShell logging, LAPS, AppLocker), logon-script contents, NTLM-relay preconditions, Tier 0 service accounts in privileged groups, AD CS ESC1 to ESC16, Entra sync account hygiene, shadow credentials, attack paths to Tier 0	Effective (RSOP) user rights, member-server local groups and tasks, patch state, folders outside SYSVOL
BloodHound	SharpHound collector, BloodHound CE for the graph	ACL edges, nesting, sessions, local admin (with the right collection), delegation, AD CS (CE)	Anything that is not an edge: settings, policies, patch state
ADeleg	<code>adeleg.exe</code> (GUI); check <code>adeleg.exe --help</code> for CSV export	Every non-default ACE on every container and object, grouped by trustee	Group membership, settings, GPO contents
Locksmith	<code>Invoke-Locksmith -Mode 1</code> (report), <code>-Mode 4</code> (fix)	Certificate templates, CA settings and ACLs, enrollment endpoints	Anything outside AD CS
ScriptSentry	dot-source the script, then <code>Invoke-ScriptSentry</code>	Logon scripts (user attribute, GPO, NETLOGON), the shares they reference, their contents	Scripts and folders on member servers that no logon references

Scoring trap: PingCastle's global score is the **highest** of its four category scores, not a sum. Fixing ten small items in one category does nothing to the score if another category still has a 50-point finding. Use the score as a lagging indicator; fix attack paths, not points.

Before you start

☐ Confirm every change can land on every DC

SET TO	<code>repadmin /replsummary</code> and <code>repadmin /showrepl</code> clean on every DC; DFSR SYSVOL healthy (<code>dfsrdiag replicationstate</code>)
WHY	Every GPO, SYSVOL and ACL change below has to reach all DCs. Half-applied security is worse than none because you will believe it is done.
WHERE	PowerShell on any DC
WHO CATCHES IT	PINGCASTLE GUERRILLA (ADDOM-007)

☐ Take a full backup first

SET TO	<code>wbadmin start systemstatebackup</code> on one DC to a share only DCs can write, plus <code>Backup-GPO -All</code> , plus an export of every admin group's membership and every GPO's links
WHY	Several items below edit the Default Domain Controllers Policy and SYSVOL permissions. The undo is a restore.
WHERE	Recipe R8
WHO CATCHES IT	PINGCASTLE (A-BackupMetadata flags a DC with no backup in 7 days)

☐ Create a break-glass Domain Admin

SET TO	One account, Domain Admins only, not in Protected Users and excluded from any Authentication Policy Silo, 30+ random characters stored offline (sealed envelope or vault), <code>LogonWorkstations</code> limited to the DCs and one admin host, an alert on any 4624/4768 for it
WHY	Phase 1 removes NTLM and cached credentials from every real admin. If Kerberos, DNS or time breaks, this is the only account that can still sign in.
WHERE	ADUC; alert in Phase 9
WHO CATCHES IT	MANUAL (a scanner will flag it as an admin not in Protected Users; that is intentional)

☐ Turn on the AD Recycle Bin

SET TO	<code>Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target <forest> ; check tombstoneLifetime and msDS-DeletedObjectLifetime (blank means it uses tombstoneLifetime); if either is 60 (forests created before 2003 SP1), set it to 180</code>
WHY	Phase 7 deletes a lot of objects. With the Recycle Bin on, <code>Restore-ADObject</code> brings any of them back with attributes and group memberships for 180 days.
WHERE	PowerShell on a DC (irreversible, but there is no reason to want it off)
WHO CATCHES IT	PINGCASTLE GUERRILLA (ADDOM-009)

☐ Pick a pilot OU

SET TO	One building or grade band for workstation changes; one non-critical member server for server changes
WHY	Every phase goes to pilot first. Several items in this handout caused district-wide prompts or lockouts when applied domain-wide in one step.
WHERE	ADUC
WHO CATCHES IT	N/A

☐ Run every free scanner once and keep the output

SET TO	PingCastle (<code>PingCastle.exe --healthcheck --server <domain></code> , archive the <code>.xml</code> next to the HTML); Guerrilla (AD assessment from PowerShell 7, keep the JSON and HTML); SharpHound collection into BloodHound CE; <code>adeleg.exe --csv baseline.csv ; Invoke-ScriptSentry ; Invoke-Locksmith -Mode 1</code> if a CA exists. All read-only; all from the admin host as a Domain Admin
WHY	Six baselines on day one. PingCastle's XML and Guerrilla's JSON hold the scores and verdicts for diffing between runs; ADeleg's CSV is the delegation inventory you diff every quarter; the BloodHound graph is where you confirm the paths the rest of this handout closes.
WHERE	Admin host. Guerrilla's AD attack-detection files may be blocked by Defender heuristics on import; add a path exclusion for the module folder from an elevated prompt (the files are inert PowerShell)
WHO CATCHES IT	N/A

Phase 0: Inventory (what to read before changing anything)

One day of reading finds the paths that matter. Do all of these before Phase 1; Recipe R1 has the commands.

☐ Effective user rights on every DC

SET TO	Dump <code>RSOP_UserPrivilegeRight</code> on each DC and on one hypervisor, one server and one workstation. Any principal other than the built-in defaults on <code>SeTakeOwnershipPrivilege</code> , <code>SeBackupPrivilege</code> , <code>SeRestorePrivilege</code> , <code>SeDebugPrivilege</code> , <code>SeTcbPrivilege</code> , <code>SeLoadDriverPrivilege</code> , <code>SeImpersonatePrivilege</code> , <code>SeRemoteShutdownPrivilege</code> , <code>SeEnableDelegationPrivilege</code> or <code>SeMachineAccountPrivilege</code> is a finding
WHY	A user right granted by an Enforced GPO at the domain root beats the Default Domain Controllers Policy and lands on DCs. A staff group holding "Take ownership" on a DC is a one-step path to Domain Admin, and no scanner computes RSOP.
WHERE	<code>Get-CimInstance -Namespace root\rsop\computer RSOP_UserPrivilegeRight</code>
WHO CATCHES IT	MANUAL (no scanner computes RSOP; Guerrilla ADGPO-017 reads Restricted Groups, not user rights)

☐ Every GPO linked at the domain root, and every Enforced link anywhere

SET TO	<code>Get-GPInheritance -Target <domain DN></code> and the same for each top-level OU; read each GPO's report (<code>Get-GPOReport -ReportType Xml</code>)
WHY	Root-linked GPOs apply to servers and DCs unless an OU blocks inheritance. Restricted Groups, user rights, scheduled tasks, Point-and-Print and update settings in a root GPO are the usual surprises.
WHERE	GroupPolicy module on a DC
WHO CATCHES IT	MANUAL for contents and Enforced flags; GUERRILLA (ADGPO-013/015/017: scripts, scheduled tasks and Restricted Groups inside GPOs)

☐ Local Administrators on every server

SET TO	<code>Get-LocalGroupMember Administrators</code> on every enabled server; record which members arrive by Restricted Groups and which are direct
WHY	Helpdesk or workstation-admin groups on a server that holds a sync credential, a backup, or ntds.dit copies is a path from any classroom PC to Tier 0.
WHERE	<code>Invoke-Command</code> to all servers (Recipe R1)
WHO CATCHES IT	BLOODHOUND (if SharpHound collected local groups) MANUAL

☐ Scheduled tasks and services with a stored domain credential, on every server

SET TO	Tasks with <code>LogonType = Password</code> and a domain <code>UserId</code> ; services whose <code>StartName</code> is a domain user
WHY	A stored password is recoverable by any local admin on that server. A task that is dead but still scheduled keeps trying the old password daily and looks like an attack in the DC logs.
WHERE	Recipe R1
WHO CATCHES IT	MANUAL (GUERRILLA ADTIER-002 to 005 flag backup, hypervisor, config-management and SQL service accounts that sit in privileged groups, not tasks)

☐ Contents of CN=Computers and CN=Users

SET TO	List every object in both default containers with OS and last logon
WHY	Objects there receive every domain-root GPO with no OU to block it, and no OU-linked policy of their own. Servers that were never moved out are the ones that quietly get the workstation GPOs.
WHERE	<code>Get-ADComputer -SearchBase "CN=Computers,<domain DN>"</code>
WHO CATCHES IT	GUERRILLA (ADTIER-006 for admin accounts outside a Tier 0 OU) MANUAL for the policy consequence

☐ SYSVOL and NETLOGON ACLs and ownership, on each DC separately

SET TO	<code>icacls \\<dc>\SYSVOL\<domain>\scripts</code> and <code>Get-Acl</code> on <code>Policies*</code> grouped by owner, run against each DC's UNC path
WHY	A write ACE for Authenticated Users on NETLOGON, or ownership of Policies by a disabled account, is a path to code execution on every machine. Folder ACLs do not always replicate between DCs, so reading one DC proves nothing about the other.
WHERE	PowerShell
WHO CATCHES IT	PINGCASTLE (P-DelegationLoginScript, P-DelegationGPOData) SCRIPTSENTRY GUERRILLA (ADSCRIPT-001/002/007, ADACL-011) MANUAL for the per-DC comparison

❑ Patch level of DCs, hypervisors and Tier 0 servers

SET TO	Build number plus UBR from <code>HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion</code> , compared to the current cumulative update; and the effective Windows Update policy on the server OUs
WHY	<code>AUOptions=3</code> (download and notify) on a server OU means updates wait for a click that never comes. Scanners do not check patch state at all.
WHERE	Recipe R1
WHO CATCHES IT	MANUAL (GUERRILLA ADDOM-005 and ADSTALE-006 catch obsolete OS versions only, not missing updates)

❑ Who can DCSync

SET TO	ACEs on the domain root for <code>DS-Replication-Get-Changes</code> and <code>-All</code> (GUIDs <code>1131f6aa-...</code> and <code>1131f6ad-...</code>). Expect Administrators, Domain Controllers, Enterprise Domain Controllers (plus Enterprise Read-only Domain Controllers on Get-Changes only), and exactly one Entra Connect sync account
WHY	Any other principal can pull every password hash. Stale <code>MSOL_*</code> accounts left by a retired or reinstalled Entra Connect server are the usual extra.
WHERE	Recipe R13
WHO CATCHES IT	BLOODHOUND (DCSync edge) PINGCASTLE ADELEG GUERRILLA (ADPRIV-028, ADACL-012)

❑ Where ntds.dit copies live

SET TO	Find every IFM, system-state, VM checkpoint and backup repository that contains a DC's disk; list who is local admin on each host. If an IFM job exists and nobody can say what it is for, that is the first copy to delete
WHY	Whoever can read the file has every hash. Backup servers and hypervisors are Tier 0 whether or not they are treated that way. Fewer copies beats better ACLs.
WHERE	Backup console, Hyper-V/vSphere, file search for <code>ntds.dit</code>
WHO CATCHES IT	MANUAL

❑ Plaintext credentials in script and export folders on automation servers

SET TO	Search every scripts, tools and automation folder for CSV/TXT/LOG files whose header contains <code>password</code> ; check the folder's NTFS ACL for inherited BUILTIN\Users read
WHY	Legacy SIS-to-AD-to-Google sync scripts commonly dump their full input, passwords included, into a log folder on every run, for years, readable by every local user.
WHERE	Recipe R11
WHO CATCHES IT	MANUAL (SCRIPTSENTRY and GUERRILLA ADSCRIPT-004/006 cover logon scripts and SYSVOL/NETLOGON, not arbitrary folders on member servers)

Gate: inventory written down, backup taken, break-glass account tested from the admin host, pilot OU chosen.

Phase 1: Privileged accounts and tiering

☐ Domain Admins = named human admin accounts only

SET TO	Remove every vendor, service, LDAP-bind, test, seasonal and "temporary" account; Enterprise Admins empty except when a forest-level change is in progress; Schema Admins empty
WHY	Every member can DCSync the krbtgt hash and forge Golden Tickets. Firewall LDAP-bind accounts, secretaries added "to fix a permission once", and accounts named after a season are the classic residents.
WHERE	ADUC, or <code>Get-ADGroupMember -Recursive</code> for the nine groups in Recipe R1
WHO CATCHES IT	PINGCASTLE (P-AdminNum, P-SchemaAdmin, P-AdminPwdTooOld) BLOODHOUND GUERRILLA (ADPRIV-001 to 003, 024, 025)

☐ Clear adminCount and re-enable inheritance after every removal

SET TO	<code>Set-ADUser <user> -Clear adminCount</code> , then <code>\$acl.SetAccessRuleProtection(\$false,\$true)</code> on the object
WHY	Removing an account from a protected group does not undo what AdminSDHolder did to it. The account keeps a protected ACL (no inheritance, no delegated helpdesk rights), and PingCastle keeps flagging it.
WHERE	Recipe R1 (last block)
WHO CATCHES IT	PINGCASTLE (A-AdminSDHolder) GUERRILLA (ADPRIV-020/021)

☐ Operators and other legacy groups empty

SET TO	Account Operators, Server Operators, Backup Operators, Print Operators, DnsAdmins, Group Policy Creator Owners, Cert Publishers, Key Admins: all empty, or Domain Admins only where something truly needs it
WHY	Each one is a documented path to Domain Admin (Backup Operators can read ntds.dit; DnsAdmins can load a DLL on the DC; Group Policy Creator Owners can author a GPO that any later link turns into code execution).
WHERE	ADUC
WHO CATCHES IT	PINGCASTLE BLOODHOUND GUERRILLA (ADPRIV-004 to 008, ADTRADE-008/009)

☐ Separate admin accounts per person

SET TO	<code><user>-adm</code> holds every admin group membership; the everyday <code><user></code> account is a plain user with mail and M365 only. The <code>-adm</code> account never signs in interactively to a workstation
WHY	The everyday account is the one typed on staff PCs, phished, and used in the browser. Whatever it can reach is what an attacker gets with one stolen session or one keylogger. This applies to the helpdesk technician first: their daily account is usually local admin on half the servers.
WHERE	ADUC; Phase 1 deny-logon GPO enforces the "never on a workstation" half
WHO CATCHES IT	BLOODHOUND (shows the everyday account's sessions on workstations) MANUAL

☐ Built-in Administrator (RID 500) as sealed break-glass only

SET TO	Remove it from every group it was added to over the years (teacher, office, department groups) but leave its default built-in memberships alone; Account is sensitive and cannot be delegated; 30+ character password rotated and stored offline; never used interactively; in a GPO on the DC OU and another on the server and workstation OUs (never the domain root), add <code><DOMAIN>\Administrator</code> to Deny access to this computer from the network, Deny log on as a batch job, Deny log on as a service and Deny log on through Remote Desktop Services
WHY	The built-in Administrator cannot be locked out and is the account every attacker tries first. A domain-wide group membership on it means any share or GPO scoped to that group includes a never-expiring Domain Admin.
WHERE	ADUC; DDCP user rights
WHO CATCHES IT	PINGCASTLE (S-PwdNeverExpires, P-AdminLogin) GUERRILLA (ADPRIV-010, 017) MANUAL for the group memberships

☐ No "password never expires" on any human admin

SET TO	Unchecked on every Domain/Enterprise Admin; password age under one year
WHY	A years-old password on a Domain Admin is the one in every old backup, old export and old breach dump.
WHERE	ADUC
WHO CATCHES IT	PINGCASTLE (S-PwdNeverExpires, P-AdminPwdTooOld) GUERRILLA (ADPRIV-010, ADPRIV-017)

❑ Every human admin in Protected Users

SET TO	Domain Admins, Enterprise Admins, Schema Admins and every <code>-adm</code> account: member of Protected Users. Not the break-glass account, not service accounts. Roll out one account at a time, a day apart (Recipe R3)
WHY	Members cannot use NTLM, DES or RC4, cannot be delegated, get no cached credentials, and hold a 4-hour non-renewable TGT. Pass-the-hash and NTLM relay against those accounts stop working. This is the single highest-value control in the handout and also the one with the longest gotcha list; read Recipe R3 and the Gotchas section first.
WHERE	ADUC > Users > Protected Users
WHO CATCHES IT	PINGCASTLE (P-ProtectedUsers) GUERRILLA (ADPRIV-029/030)

Watch out: RDP, SMB and WMI **by IP address** stop working for these accounts (no SPN, so NTLM fallback, which is now refused). Connect by FQDN. See the Gotchas section.

❑ Deny admin logon to workstations

SET TO	A GPO linked only at the workstation OU: Deny log on locally, Deny log on through Remote Desktop Services, Deny log on as a batch job, Deny log on as a service = Domain Admins, Enterprise Admins (and the <code>-adm</code> accounts' group). Network logon is not denied (Recipe R4)
WHY	Guarantees a Tier 0 credential is never typed on a classroom PC, which is where keyloggers and LSASS dumps happen. Leaving network logon alone keeps remote management (WMI, WinRM, SMB) working from the admin host.
WHERE	Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment
WHO CATCHES IT	PINGCASTLE (P-LogonDenied) GUERRILLA (ADPRIV-026/027 cover the DC side)

Watch out: Never link it to a server or DC OU. Tell the admins first; the first one to RDP to a staff PC afterwards will think the domain is broken.

❑ Local Administrators on Tier 0 = Domain Admins only

SET TO	DCs (implicit), hypervisors, the backup server, the Entra Connect server, any server holding ntds.dit copies, the print server if drivers come from it: local Administrators = Domain Admins plus the one service account that must be there. No helpdesk group, no "WorkstationAdmins", no legacy automation account
WHY	A local admin on any of these can read every hash, decrypt the sync credential, or push a driver to every PC. This is where the "helpdesk → Entra Connect → DCSync" path is cut.
WHERE	Restricted Groups in a Tier 0 GPO, or by hand; verify with <code>Get-LocalGroupMember</code>
WHO CATCHES IT	BLOODHOUND (AdminTo edges, if collected) GUERRILLA (ADTIER-002/003 for backup and hypervisor accounts in privileged groups) MANUAL

❑ Helpdesk rights delegated, not granted

SET TO	Four scoped groups with explicit AD ACEs: password reset (ResetPassword + write pwdLastSet/lockoutTime on user objects under the staff OU), user creation (CreateChild user + GenericAll on descendant users in the staff OU), computer management (CreateChild/DeleteChild computer + GenericAll on descendant computers in the workstation OU), group membership (write <code>member</code> on the operational groups' containers). Explicit Deny of all four on the IT/service-account OU and on infrastructure groups (Recipe R12)
WHY	Helpdesk does its job without Account Operators, Domain Admins, or local admin on servers. The deny on the IT OU stops a helpdesk account resetting an admin's password.
WHERE	ADUC > Delegate Control, or <code>Set-Acl</code> on an <code>AD:</code> drive
WHO CATCHES IT	BLOODHOUND ADELEG (shows every non-default delegation per container; confirm each one is intended) GUERRILLA (ADACL-008)

Watch out: A technician whose RDP session predates the group will report "still can't reset passwords". The token is stale. Full sign-out, not disconnect/reconnect.

❑ Admin work only from an admin host

SET TO	Domain Admin credentials are used from DCs, a dedicated admin host or PAW, and nowhere else. Never from a personal laptop, never from a non-domain device, never over RDP from a workstation
WHY	Every host an admin password touches is a place it can be dumped. DC 4768 events show exactly which hosts those are (Recipe R13).
WHERE	Policy, enforced by the deny-logon GPO and (later) an Authentication Policy Silo
WHO CATCHES IT	BLOODHOUND (HasSession) GUERRILLA (ADPRIV-026/027) MANUAL (4768 source review)

❑ Authentication Policy Silo for Domain Admins (advanced, do last)

SET TO	One Authentication Policy: <code>UserAllowedToAuthenticateFrom</code> = DCs plus the admin host, <code>UserTGTLifetimeMins</code> = 240; one Silo containing the admin accounts and those computers. Create with <code>-Enforce:\$false</code> (audit mode) and read <code>Microsoft-Windows-Authentication/AuthenticationPolicyFailures-DomainController</code> for 2 to 4 weeks before enforcing
WHY	Protected Users stops NTLM; a Silo stops the Kerberos ticket itself from being issued anywhere but the admin host. Requires 2012 R2 domain functional level, Kerberos armoring on the DCs (Phase 2), and Kerberos client support for claims, compound authentication and Kerberos armoring = Enabled on the admin host.
WHERE	Active Directory Administrative Center > Authentication
WHO CATCHES IT	MANUAL

Watch out: The break-glass account must be **outside** the Silo and tested before enforcement. An enforced Silo with a wrong computer list locks every admin out at once.

❑ Rotate krbtgt twice

SET TO	Reset the krbtgt password, wait longer than the maximum TGT lifetime (10 hours default) plus replication, reset again; repeat annually
WHY	Any Golden Ticket forged from an old krbtgt hash stops working after the second reset. One reset is not enough: the DC accepts tickets signed with the previous password.
WHERE	Microsoft's <code>New-KrbtgtKeys.ps1</code> , or ADUC on the PDC emulator
WHO CATCHES IT	PINGCASTLE (A-Krbtgt) GUERRILLA (ADPRIV-022/023)

❑ No shadow credentials or stray key material on privileged principals

SET TO	<code>msDS-KeyCredentialLink</code> empty on every admin account, DC and Tier 0 computer object unless Windows Hello for Business or a certificate-based logon is deliberately in use; Key Admins and Enterprise Key Admins empty
WHY	A write to that attribute lets an attacker authenticate as the object with a certificate they generated, without knowing or changing its password. It survives password resets.
WHERE	<code>Get-ADObject -Filter {msDS-KeyCredentialLink -like '*'} -Properties msDS-KeyCredentialLink</code> ; ADUC for the two groups
WHO CATCHES IT	GUERRILLA (ADTRADE-006, ADTRADE-008) BLOODHOUND (AddKeyCredentialLink edge)

Gate: admin group membership matches the written list; every removed account has `adminCount` cleared; break-glass signs in from the admin host; deny-logon GPO verified present on a workstation and absent on a DC.

Phase 2: Authentication protocols

☐ NTLMv2 only, LM hash never stored

SET TO	Network security: LAN Manager authentication level = Send NTLMv2 response only. Refuse LM & NTLM (<code>LmCompatibilityLevel=5</code>) in the Default Domain Controllers Policy first, then the domain; Do not store LAN Manager hash value on next password change = Enabled
WHY	NTLMv1 and LM responses are crackable offline in minutes from a single captured handshake.
WHERE	Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options
WHO CATCHES IT	PINGCASTLE (S-OldNtlm, A-LMHashAuthorized) GUERRILLA (ADDOM-016/017)

Watch out: Audit 4624 events whose `LmPackageName` is `NTLM V1` for two weeks first. Multifunction copiers doing scan-to-folder and old NAS units are the usual NTLMv1 holdouts. Do not test with a Protected Users account; it fails regardless.

☐ NTLM minimum session security

SET TO	Minimum session security for NTLM SSP based clients and ... servers = Require NTLMv2 session security + Require 128-bit encryption (<code>0x20080000</code>)
WHY	Without it, an NTLMv2 session can still negotiate down to weak session keys that relay tools exploit.
WHERE	Same Security Options node
WHO CATCHES IT	MANUAL

❑ NTLM auditing, then restriction

SET TO	Restrict NTLM: Audit NTLM authentication in this domain = Enable all, and Audit Incoming NTLM Traffic = Enable auditing for all accounts, for 30 days; read Microsoft-Windows-NTLM/Operational (events 8001-8004) on the DCs; then Restrict NTLM: NTLM authentication in this domain = Deny for domain accounts to domain servers, with exceptions listed by server name
WHY	Protected Users only covers the admins. Restricting NTLM domain-wide closes relay for everyone, but only after you know which copier, NAS, legacy app and by-IP management tool still depends on it.
WHERE	Same Security Options node; exceptions in Add server exceptions in this domain
WHO CATCHES IT	MANUAL

Watch out: Every tool that connects by IP address uses NTLM. See the Gotchas section.

❑ LDAP signing required, channel binding enforced

SET TO	Domain controller: LDAP server signing requirements = Require signing; LDAP server channel binding token requirements = When supported first (LdapEnforceChannelBinding=1), then Always (=2) after the audit is clean
WHY	Stops LDAP relay (an attacker relaying a captured machine authentication to LDAP to add a computer account or change an ACL).
WHERE	DDCP > Security Options; audit events 2889 (unsigned binds) and 3039/3040/3041 (CBT) in Directory Service log after setting 16 LDAP Interface Events diagnostics to 2
WHO CATCHES IT	PINGCASTLE GUERRILLA (ADDOM-013/014, ADNET-001/002)

Watch out: Firewalls, VPN appliances, wireless controllers and copiers doing LDAP user lookup must be moved to LDAPS (636) or StartTLS first. Each 2889 event names one of them. LDAPS satisfies signing, but under channel binding = Always an LDAPS client that does not send a channel-binding token fails; watch event 3039 before moving to Always.

☐ SMB signing required everywhere, SMB1 removed

SET TO	Microsoft network server: Digitally sign communications (always) = Enabled and Microsoft network client: ... (always) = Enabled on DCs, servers and workstations; <code>Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol / Remove-WindowsFeature FS-SMB1</code>
WHY	DCs usually already require signing; member servers and hypervisors usually do not, and an unsigned-SMB hypervisor is the relay target that yields a DC's disk. Windows 11 24H2 Pro/Education/Enterprise require signing both ways by default; Server 2025 requires it outbound only, so member servers still need the server-side GPO. Required signing also disables guest share access, which breaks some copier scan-to-folder setups.
WHERE	Security Options; Server Manager / DISM
WHO CATCHES IT	PINGCASTLE (S-SMB-v1; signing on DCs) GUERRILLA (ADDOM-015, ADNET-003/004, domain policy) MANUAL for individual member servers

Watch out: Old copiers and scanners that write to SMB shares may only speak SMB1. Replace the destination share with an SFTP or cloud drop, or isolate them.

☐ Netlogon secure channel signed and sealed

SET TO	Domain member: Digitally encrypt or sign secure channel data (always) = Enabled; Domain controller: Allow vulnerable Netlogon secure channel connections not configured (enforcement is the default since 2021)
WHY	Zerologon-class attacks.
WHERE	Security Options
WHO CATCHES IT	BUILT-IN (confirm)

☐ Kerberos AES only

SET TO	Network security: Configure encryption types allowed for Kerberos = AES128, AES256, Future; set <code>msDS-SupportedEncryptionTypes</code> to AES on every service account with an SPN; reset the krbtgt and service account passwords once after the change so AES keys exist
WHY	RC4 tickets are what Kerberoasting cracks. A 4769 with encryption type <code>0x17</code> is a roastable ticket. Since the April and July 2026 updates (CVE-2026-20833), DCs default to AES-only for accounts without an explicit <code>msDS-SupportedEncryptionTypes</code> , so RC4 is now opt-in per account; check System log Kdcsvc events 201-209 (203/204/208/209 = blocked) as well as 4769 <code>0x17</code> . A legacy device that still needs RC4 needs an explicit per-account exception.
WHERE	Security Options; <code>Set-ADUser -KerberosEncryptionType AES128,AES256</code>
WHO CATCHES IT	PINGCASTLE (S-DesEnabled; RC4 rules) GUERRILLA (ADKERB-009, ADPRIV-014) MANUAL (watch 4769 0x17 for a month before removing RC4; old Macs, Linux boxes and appliances may need it)

☐ No Kerberos delegation

SET TO	Zero objects with unconstrained delegation (<code>TrustedForDelegation</code>) other than DCs; constrained and resource-based delegation only where a documented app needs it; every admin account flagged Account is sensitive and cannot be delegated
WHY	A server with unconstrained delegation that an attacker controls collects the TGT of every user and computer that connects to it, DCs included.
WHERE	<code>Get-ADComputer -Filter {TrustedForDelegation -eq \$true} ; Get-ADObject -LDAPFilter '(msDS-AllowedToActOnBehalfOfOtherIdentity=*)'</code> ; ADUC account options
WHO CATCHES IT	PINGCASTLE (P-UnconstrainedDelegation, P-Delegated) BLOODHOUND GUERRILLA (ADKERB-004 to 008)

☐ No SPNs on user accounts; gMSA where a service needs one

SET TO	<code>Get-ADUser -Filter {ServicePrincipalName -like '*'}'</code> returns only accounts with 30+ character random passwords or nothing; prefer a group Managed Service Account for anything that needs an SPN
WHY	Any domain user can request a service ticket for any SPN and crack it offline (Kerberoasting). A gMSA's password is 240 bytes, random, and rotates itself (every 30 days by default).
WHERE	<code>New-ADServiceAccount ; Set-ADUser -ServicePrincipalNames</code>
WHO CATCHES IT	PINGCASTLE (P-Kerberoasting) BLOODHOUND GUERRILLA (ADKERB-001/002, ADTRADE-010)

☐ No accounts with pre-authentication disabled

SET TO	<code>Get-ADUser -Filter {DoesNotRequirePreAuth -eq \$true}</code> returns nothing
WHY	AS-REP roasting needs no credentials at all.
WHERE	ADUC account options
WHO CATCHES IT	PINGCASTLE BLOODHOUND GUERRILLA (ADKERB-003, ADPRIV-012)

☐ LLMNR, NetBIOS name service and mDNS off; WPAD blocked

SET TO	Turn off multicast name resolution = Enabled (Computer Configuration > Administrative Templates > Network > DNS Client); NetBIOS over TCP/IP disabled via DHCP option 001 Microsoft Disable NetBIOS = 2 or per-NIC; DNS Global Query Block List keeps <code>wpad</code> and <code>isatap</code> (default)
WHY	Responder-style poisoning of these broadcasts is how an attacker on the student Wi-Fi gets the first NTLM hash.
WHERE	GPO; DHCP console; <code>dnscmd /info /globalqueryblocklist</code>
WHO CATCHES IT	GUERRILLA (ADNET-005 to 008) PINGCASTLE (A-NoGPOLLNMR)

❑ Nobody can add computers to the domain by default

SET TO	<code>Set-ADDomain -Identity (Get-ADDomain) -Replace @{'ms-DS-MachineAccountQuota'=0}</code> ; DDCP Add workstations to domain = Administrators (and the helpdesk computer-management group via delegation, Recipe R12)
WHY	The default lets every user create 10 computer objects, which is the starting point for resource-based delegation and relay attacks.
WHERE	PowerShell; DDCP User Rights Assignment
WHO CATCHES IT	PINGCASTLE BLOODHOUND GUERRILLA (ADACL-009)

Watch out: Delegated CreateChild on the computer OU is not subject to the quota, so the helpdesk group keeps working.

❑ Anonymous and Pre-Windows 2000 access closed

SET TO	Network access: Do not allow anonymous enumeration of SAM accounts and shares = Enabled; remove Authenticated Users (and Anonymous Logon, Everyone) from Pre-Windows 2000 Compatible Access after confirming no legacy app enumerates the directory anonymously; <code>SeNetworkLogonRight</code> on DCs = Administrators, Authenticated Users, Enterprise Domain Controllers (not Everyone)
WHY	Lets unauthenticated devices on the network list users and groups for password spraying.
WHERE	Security Options; ADUC Builtin container; DDCP User Rights
WHO CATCHES IT	PINGCASTLE (A-PreWin2000AuthenticatedUsers, A-PreWin2000Anonymous) GUERRILLA (ADDOM-018)

Watch out: Some older NAS, RADIUS and LDAP-browsing appliances rely on Pre-Win2000 membership. Pilot by removing it for a week and watching for failures.

❑ Kerberos armoring (FAST) and claims

SET TO	DDCP: KDC support for claims, compound authentication and Kerberos armoring = Supported (not "Always provide claims" or "Fail unarmored authentication requests"); Default Domain Policy: Kerberos client support for claims, compound authentication and Kerberos armoring = Enabled. Leave "fail unarmored requests" off until non-Windows clients (Macs, copiers, LDAP-bind appliances) are confirmed working
WHY	Prerequisite for Authentication Policy Silos; also protects the AS exchange from offline password guessing against the TGT.
WHERE	Computer Configuration > Administrative Templates > System > KDC and > Kerberos
WHO CATCHES IT	MANUAL

❑ RDP requires Network Level Authentication, no shadowing without consent

SET TO	Require user authentication for remote connections by using Network Level Authentication = Enabled (<code>UserAuthentication=1</code>); Set rules for remote control of Remote Desktop Services user sessions = Full control with user's permission or No remote control (not <code>Shadow=2</code>)
WHY	NLA removes the pre-authentication RCE surface and credential-capture MITM. A workstation GPO that enables RDP with NLA off and silent shadowing is common in old K-12 baselines.
WHERE	Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security and > Connections
WHO CATCHES IT	MANUAL

❑ Certificate Services: every ESC path closed (only if AD CS exists)

SET TO	No template that combines client-authentication ECU with Enrollee supplies subject and enrollment open to broad groups (ESC1); no Any Purpose or empty ECU templates (ESC2); enrollment-agent templates restricted (ESC3); template and CA object ACLs writable by admins only (ESC4, ESC5, ESC7); <code>EDITF_ATTRIBUTESUBJECTALTNAME2</code> off on the CA (ESC6); web enrollment and CES/CEP endpoints removed, or HTTPS with Extended Protection only (ESC8); <code>IF_ENFORCEENCRYPTICERTREQUEST</code> set on the CA (<code>certutil -setreg CA\InterfaceFlags +IF_ENFORCEENCRYPTICERTREQUEST</code>) (ESC11); CA auditing on; Manager approval on any template that must stay loose
WHY	A misconfigured template lets any domain user request a certificate as any user, Domain Admins included, and the certificate keeps working after password resets. It is the most common Domain Admin path in domains that have a CA, and the one least likely to be noticed because the CA "just works."
WHERE	<code>Invoke-Locksmith -Mode 1</code> (report) and <code>-Mode 4</code> (interactive fix, with backups); Certificate Templates console; <code>certutil -getreg policy\EditFlags</code> on the CA
WHO CATCHES IT	LOCKSMITH (ESC1 to ESC8 plus ESC11/13/15 in current builds) GUERRILLA (ADCS-001 to 019, ESC1 to ESC16 and EKUwu) BLOODHOUND (CE edition ADCS edges) PINGCASTLE (partial)

Watch out: If there is no CA, every tool reports nothing and this row is done. Do not stand up a CA "to modernize" without reading the ESC list first; a default-template CA is born vulnerable.

Gate: 30 days of NTLM and LDAP audit reviewed and every legacy source named; copiers and appliances moved to LDAPS/NTLMv2 or isolated; no 4769 with `0x17` from a Windows client.

Phase 3: Group Policy and SYSVOL

☐ No user right in any GPO beyond Windows defaults, especially in Enforced GPOs

SET TO	Every [Privilege Rights] line in every GptTmpl.inf reviewed; SeTakeOwnershipPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeLoadDriverPrivilege, SeRemoteShutdownPrivilege = *S-1-5-32-544 (Administrators) only, or not set (the default DC grants to Backup/Server/Print Operators are acceptable only if those groups are empty, per Phase 1); SeImpersonatePrivilege = Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE (the default; do not trim it); SeTcbPrivilege empty; SeEnableDelegationPrivilege empty on non-DCs
--------	--

WHY	One line granting a staff group "Take ownership" in an Enforced root GPO reaches every DC and gives every member a trivial path to Domain Admin. Scanners do not parse this file.
-----	---

WHERE	\\<domain>\SYSVOL\<domain>\Policies\{GUID}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf, or the GPO editor > User Rights Assignment; verify with RSOP (Phase 0)
-------	---

WHO CATCHES IT	MANUAL
----------------	--------

Watch out: GptTmpl.inf is UTF-16LE. If you edit it directly instead of through the editor, bump the version (Recipe R2) or clients ignore the change.

☐ Enforced links only where a lower OU must not override

SET TO	Review every link with Enforced set; remove it unless there is a written reason
--------	---

WHY	Enforced inverts the normal precedence: an Enforced root link beats the DDCP on every DC. Most Enforced flags in old domains were set to "make it apply" during troubleshooting and never removed.
-----	--

WHERE	GPMC > link > Enforced
-------	------------------------

WHO CATCHES IT	MANUAL
----------------	--------

❑ NETLOGON and SYSVOL: Authenticated Users read-only

SET TO	<code>icacls \\<dc>\SYSVOL\<domain>\scripts /grant:r "Authenticated Users:(OI)(CI)(RX)" after /save</code> -ing a backup; same for <code>Policies</code> . Apply and verify on each DC
WHY	Anything run from NETLOGON at logon (BGInfo, mapping scripts, inventory agents) runs as every user, admins included. A write ACE for Authenticated Users there is code execution on every machine.
WHERE	Recipe R2
WHO CATCHES IT	PINGCASTLE (P-DelegationLoginScript, P-DelegationGPOData) SCRIPTSENTRY GUERRILLA (ADSCRIPT-001/002/007)

Watch out: ACL changes replicate through DFSR, but a stalled or legacy-FRS SYSVOL will not carry them, and the replicated folder's root ACL is not replicated. Read the ACL back on every DC; apply per-DC if needed.

❑ SYSVOL owned by Administrators, not by a former admin

SET TO	Owner of <code>Policies</code> , <code>scripts</code> and every object beneath = <code>BUILTIN\Administrators</code> on each DC; remove explicit ACEs for disabled or departed accounts
WHY	An owner can rewrite the ACL regardless of what the ACL says. A disabled account that owns every GPO folder becomes Domain Admin the day it is re-enabled.
WHERE	<code>Get-ChildItem ... \ Get-Acl \ Group-Object Owner ; icacls /setowner</code>
WHO CATCHES IT	GUERRILLA (ADACL-011) MANUAL

❑ GPO edit rights = Domain Admins and the GPO's creator only

SET TO	Review each GPO's delegation tab; vendor accounts, helpdesk and "Authenticated Users: Edit" removed; Group Policy Creator Owners empty (Phase 1)
WHY	Edit on a GPO linked to any OU is code execution on every machine in that OU at next refresh.
WHERE	GPMC > GPO > Delegation; <code>Get-GPPermission -All</code>
WHO CATCHES IT	PINGCASTLE (P-DelegationGPOData) BLOODHOUND (GenericWrite on GPO) ADELEG GUERRILLA (ADACL-013/014, ADGPO-007)

☐ No passwords in Group Policy Preferences

SET TO	<code>findstr /S /I cpassword \\<domain>\SYSVOL\<domain>\Policies*.xml</code> returns nothing; any hit means the item is deleted and the account's password reset
WHY	The GPP encryption key has been public since 2012. Every domain user can read SYSVOL.
WHERE	SYSVOL
WHO CATCHES IT	PINGCASTLE (A-PwdGPO) SCRIPTSENTRY GUERRILLA (ADGPO-012, ADTRADE-001)

☐ Logon scripts: no credentials, no writable or non-DC shares

SET TO	Every script referenced by a user's <code>scriptPath</code> , by a GPO, or sitting in NETLOGON reviewed: no hard-coded usernames or passwords, no <code>net use</code> with a password, no calls to shares on member servers that are writable by Authenticated Users, no references to shares or hosts that no longer exist; unused scripts deleted
WHY	A logon script runs as every user who gets it, including admins. A script that maps a drive with an embedded service password leaks it to every user; one that runs an executable from a writable share on a file server runs whatever a student put there; one that points at a hostname nobody owns can be claimed.
WHERE	<code>Invoke-ScriptSentry</code> (reports each class of problem with the file and the offending line); <code>Get-ADUser -Filter {scriptPath -like '*'} -Properties scriptPath</code>
WHO CATCHES IT	SCRIPTSENTRY GUERRILLA (ADSCRIPT-003 to 010) PINGCASTLE (writable-script cases only)

☐ Disabled and "old" GPOs deleted, not kept

SET TO	Any GPO with both halves disabled, or named "old", "test", "copy of", reviewed and deleted (back up first with <code>Backup-GPO</code>)
WHY	They still exist in SYSVOL with their settings (cleartext-password-allowed, minimum length 3, legacy SIDs with batch logon rights) and are one re-enable away from applying.
WHERE	GPMC
WHO CATCHES IT	GUERRILLA (ADGPO-002 to 004) MANUAL

☐ Hardened UNC paths for SYSVOL and NETLOGON

SET TO	Computer Configuration > Administrative Templates > Network > Network Provider > Hardened UNC Paths: <code>*\SYSVOL</code> and <code>*\NETLOGON</code> = <code>RequireMutualAuthentication=1, RequireIntegrity=1</code>
WHY	Prevents a spoofed DC from serving policy to a workstation.
WHERE	GPO linked at the domain root
WHO CATCHES IT	BUILT-IN (default since 2015; confirm it was not undone)

☐ Default Domain Controllers Policy left close to default

SET TO	Non-default user rights removed: <code>SeTcbPrivilege</code> for Backup Operators, batch/service logon for the built-in Administrator; <code>SeNetworkLogonRight</code> hardened from its default (which includes Everyone) to Administrators, Authenticated Users, Enterprise Domain Controllers; <code>SeMachineAccountPrivilege</code> empty or Administrators
WHY	The DDCP is where ten years of "fix the backup job" edits accumulate. Each is a small step an attacker chains.
WHERE	GPMC > Default Domain Controllers Policy > User Rights Assignment
WHO CATCHES IT	MANUAL

☐ GPO backup weekly

SET TO	<code>Backup-GPO -All -Path <backup share></code> plus <code>Get-GPOReport -All -ReportType Html</code> in the AD backup job (Recipe R8)
WHY	Restoring one GPO is a two-minute operation if you have the backup and a rebuild if you do not.
WHERE	Recipe R8
WHO CATCHES IT	N/A

Gate: RSOP on both DCs shows default user rights; SYSVOL ACL and ownership identical on every DC; no `cpassword` hits; every Enforced link documented.

Phase 4: Tier 0 servers, hypervisors and backups

Tier 0 is anything that can yield a DC: the DCs, the hypervisors that run them, the backup server and its repository, the Entra Connect server, any server holding ntds.dit copies, and (for driver reasons, Phase 5) the print server. Treat all of them like DCs.

❑ Servers install updates on a schedule, not on a click

SET TO	Configure Automatic Updates = 4 - Auto download and schedule the install , scheduled day/time and Always automatically restart at the scheduled time on the server and DC OUs; or servers managed by the endpoint tool with a monthly ring
WHY	Option 3 (download and notify) on a server OU means nobody is ever notified. DCs and hypervisors fall a year or two behind while workstations stay current, and public exploit code for Netlogon, Kerberos, LDAP and Hyper-V bugs is live against Tier 0.
WHERE	Computer Configuration > Administrative Templates > Windows Components > Windows Update > Manage end user experience
WHO CATCHES IT	MANUAL (compare build and UBR monthly; Recipe R1)

Watch out: Patch one hypervisor at a time after confirming the other DC is healthy; verify `repadmin /showrepl` after each DC reboot. Guest clocks after a cold boot can be hours off until w32time corrects them, so events right after a reboot are mistimed.

❑ Every server in a server OU; nothing in CN=Computers

SET TO	<code>redircmp "OU=New Joins - Staging,<domain DN>"</code> (run as Domain Admin from any domain-joined machine; it writes to the PDC emulator, which must be online; the OU must already exist); every existing server moved into <code>OU=Servers</code> (block inheritance there) or <code>OU=Tier0,OU=Servers</code> ; staging OU emptied weekly
WHY	Objects in CN=Computers receive every domain-root GPO, including workstation Restricted Groups, shutdown tasks, and Point-and-Print settings. Servers that have sat there for years are the ones the helpdesk is local admin on.
WHERE	<code>redircmp</code> ; ADUC
WHO CATCHES IT	PINGCASTLE (counts CN=Computers objects) GUERRILLA (ADTIER-006) MANUAL for the consequence

Watch out: "Unwilling To Perform" from `redircmp` means the domain functional level is below 2003 or the target DN is wrong (OU= vs CN=); "No Such Object" means the OU doesn't exist. Blocking inheritance on `OU=Servers` also cuts off domain-linked baselines and update policy unless those links are Enforced. Moving a server changes which GPOs it gets (update policy, baseline, loss of workstation GPOs); review the destination OU's links first. The helpdesk may lose RDP to a server they used for ADUC; add them to local Remote Desktop Users there, not Administrators.

❑ Hypervisors as Tier 0

SET TO	Local Administrators = Domain Admins (+ the backup service account); SMB signing required; Print Spooler disabled; no RDP from workstations; patched on the same cadence as DCs; VM configuration and VHDX folders not shared; management NIC on an admin VLAN
WHY	Hypervisor admin = mount the DC's VHDX offline = ntfs.dit + SYSTEM hive = every hash.
WHERE	Hyper-V / vSphere host configuration
WHO CATCHES IT	GUERRILLA (ADTIER-003) MANUAL

❑ Backup server and repository as Tier 0

SET TO	Backup software runs as a dedicated <code>svc-backup</code> account (never a human Domain Admin); that account is local admin on the hypervisors and the backup server only; repository is immutable, offline-copied, or at minimum on a share only the backup account can write; backup console admins = Domain Admins
WHY	The backup server can restore a DC anywhere and holds credentials to every host. A human admin's password stored in the backup console is recoverable by any local admin there and breaks every job the day that admin goes into Protected Users.
WHERE	Backup console > Credentials; local groups on hosts
WHO CATCHES IT	GUERRILLA (ADTIER-002) MANUAL

Watch out: Give the backup server a DNS A record and connect to it by name. Backup servers are often reachable only by IP, which forces NTLM.

❑ Entra Connect server as Tier 0

SET TO	Local Administrators = Domain Admins only; <code>ADSyncAdmins</code> = current Domain Admins only; exactly one <code>MSOL_*</code> (or the newer connector account) holds DCSync; stale <code>MSOL_*</code> accounts from retired or reinstalled Entra Connect servers deleted along with their explicit ACEs on the domain root and AdminSDHolder; patched; off the user VLAN
WHY	The sync account can replicate every hash by design. Anyone who is local admin on this server, or in <code>ADSyncAdmins</code> , can extract its credential from the <code>ADSync</code> database.
WHERE	ADUC; <code>Get-Acl AD:\<domain DN></code> and <code>AD:\CN=AdminSDHolder,CN=System,...</code> ; Synchronization Service Manager
WHO CATCHES IT	BLOODHOUND (DCSync edge) PINGCASTLE GUERRILLA (ADTIER-001, ADPRIV-028) MANUAL for <code>ADSyncAdmins</code> and local admins

❑ DC backups: VM-level first, system state second, IFM only with eyes open

SET TO

(1) Application-consistent VM-level backups of every DC, taken by a Tier 0 backup server with VSS / application-aware processing on, to an immutable or offline-copied repository; this is the restore you will actually use. (2) A `wbadmin` system-state backup on one DC to a share only DCs can write, on its own schedule; this is the authoritative-restore path. (3) `Backup-GPO -All` plus an LDIF/CSV export weekly for the "restore one GPO, one OU, one group" cases. (4) An IFM copy (`ntdsutil ifm`) is **optional and not generally advised**: it is a complete `ntds.dit` with every password hash as a plain file on whatever server the script wrote to. Take one only when you need an offline-mountable copy for forensics, keep it on a DC or an encrypted Tier 0 volume, and delete it on a schedule (Recipe R8)

WHY

Every backup that holds a DC's disk holds every hash; the question is how many copies exist and who can reach them. A VM backup is one copy, inside the backup repository, behind the backup product's access control. An IFM is a second copy sitting as files, and in practice it ends up on an automation server with a helpdesk group in local Administrators. PingCastle's and Guerrilla's "backup too old" rules are satisfied by any method that updates the DC's backup timestamp (system state, and VM backups that invoke the in-guest NTDS VSS writer as a full, not copy, backup), so there is no scanner reason to prefer IFM.

WHERE

Backup console (application-aware processing on for DC VMs; repository immutability on); `wbadmin start systemstatebackup` ; Recipe R8

WHO CATCHES IT

PINGCASTLE (A-BackupMetadata) **GUERRILLA** (ADTIER-002 for the backup account's group membership) **MANUAL** for where the copies land and who can read them

Watch out: Never revert a DC VM to a checkpoint or restore a VM backup older than the tombstone lifetime; VM-GenerationID (Server 2012+ guest on a hypervisor that exposes it) protects against USN rollback when a checkpoint is applied or an image restored, but it is not a substitute for a VSS backup and does nothing on hosts that don't expose it, so still avoid checkpoint reverts on DCs. Verify `repadmin /showrepl` and `Get-ADReplicationAttributeMetadata` after any restore. If you do schedule an IFM or export task as SYSTEM on a DC, read the log after the **first** run: a task that "succeeds" in one second with exit code 1 is application control blocking PowerShell from reading the script; allow the hash before scheduling. The existing system-state job that "has always run" may have stopped months ago; check its last-success date.

☐ If ntds.dit copies exist as files: Domain Admins only, and not local admins

SET TO	First ask whether the copy needs to exist (previous row). If it does: destination folder ACL = SYSTEM, the DC's computer account (Modify), and Domain Admins; inheritance off; no helpdesk or automation group in local Administrators on the host; encrypted volume. Optionally a conditional ACE requiring Domain Admins and Protected Users ((XA;OICI;FA;;;WD;((Member_of {SID(DA)}) && (Member_of {SID(AP)}))))
WHY	The folder ACL does not stop a local admin (take ownership, backup privilege). Only tiering the host does, and only not making the copy removes the risk.
WHERE	<code>icacls</code> ; conditional ACE via <code>ConvertStringSecurityDescriptorToSecurityDescriptorW</code> (the .NET SDDL parser rejects callback ACEs)
WHO CATCHES IT	MANUAL

Watch out: Never point a backup at a drive letter that is a cloud-sync client. A non-elevated admin session that tightens the ACL can lock itself out of its own output; keep an explicit ACE for your own account while working.

☐ Print Spooler off on every server that does not print

SET TO	<code>Stop-Service Spooler; Set-Service Spooler -StartupType Disabled</code> on DCs (mandatory), hypervisors, DHCP, DNS, Entra Connect, backup, automation and file servers
WHY	PrintNightmare and its successors are SYSTEM on the DC. Nothing on a DC needs to print.
WHERE	GPO > System Services, or per server
WHO CATCHES IT	PINGCASTLE (A-DC-Spooler) GUERRILLA (ADDOM-019, ADNET-009) for DCs MANUAL for other servers

☐ Security log large enough to matter

SET TO	Specify the maximum log file size for Security = 4,194,240 KB (4 GB) on DCs, 1 GB on servers
WHY	A busy DC at the default size (20 MB on clients, larger on recent servers) keeps only days. Investigations start a week after the event.
WHERE	Computer Configuration > Administrative Templates > Windows Components > Event Log Service > Security
WHO CATCHES IT	MANUAL

❑ DCs take time from a real source, not the hypervisor

SET TO	PDC emulator: <code>w32tm /config /manualpeerlist:"<ntp1>,0x9 <ntp2>,0x9" /syncfromflags:manual /reliable:yes</code> ; on every DC VM, <code>VMICTimeProvider</code> Enabled=0 under <code>HKLM\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders</code> ; hypervisors sync to the same external source, never to a DC they host
WHY	A DC that takes time from the host which takes time from the DC is circular. Kerberos tolerates 5 minutes; a cold boot can be hours off.
WHERE	<code>w32tm</code> ; registry
WHO CATCHES IT	MANUAL

❑ DNS hygiene

SET TO	Secure dynamic updates only on every AD-integrated zone; scavenging on with sane refresh/no-refresh; A/PTR/SRV records for retired DCs deleted; every server has an A record (so management can use FQDN); forwarders reachable and a second resolver path tested
WHY	A stale DC name that resolves to a reusable IP can be impersonated for anything still configured against it. A server without a DNS record forces NTLM.
WHERE	DNS Manager
WHO CATCHES IT	PINGCASTLE (A-DnsZoneUpdate rules) GUERRILLA (ADDOM-012, ADSTALE-011) MANUAL

Gate: every Tier 0 host patched to the current cumulative update; local Administrators on each = Domain Admins plus documented service accounts; weekly AD backup produced output twice; no object left in CN=Computers.

Phase 5: Workstations

❑ Windows LAPS

SET TO	Update-LapsADSchema once (schema master, Schema Admins membership added for the duration and removed after); Set-LapsADComputerSelfPermission on the workstation and server OUs; GPO: Configure password backup directory = Active Directory, Password Settings = 24 characters / 30 days, Post-authentication actions = Reset password and log off, Name of administrator account to manage only if the built-in account was renamed (Recipe R6)
WHY	Every imaged PC shares one local Administrator password. One compromised PC becomes every PC by pass-the-hash. LAPS makes each password unique and rotating.
WHERE	Computer Configuration > Administrative Templates > System > LAPS
WHO CATCHES IT	PINGCASTLE (A-LAPS-Not-Installed) GUERRILLA (ADPWD-016 to 018, ADGPO-023)

Watch out: Extending the schema needs a fresh Kerberos ticket after being added to Schema Admins. If the admin is in Protected Users, that means lock/unlock or sign-out, not [klist purge](#). Remove yourself from Schema Admins afterwards; PingCastle charges for a non-empty Schema Admins.

❑ No extra local administrators; local accounts cannot log on over the network

SET TO	Local Administrators on workstations = the LAPS-managed account, Domain Admins (harmless with the deny-logon GPO) and the workstation-admin group; every vendor, imaging, "admin" and "tech" local account removed; Deny access to this computer from the network = S-1-5-114 (Local account and member of Administrators group)
WHY	Leftover local accounts share passwords across the fleet and are exempt from LAPS. The S-1-5-114 deny makes even a leaked local admin password useless remotely.
WHERE	Restricted Groups; User Rights Assignment
WHO CATCHES IT	BLOODHOUND (if local groups collected) MANUAL

❑ Credential Guard and LSA protection on

SET TO	Turn On Virtualization Based Security = Enabled, Credential Guard = Enabled with UEFI lock; LSASS as protected process (<code>RunAsPPL=2</code> under <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa</code> , or the Configures LSASS to run as a protected process template on 22H2+)
WHY	Stops Mimikatz-style credential dumping from memory on the PC. Does not stop ticket theft from a process the user runs, which is why the deny-logon GPO still matters.
WHERE	Computer Configuration > Administrative Templates > System > Device Guard; > System > Local Security Authority
WHO CATCHES IT	BUILT-IN only on Windows 11 22H2+ Enterprise/Education, domain-joined, on capable hardware (LSA protection only on clean installs, and without UEFI lock; <code>RunAsPPL=2</code> is honored only on Windows 11 22H2+, older builds need <code>1</code>) (confirm with <code>Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard</code>)

❑ RDP on workstations: NLA, restricted, or off

SET TO	Either RDP disabled on workstations, or enabled with NLA (Phase 2), Allow log on through Remote Desktop Services = Remote Desktop Users only, and shadowing with consent
WHY	Workstation RDP enabled domain-wide "for support" with NLA off is a pre-auth attack surface on every PC.
WHERE	Remote Desktop Session Host policies; User Rights Assignment
WHO CATCHES IT	MANUAL

❑ Point and Print restrictions at Microsoft defaults, after drivers are pre-staged

SET TO	<code>RestrictDriverInstallationToAdministrators=1</code> , <code>NoWarningNoElevationOnInstall=0</code> , <code>UpdatePromptSettings=0</code> (Computer Configuration > Administrative Templates > Printers > Point and Print Restrictions and Limits print driver installation to Administrators); Package Point and print - Approved servers = the print server's FQDN. Only after every driver model name the print server uses has been installed on every PC in machine context (Recipe R7)
WHY	With the restrictions off, anyone who controls the print server (or any server a PC can be pointed at) installs a driver as SYSTEM on every PC without a prompt. With the restrictions on but drivers not pre-staged, every staff member gets a UAC prompt for every printer, district-wide, the next morning.
WHERE	Recipe R7
WHO CATCHES IT	MANUAL

Watch out: Group Policy Preferences printer items re-evaluate connections at every refresh, so the number of PCs that need a driver pull is far larger than a small sample suggests. Pilot one building for a week.

❑ Print Spooler does not accept inbound connections on workstations

SET TO	Allow Print Spooler to accept client connections = Disabled (<code>RegisterSpoolerRemoteRpcEndPoint=2</code>) linked at the workstation OU and the server OU, with a Deny Apply-Group-Policy ACE for the print server's computer account
WHY	Removes the spooler RPC interface from every machine that does not share a printer, which is all of them except the print server. No user impact.
WHERE	Computer Configuration > Administrative Templates > Printers
WHO CATCHES IT	MANUAL

❑ Computer names 15 characters or fewer

SET TO	Naming standard enforced at imaging; for existing longer names, add <code>HOST/<fullname></code> and <code>RestrictedKrbHost/<fullname></code> SPNs to the computer object (Recipe R10), or rename
WHY	Only the short-name SPN is truncated to 15 characters, so a request for <code>HOST/<full short name></code> (no domain suffix) finds no SPN. DCOM/WMI's second authentication step asks for <code>RPCSS/<fullname></code> , finds no SPN, and falls back to NTLM, which Protected Users refuses: remote management of those PCs fails with "Access is denied" for every protected admin. Long names also break the secure channel on some builds (symptom: "the clock is always wrong").
WHERE	Recipe R10
WHO CATCHES IT	MANUAL

❑ Windows 10 and other end-of-life machines retired

SET TO	No enabled computer object with an OS past end of support; Windows 10 (October 2025), Server 2012 R2 (October 2023), Server 2016 (January 2027)
WHY	Unpatchable OS = permanent foothold.
WHERE	<code>Get-ADComputer -Filter * -Properties OperatingSystem,OperatingSystemVersion</code>
WHO CATCHES IT	PINGCASTLE (S-OS-W10, S-OS-2012 and similar) GUERRILLA (ADSTALE-005/006)

❑ Host firewall on, management ports only from the admin host

SET TO	Windows Firewall on in all profiles; inbound 135, 445, 5985/5986 and the dynamic RPC range allowed only from the admin host and IT subnet; everything else default-deny
WHY	Lateral movement between workstations needs these ports. Students on the same VLAN should not be able to reach a teacher PC's SMB.
WHERE	Computer Configuration > Windows Settings > Security Settings > Windows Defender Firewall
WHO CATCHES IT	GUERRILLA (ADGPO-019, policy present) MANUAL for the rule contents

❑ Application control with a documented allow process

SET TO	ThreatLocker, AppLocker or WDAC in enforce mode on servers and DCs first, workstations after a learning period; a written procedure for allowing a new hash, and for lifting a time-based lockdown policy out of hours
WHY	Stops the payload even when a credential is stolen.
WHERE	Vendor console or Computer Configuration > Windows Settings > Security Settings > Application Control Policies
WHO CATCHES IT	GUERRILLA (ADGPO-022, AppLocker/WDAC policy present)

Watch out: See the Gotchas section. Application control will block your own scheduled backup script, your own logon-time utility from NETLOGON, and your diagnosis of a network problem (some products rewrite DNS answers on the host). Every one of those looks like something else.

❑ Defender tamper protection, ASR rules, and cached logons

SET TO	Tamper protection on (including DCs); attack surface reduction rules in block mode for Office child processes, credential stealing from LSASS, and executable content from email; Interactive logon: Number of previous logons to cache = 0 on servers (leave laptops at the default)
WHY	Defaults that get turned off during troubleshooting and never turned back on.
WHERE	Defender policy; Security Options
WHO CATCHES IT	BUILT-IN (confirm) GUERRILLA (ADLOG-005)

Gate: LAPS password readable for every pilot PC; Point-and-Print pilot building one week with no prompts; no long host names without SPNs; firewall rules verified from a student VLAN.

Phase 6: Service accounts, scheduled tasks and applications

☐ No scheduled task or service runs as a human admin

SET TO	Every task with a stored domain password and every service with a domain <code>StartName</code> moved to a gMSA, a <code>svc-</code> account, LocalSystem, or deleted (Recipe R5)
WHY	A stored password is recoverable by any local admin on that server. A task running as the admin "interactively" (no stored password) depends on that admin's live Kerberos ticket and silently fails overnight once the admin is in Protected Users. A service running as an admin fails with error 1069 the first time that admin's password changes, usually at a weekend reboot.
WHERE	Recipe R1 (find), Recipe R5 (fix)
WHO CATCHES IT	MANUAL

☐ Service account pattern

SET TO	<code>svc-<purpose></code> in a Service Accounts OU; not a member of any admin group; password never expires, cannot change password, 30+ random characters typed into the task and stored nowhere else; <code>LogonWorkstations</code> = the one host; NTFS Modify on the script folder only; Log on as a batch job granted on that host; task logon type Password (runs whether or not anyone is signed in); fine-grained password policy applied to a global security group that holds every <code>svc-</code> account (a PSO cannot be applied to an OU; Phase 7)
WHY	Least privilege and no human dependency. The error for a missing batch-logon right is <code>0x80070569</code> .
WHERE	Recipe R5
WHO CATCHES IT	PINGCASTLE (A-NoServicePolicy if no FGPP exists for them) GUERRILLA (ADPWD-002/003, ADTIER-007) MANUAL

Watch out: Granting the batch-logon right needs an **elevated** session on the host; a non-elevated admin session cannot. A DPAPI-protected credential file is bound to the user who created it; the service account needs its own copy, created in its own context. Anything that reads a mapped cloud drive (Google Drive for desktop, OneDrive) only works in the interactive session of the user who mounted it and cannot move to a service account without rework.

❑ Applications that validate admin logins over NTLM get their own login

SET TO	Print management, monitoring, helpdesk and backup consoles that authenticate "Windows users" via NTLM: create a dedicated non-protected login per admin (<code><user>-pc</code> style) in the application, or switch the app to Kerberos/SAML
WHY	Once the real admin is in Protected Users the app says "invalid username or password" and the DC logs <code>0xC000006E</code> . Weakening the admin to fix the app is the wrong direction.
WHERE	Application's own user management
WHO CATCHES IT	MANUAL

❑ LDAP bind accounts for firewalls, VPNs, wireless, copiers

SET TO	One non-privileged account per appliance, in the Service Accounts OU, LDAPS only, read-only, no group memberships beyond Domain Users, password rotated and the appliance updated at the same time
WHY	The bind password sits in the appliance config, often exportable. It must not be a Domain Admin, and it must not travel over cleartext LDAP.
WHERE	ADUC; appliance LDAP settings
WHO CATCHES IT	PINGCASTLE GUERRILLA (ADPRIV-024, flags it only if it is privileged or has an SPN)

❑ Script and credential folders on automation servers

SET TO	<code>C:\Scripts</code> (or wherever tasks run from) = SYSTEM, Administrators and the specific <code>svc-</code> accounts; inherited BUILTIN\Users CreateFiles/CreateDirectories removed; credential files (API keys, service-account JSON, DPAPI blobs) in a sub-folder with an explicit ACL for the one account that uses them
WHY	With the default inherited ACL any local user can plant a file where a Domain Admin task executes, or read the Google service-account key.
WHERE	<code>icacls <folder> /inheritance:r /grant:r "SYSTEM:(OI)(CI)F" "Administrators:(OI)(CI)F" "<svc>:(OI)(CI)M"</code>
WHO CATCHES IT	MANUAL

Watch out: `icacls /reset /T` re-inherits the parent; do `/inheritance:r /grant` on the parent **after** resetting children. A non-elevated admin session cannot set an owner.

❑ Legacy sync scripts write no PII and no passwords to logs

SET TO	Every scheduled script's output reviewed; logs contain usernames and IDs only; any credential hand-off file (new-student passwords for an office) written to an ACL'd folder and deleted on a schedule; old log archives containing password columns deleted (Recipe R11)
WHY	A SIS export with a password column, copied to a log folder hourly for a year, is every student password in the district in plaintext, readable by every local user.
WHERE	Recipe R11
WHO CATCHES IT	MANUAL (SCRIPTSENTRY and GUERRILLA ADSCRIPT-004/006 cover logon scripts only)

❑ Assistants and automation tooling denied the credential folders

SET TO	Deny rules in any AI assistant, RMM or scripting tool configuration for the credential folder, the SIS export file, and backup locations
WHY	A tool that can read the folder will eventually read it into a transcript or a ticket.
WHERE	Tool's settings (for Claude Code: <code>permissions.deny</code> entries in <code>settings.json</code>)
WHO CATCHES IT	MANUAL

Gate: Recipe R1's task and service query returns only `svc-` , gMSA and built-in accounts; every `svc-` account documented with owner, host and purpose.

Phase 7: Directory hygiene

❑ Stale users disabled, then deleted

SET TO	Enabled users with no logon in 180 days disabled and moved to a Disabled OU with a description stamp; never-logged-on accounts older than 90 days disabled; disabled accounts older than one year deleted (Recycle Bin on)
WHY	Hundreds of dormant accounts are the password-spraying surface. A seasonal or default password on an account nobody watches is the first foothold.
WHERE	<code>Search-ADAccount -AccountInactive -TimeSpan 180 -UsersOnly</code>
WHO CATCHES IT	PINGCASTLE (S-Inactive, P-Inactive) GUERRILLA (ADSTALE-001/003)

❑ pwdLastSet = 0 forced to change; no "password not required"

SET TO	Every enabled account with <code>pwdLastSet=0</code> ("must change at next logon" left set from creation) either used or disabled; <code>PasswordNotRequired</code> false on every account
WHY	An account that was never logged on since creation still has the creation password; those are predictable. <code>PasswordNotRequired</code> allows a blank password regardless of policy.
WHERE	<code>Get-ADUser -Filter {pwdLastSet -eq 0 -and Enabled -eq \$true} ; -Filter {PasswordNotRequired -eq \$true}</code>
WHO CATCHES IT	PINGCASTLE (S-PwdNotRequired) GUERRILLA (ADPWD-010, ADPRIV-011)

Watch out: An account with "must change at next logon" cannot authenticate to applications that do username/password against AD (print release, web portals) until someone signs in interactively once.

❑ Password policy with fine-grained policies

SET TO	Default domain policy: 12+ characters, complexity on, history 24, lockout 10 / 15 min; FGPP for <code>svc-</code> accounts: 30+ characters, never expires; FGPP for admins: 15+ characters, 365-day maximum age; consider Entra password protection or a banned-password list
WHY	One policy cannot fit staff, service accounts and admins. A missing FGPP for service accounts is a PingCastle finding on its own.
WHERE	Active Directory Administrative Center > System > Password Settings Container
WHO CATCHES IT	PINGCASTLE (A-MinPwdLen, A-NoServicePolicy) GUERRILLA (ADPWD-001 to 008, 021/022)

❑ Stale computers disabled, then deleted, after BitLocker keys are exported

SET TO	Computers with no logon and no machine-password change in 90+ days disabled, stamped, and moved to a Disabled OU; deleted after a further 90 days; before any delete , export every <code>msFVE-RecoveryInformation</code> object (recovery password, GUID, parent computer) to a file kept with the backups
WHY	Stale computer objects are relay and resource-based-delegation fodder. BitLocker recovery keys are child objects of the computer and die with it.
WHERE	<code>Search-ADAccount -AccountInactive -ComputersOnly ; Get-ADObject -Filter {objectClass -eq 'msFVE-RecoveryInformation'} -Properties msFVE-RecoveryPassword</code>
WHO CATCHES IT	PINGCASTLE (S-C-Inactive) GUERRILLA (ADSTALE-002, ADPWD-020, ADTRADE-003)

Watch out: A decommission list from a human will contain machines that authenticated this morning. Check `LastLogonDate`, `PasswordLastSet` and recent 4768 events before deleting anything from a list. Exclude `AZUREADSSOACC` (it never logs on; its password changes only when you roll the key) and the Entra Connect server from stale sweeps. If Entra Connect syncs computer objects, a bulk delete shows up as a bulk Entra device delete on the next cycle, and Entra Connect stops export at its accidental-delete threshold (default 500) until you raise or disable it temporarily.

❑ Student accounts out of AD if students live in Google

SET TO	If student identity is Google (Chromebooks, SIS-provisioned Google accounts), delete the student user tree from AD after the checks in Recipe R9; keep student OUs and groups only if something references them
WHY	Thousands of accounts nobody uses are thousands of spraying targets and a password-divergence problem every time the SIS and AD disagree. Removing them also shrinks every other query in this handout.
WHERE	Recipe R9
WHO CATCHES IT	PINGCASTLE (counts them as inactive) GUERRILLA (ADSTALE-001)

Watch out: Find and neutralise every directory-sync tool first (Recipe R9). A dormant Google Cloud Directory Sync config pointed at the student OU with "suspend users" will suspend every student Google account the next time someone runs it.

❑ OU structure that policies can be scoped to

SET TO	Separate OUs for workstations (by building if useful), servers, Tier 0 servers, staging, service accounts, admin accounts, disabled users, disabled computers; nothing live in CN=Users or CN=Computers; empty OUs deleted
WHY	Every GPO and every delegation in this handout is applied per OU.
WHERE	ADUC
WHO CATCHES IT	GUERRILLA (ADSTALE-009, abandoned OUs) MANUAL

❑ Orphaned ACEs and legacy groups removed

SET TO	Explicit ACEs for deleted SIDs, for Exchange groups when Exchange is gone, for RAS and IAS Servers, MDT, imaging groups and individual humans on OUs: removed; empty legacy groups that still hold Write on something: deleted
WHY	Any future member of an empty group with GenericAll on an OU inherits it. An individual's <code>User-Force-Change-Password</code> on a staff OU is a takeover of every account in it.
WHERE	BloodHound, or a <code>Get-Acl</code> sweep of every OU and container filtered to GenericAll / WriteDacl / WriteOwner / ExtendedRight / WriteProperty
WHO CATCHES IT	BLOODHOUND ADELEG (built for exactly this: every ACE that is not a Windows default, per container, diffable between runs) PINGCASTLE (P-Delegated* rules) GUERRILLA (ADACL-001 to 008, 010, 012, 015)

❑ Retired DC remnants gone

SET TO	No computer object, DNS A/SRV record, NTDS Settings object, or SPN left for a DC that no longer exists; <code>nltest /dclist</code> and <code>Get-ADDomainController -Filter *</code> agree with reality
WHY	A retired DC's name pointing at a reusable IP can be impersonated for any client still configured against it.
WHERE	<code>ntdsutil</code> metadata cleanup; DNS Manager; Sites and Services
WHO CATCHES IT	PINGCASTLE (S-DC rules) GUERRILLA (ADDOM-004, ADTRADE-002)

❑ Vendor and contractor accounts scoped and expiring

SET TO	Every vendor account has an owner, an expiration date (Set-ADAccountExpiration), no admin group membership, and membership in Remote Desktop Users only on the host it needs
WHY	Vendor accounts with 10-year-old passwords and domain-wide RDP are a reliable finding.
WHERE	ADUC
WHO CATCHES IT	PINGCASTLE (password age, never expires) GUERRILLA (ADPWD-009, ADPWD-015) MANUAL for scope

Gate: zero enabled accounts inactive over 180 days; zero [pwdLastSet=0](#) on enabled accounts; FGPPs in place; CN=Users holds only built-ins; BitLocker export file verified readable.

Phase 8: Cloud sync boundaries (Entra Connect, Google sync)

☐ Entra Connect OU filtering matches intent

SET TO	Synchronization Service Manager > AD connector > Configure Directory Partitions > Containers: only the OUs that should become Entra users; the student OU excluded if students are Google-only; the Disabled OUs excluded; computer objects excluded unless hybrid join is wanted; verified in the wizard, not assumed
WHY	Sync scope decides what a bulk AD change does in the cloud. Including computers means a stale-computer purge becomes an Entra device purge.
WHERE	Entra Connect wizard > Customize synchronization options > Domain and OU filtering; Device options
WHO CATCHES IT	MANUAL

☐ Hybrid join and device registration only if wanted

SET TO	If devices should not be in Entra: set Register domain joined computers as devices to Disabled (deleting the GPO leaves it unconfigured), delete the forest Service Connection Point (<code>CN=62a0ff2e-97b9-4513-943f-0d221bd30080,CN=Device Registration Configuration,CN=Services,CN=Configuration,<forest DN></code>) after exporting it, and run <code>dsregcmd /leave</code> on already-joined PCs
WHY	Every hybrid-joined device is another identity in the cloud with its own attack surface, and the SCP makes every new domain join register automatically.
WHERE	GPO; ADSI Edit (Configuration partition); <code>dsregcmd</code>
WHO CATCHES IT	MANUAL

☐ Seamless SSO computer account handled deliberately

SET TO	If Seamless SSO is used: <code>AZUREADSSOACC</code> excluded from stale sweeps and its Kerberos key rolled every 30 days (<code>Update-AzureADSSOForest</code>). If not used: disable Seamless SSO in Entra Connect, then delete the account (export with <code>Export-Clxml</code> first; Recycle Bin keeps it 180 days)
WHY	The account's key decrypts every user's SSO ticket. A key that has never been rotated is a silver-ticket generator; a stale-sweep that disables it breaks SSO for everyone.
WHERE	Entra Connect wizard; PowerShell
WHO CATCHES IT	PINGCASTLE (T-AzureADSSO) GUERRILLA (ADTRADE-005)

❑ Google Cloud Directory Sync removed or scoped

SET TO	If Google accounts are provisioned from the SIS by scripts, GCDS is uninstalled, its config files deleted, and its OAuth grant revoked in the Admin console. If GCDS is used: scope limited to the staff OU, suspension limit set, config backed up, and a documented owner
WHY	GCDS reads an OU and makes Google match it. Left configured against an OU that is about to be emptied, it suspends or deletes the Google accounts to match.
WHERE	GCDS Configuration Manager; Admin console > Security > API controls > Domain-wide delegation and the admin user's connected apps
WHO CATCHES IT	MANUAL

❑ Print management and other AD-fed systems: scope checked

SET TO	Any system that syncs users or groups from AD (print management, library, cafeteria, LMS) reviewed for "delete on sync" and "suspend on sync" flags before any bulk AD change
WHY	Same failure as GCDS, one system at a time.
WHERE	Each product's sync settings
WHO CATCHES IT	MANUAL

❑ SIS-to-Google provisioning: no plaintext password trail

SET TO	The provisioning script keeps a state file of minted credentials (so it never re-randomises a password Google already has), logs usernames and IDs only, hands credentials to offices through an ACL'd folder with scheduled deletion, and never copies the SIS export anywhere else
WHY	See Phase 6 and Recipe R11.
WHERE	Script review
WHO CATCHES IT	MANUAL

Watch out: Do not use Google's `lastLoginTime` to decide a student is locked out. Chromebook users sign in with cached credentials and the field rarely updates; a bulk password reset based on it changes passwords for students who knew theirs, and their Chromebooks report "password changed" days later.

Gate: Entra Connect scope documented; no sync tool exists without an owner; a bulk test delete of one disabled test user and one disabled test computer produces the expected (and only the expected) cloud effect.

Phase 9: Detection

☐ Advanced audit policy on DCs

SET TO	Audit: Force audit policy subcategory settings to override = Enabled; Success+Failure for Logon, Kerberos Authentication Service, Kerberos Service Ticket Operations, Credential Validation, Directory Service Access, Directory Service Changes, Security Group Management, User Account Management, Process Creation (with command line), Sensitive Privilege Use, Audit Policy Change; Success for Computer Account Management
WHY	Without subcategory auditing the DC does not log 5136 (GPO/ACL change), and the legacy category policies cannot be tuned.
WHERE	Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration (DC GPO)
WHO CATCHES IT	PINGCASTLE (A-AuditDC) GUERRILLA (ADLOG-001, ADLOG-004, ADGPO-018)

☐ SACL for DCSync on the domain root

SET TO	Auditing entry on the domain root: Everyone, Success+Failure, All extended rights, this object only
WHY	Produces a 4662 with the replication GUIDs every time anything replicates. Alert when the subject is not a DC or the one Entra Connect account (Recipe R13).
WHERE	ADSI Edit > domain root > Properties > Security > Advanced > Auditing
WHO CATCHES IT	MANUAL

☐ PowerShell logging

SET TO	Turn on Module Logging (*), Turn on PowerShell Script Block Logging, and transcription to a write-only share, on DCs and servers at minimum
WHY	Most post-exploitation is PowerShell.
WHERE	Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell
WHO CATCHES IT	PINGCASTLE (A-AuditPowershell) GUERRILLA (ADLOG-002/003, ADGPO-021)

❑ Events forwarded off the box

SET TO	Windows Event Forwarding (source-initiated, GPO Configure target Subscription Manager) from DCs and Tier 0 servers to a collector, or a SIEM agent; at minimum 4624, 4625, 4648, 4662, 4672, 4688, 4697, 4698, 4719, 4720, 4724, 4728, 4732, 4756, 4768, 4769, 4771, 4776, 5136, 5137, 5141, 7045
WHY	A DC's log is the first thing an attacker clears, and a 4 GB log still wraps in a week on a busy DC.
WHERE	Computer Configuration > Administrative Templates > Windows Components > Event Forwarding; <code>wecutil</code> on the collector
WHO CATCHES IT	GUERRILLA (ADLOG-006, subscription manager configured) MANUAL (PINGCASTLE checks only that the audit policy exists)

❑ Alerts that matter

SET TO	Any 4662 with GUID <code>1131f6ad-9c07-11d1-f79f-00c04fc2dcd2</code> or <code>1131f6aa-...</code> from a subject that is not a DC or the sync account; 4728/4732/4756 on Domain Admins, Enterprise Admins, Schema Admins, Administrators, Protected Users, Group Policy Creator Owners; 4769 with ticket encryption <code>0x17</code> ; 4768 for an admin from a new source IP; 5136/5137 on any GPO or on AdminSDHolder; 4624 type 10 (RDP) to a DC from anything but the admin host; 7045 (new service) on a DC; any logon for the break-glass account
WHY	Each is one line that marks a DCSync, a privilege escalation, a Kerberoast, or admin credentials in a new place.
WHERE	Collector / SIEM rules; or scheduled <code>Get-WinEvent</code> scripts that mail a digest
WHO CATCHES IT	MANUAL

❑ Know what the noise means

SET TO	Document for the helpdesk: 4776/4625 with <code>0xC000006E</code> = Protected Users refusing NTLM, not a bad password; 4771 <code>0x18</code> every ~100 minutes from a server = a stale disconnected session holding an old password (log it off; set a disconnected-session limit); 4771 at the same second daily = a scheduled task with a stored password; 4625 every 10 minutes from the backup server = a stored credential that changed
WHY	Real alerts drown in these within a week of Phase 1 unless everyone knows what they look like.
WHERE	Runbook
WHO CATCHES IT	N/A

❑ Defender for Identity on DCs (optional)

SET TO	Sensor on each DC; alerts for DCSync, Golden Ticket, lateral movement, reconnaissance
WHY	Buys most of the alerting above with no collector to build.
WHERE	Microsoft Defender portal
WHO CATCHES IT	PAID (EMS E5/A5, Microsoft 365 E5/A5 or E5/A5 Security, or a standalone Defender for Identity license; Entra ID P2 does not include it)

Gate: a test DCSync (DSInternals `Get-ADReplAccount -SamAccountName <test> -Server <dc>` run from the admin host by an account holding replication rights) produces an alert within the hour; a test addition to Domain Admins produces an alert; the helpdesk runbook is written.

Phase 9a: Seams the review surfaced

These close the gaps between the two directories, between "detect" and "respond", and in the threat model itself. The attacker's agent never touches your endpoints; it reaches you over LDAP, SMB, Kerberos and HTTPS with credentials it harvested, and its command-and-control is a legitimate AI API. Everything here assumes that: the sync server and the backup server as Tier 0, servers that cannot reach the internet, the devices that are not Windows, decoys in the places an agent looks first, automated response on the rules that are never legitimate, and the procedures a vishing call and a real compromise actually test.

The sync bridge and the backup server

☐ Sync server (Entra Connect, GCDS) treated as Tier 0

SET TO	The server running Entra Connect, Google Cloud Directory Sync or Password Sync lives in <code>OU=Tier0,OU=Servers</code> , gets the DC GPO baseline (deny-logon rights for non-Tier-0 admins, LAPS, no other roles, no browser use), is patched on the DC schedule and backed up like a DC; its admin logons come only from the PAW or jump host
WHY	It holds a credential to both directories. If passwords sync or either directory is the IdP for the other, one compromise is both, and this box is almost never treated as the Tier 0 asset it is. An agent that maps the domain values it above any single DC.
WHERE	Active Directory Users and Computers > move the computer object; the Tier 0 GPO; Phase 8 for the sync account itself
WHO CATCHES IT	GUERRILLA (Entra sync account hygiene) MANUAL (OU placement and GPO scope)

Watch out: Password hash sync to Google is a choice, not a default. If it is on, write down why; if nobody can, turn it off and let Google be the IdP for Chromebooks with its own second factor.

❑ Backup server off-domain, or Tier 0 with its own credentials

SET TO	Preferred: the backup server and repository are not domain members; local admin only, unique password in the password manager, MFA on the console. If it must be domain-joined: Tier 0 OU, deny-logon GPO for all non-Tier-0 admins, backup console admins are not Domain Admins, repository immutable (object lock) or offline-copied, alert on any job deletion or retention change
WHY	An attacker with DCSync has the backup service account. If the backup server is a domain member on the server VLAN with a writable repository, backups are deleted before encryption. Minneapolis recovered because theirs survived; most districts' would not.
WHERE	Backup console › users and roles; repository › immutability / retention lock; Phase 4 for the backup account
WHO CATCHES IT	MANUAL

Watch out: Immutability with a retention the admin can shorten is not immutability. Set the lock so that even the backup administrator cannot reduce it inside the window.

Egress and DNS from the server side

❑ Server and management VLANs: outbound deny-by-default

SET TO	Firewall policy for DC, server, hypervisor, backup and management subnets: outbound denied except patching, licensing and named vendor FQDNs; no general web browsing from any server; the jump host and admin workstations follow the same rule
WHY	A domain controller has no business reaching the internet. An agent on a compromised server phones home to a legitimate AI API over HTTPS, which every filter allows and TLS hides. The only control that stops it is that the server cannot reach anything you did not name.
WHERE	Firewall › outbound policy per VLAN; allowlist by FQDN where the firewall supports it
WHO CATCHES IT	MANUAL

Watch out: WSUS/PDQ, AV signature updates, KMS, NTP and the certificate authority's CRL/OCSP endpoints all need explicit allows; log the denies for two weeks in monitor mode before enforcing so you find them.

☐ Alert on LLM-provider hostnames from server or management subnets

SET TO DNS query logging on the internal resolvers (Windows DNS analytic log or the resolver's query log) shipped to the SIEM; a rule that fires on any query from a server, hypervisor, backup or management IP for `api.anthropic.com`, `api.openai.com`, `generativelanguage.googleapis.com`, `bedrock*.amazonaws.com`, `api.x.ai`, `api.mistral.ai`, `api.together.xyz` and similar

WHY The command-and-control of an agent-driven intrusion is a model API. Staff workstations may legitimately reach these; a server never does. It is the single most specific detection for the agent thesis.

WHERE DNS Server > Event Viewer > Applications and Services > Microsoft > Windows > DNS-Server > Analytical (enable); Wazuh rule on the DNS log

WHO CATCHES IT **MANUAL**

Watch out: Keep the hostname list in the SIEM, not the firewall, and review it quarterly; new providers appear monthly.

☐ DNS-over-HTTPS blocked; internal DNS is the only resolver

SET TO Firewall blocks known DoH resolvers (Cloudflare, Google, Quad9, NextDNS and the browser-built-in lists) and outbound 853 (DoT); Chrome policy `DnsOverHttpsMode = off`; Windows policy Configure DNS over HTTPS (DoH) name resolution = Prohibit DoH; only the internal resolvers are reachable on 53

WHY DoH bypasses the filter and hides the query from the DNS log you just started alerting on. Blocking it on the network and in policy keeps every lookup visible.

WHERE Firewall > application control / URL category; Computer Configuration > Administrative Templates > Network > DNS Client; Chrome policy

WHO CATCHES IT **MANUAL**

Wired access and the devices that are not Windows

☐ 802.1X on wired classroom ports

SET TO	Wired ports authenticate with 802.1X (certificate or device auth via NPS/RADIUS); unknown devices land on a quarantine VLAN with internet only; MAC authentication bypass only for printers and IoT that cannot do 802.1X, each pinned to its own VLAN; unused ports disabled; alert on a new MAC on a port that already has one
WHY	Guest wireless is segmented, but a device on a classroom jack gets the staff VLAN, which is the premise of the LLMNR item in Phase 2. A parent's laptop at a basketball game or a \$30 implant left behind maps what the port lets it see.
WHERE	Switch port config; NPS network policy; DHCP scopes for the quarantine VLAN
WHO CATCHES IT	MANUAL

Watch out: Start with the ports in public-facing rooms (gym, library, cafeteria, front office); classroom ports in locked rooms can follow.

☐ Copier and MFP credentials: dedicated, low-privilege, LDAPS only

SET TO	Scan-to-folder and LDAP address lookup use one dedicated account per fleet (<code>svc-mfp-scan</code>), member of Domain Users only, denied interactive and remote logon, password in the password manager; LDAP lookup over LDAPS (636) to a DC; SMB scan target is a share only that account can write; every MFP admin password changed from default and the web console on the printer VLAN only
WHY	An MFP stores an AD credential and will hand it to any host that answers as the LDAP or SMB server it was pointed at (the pass-back attack). A real domain-user credential in a copier is the first thing an automated sweep finds, and ThreatLocker never sees a copier.
WHERE	Each MFP's admin console > Network > LDAP / Scan settings; the <code>svc-mfp-scan</code> account's logon rights via GPO deny-logon lists
WHO CATCHES IT	MANUAL (GUERRILLA for the account's group membership and logon rights)

Watch out: Some older MFPs can only do plain LDAP on 389. If LDAP signing is enforced on the DCs (Phase 2) they will stop looking up addresses; that is the correct outcome. Replace or isolate the device rather than relax signing.

❑ Vendor remote-access tools on OT/IoT inventoried and gated

SET TO	A written list of every vendor remote tool reaching HVAC, cameras, door controllers, bell systems and the SIS (ScreenConnect, AnyDesk, TeamViewer, vendor VPN appliances); each reachable only from the vendor's known IPs through a firewall rule that is time-boxed and logged; the devices themselves on their own VLANs with no route to server subnets
WHY	These are standing remote-control paths into your building that no Windows control sees. The vendor's security is yours.
WHERE	Firewall > inbound rules per vendor; VLAN assignments; the inventory in the password manager or CMDB
WHO CATCHES IT	MANUAL

Finding the agent after it is in

❑ Weekly baseline diff of users, groups and ACLs

SET TO	A scheduled script exports users (created, enabled, lastLogon, adminCount), membership of every privileged group, domain and OU ACEs (Adeleg), GPO links and trusts to a dated folder on the admin host; diffs against last week; mails the delta; any new account, new privileged member or new ACE on a Tier 0 object is reviewed the same day
WHY	A documented post-access step for an automated intrusion is creating its own account for persistence. You already diff mailbox filters weekly in Workspace; the directory deserves the same. The monthly PingCastle diff in Phase 10 is too slow for this.
WHERE	Scheduled task on the admin host; Get-ADUser , Get-ADGroupMember , Adeleg export, Get-GPO ; Recipe R13 for the DCSync-rights ACE check
WHO CATCHES IT	MANUAL (BLOODHOUND for the quarterly graph diff)

Watch out: Diff the shortest paths to Domain Admins in BloodHound CE quarterly as well. PingCastle and Purple Knight score configuration; BloodHound walks the exact privilege graph an agent walks.

□ Honeytokens in the places an agent looks first

SET TO	A decoy service account with an SPN and a 25-character password that is never used (alert on any 4769 for it); a <code>creds.csv</code> or <code>passwords.txt</code> with fake contents in the scripts share, with a SACL that logs 4663 on read; a canary document in a Drive folder and a canary AWS/API key in a config file, both from canarytokens.org; one decoy computer object with a plausible name and no real host
WHY	An agent enumerates everything, in order, at machine speed. A Kerberoast request for an account nobody uses, a read of a file nobody should open, or a canary key being tried are each a single event that is never legitimate. It is the cheapest high-signal control that exists against the agent thesis.
WHERE	Phase 9 audit policy (4769, 4663 with SACLs); Wazuh rules; canarytokens.org for the document and key tokens
WHO CATCHES IT	MANUAL

Watch out: Name the decoys plausibly and leave them alone; a decoy that is in a scanner's exclusion list or documented in a wiki is not a decoy. Tell only the people who would otherwise investigate the alert.

□ Respond in minutes: automated action on the never-legitimate rules

SET TO	Wazuh active response on a short list: disable the account on a DCSync 4662 from a non-DC subject, on a Kerberoast of the decoy SPN, on a privileged-group add outside change windows; ThreatLocker host isolation on a ringfence violation from an agent process; a documented un-do procedure and a second admin who can run it at 2 AM
WHY	Detection in minutes is only half the sentence. At 2 AM on a holiday, an alert with no action is an audit log. The honest counter to machine speed is machine-speed response on the handful of rules that are never legitimate.
WHERE	Wazuh > active-response configuration; ThreatLocker > Detect policies > Isolate; the IR runbook
WHO CATCHES IT	MANUAL

Watch out: Test each automated action against a lab account first and write down what it breaks. An action that disables the sync account at 7 AM on a false positive is an outage you caused.

The procedure the vishing simulation tests

☐ Help-desk verification procedure for resets and MFA changes

SET TO	Written and rehearsed: no password reset, unlock, MFA reset or security-key enrollment for admin, finance, HR or central-office accounts by phone or chat, ever; for everyone else, callback to the number on file or a shared verification word; every reset logged with the method used and reviewed weekly against 4723/4724 and the Entra/Google reset logs
WHY	80% of a K-12 help desk's day is resets and unlocks; that is the call an attacker, or an agent with a cloned voice, makes. Trained listeners cannot tell modern clones from real voices; a procedure that does not depend on recognizing a voice is the only one that survives that.
WHERE	Written procedure; help-desk ticket template with a required verification method field; the vishing simulation grades the procedure, not the person
WHO CATCHES IT	MANUAL

Recovery you have actually rehearsed

☐ Post-compromise credential rotation runbook

SET TO	A written, ordered runbook: krbtgt twice (Recipe), every gMSA and service account, the sync account and its keys, every stored task and service password, LAPS passwords, AD CS CA key if the CA was reachable, every OAuth token and app password in Workspace and Entra, re-enrol security keys for admins, rotate the break-glass accounts; owners and estimated hours per step
WHY	After a confirmed compromise, every credential the attacker could have read is burned. That is days of work; with no runbook it is weeks of exposure while someone works out the order.
WHERE	The runbook lives printed in the break-glass envelope and in the password manager
WHO CATCHES IT	N/A

❑ Tested AD forest recovery with a measured RTO

SET TO	Annually: restore one DC from the Tier 0 backup into an isolated lab network, seize FSMO roles, reset krbtgt and the DSRM password, confirm authentication works, time it; document the steps that failed; keep the DSRM passwords and the isolated-network procedure in the break-glass envelope
WHY	A restore you have never run is a hope. Forest recovery has a dozen steps that are only obvious after you have done them once, and the first time should not be the real one.
WHERE	Backup console › restore to isolated network; Microsoft's AD Forest Recovery Guide for the sequence
WHO CATCHES IT	N/A

Watch out: Hypervisor snapshots are not backups and reverting a DC from one without VM-GenerationID support causes USN rollback; test from the backup product, not from a snapshot.

Gate: sync and backup servers in the Tier 0 OU or off-domain; server VLAN egress in enforce mode with the deny log reviewed; one honeypot of each kind placed and its alert tested; the baseline diff has run for four weeks; the verification procedure is written and the help desk has been tested against it; the rotation runbook is printed; one forest-recovery rehearsal timed.

Phase 10: Keep it that way

☐ Monthly: PingCastle and Guerrilla, diffed against last month

WHY Catches drift. The PingCastle score going up by 15 means someone re-added a vendor to Domain Admins; a Guerrilla check flipping from PASS to FAIL names the control. Keep both outputs; the diff is the report.

WHERE Scheduled task on the admin host; keep PingCastle's XML and Guerrilla's JSON

☐ Monthly, after Patch Tuesday: Tier 0 build numbers

WHY Confirms the Phase 4 update policy is still working.

WHERE Recipe R1 patch block

☐ Weekly: DC VM backup and system-state job both succeeded, and the export job's log has no errors

WHY A backup task that fails in one second is indistinguishable from one that ran, unless someone reads the log. The system-state job is the one that stops silently.

WHERE Backup console job history; `wbadmin get versions` ; export log; Recipe R8

☐ Weekly: staging OU emptied, new long host names given SPNs

WHY Every new join lands in staging with no policy; every new 16-character name is unmanageable by protected admins.

WHERE ADUC; Recipe R10

☐ Quarterly: admin group membership, local Administrators on Tier 0, DCSync ACEs, Protected Users membership

WHY The four lists that turn a stolen password into a domain.

WHERE Recipe R1 and R13

☐ Quarterly: ADeleg export diffed; ScriptSentry run; Locksmith if a CA exists

WHY Delegations accumulate one ticket at a time and nobody removes them; logon scripts get edited by hand; certificate templates get duplicated for a project and never locked down. Each tool answers one of those in minutes.

WHERE `adeleg.exe --csv <file>` (diff against last quarter); `Invoke-ScriptSentry` ; `Invoke-Locksmith -Mode 1`

☐ Quarterly: stored-credential tasks and services sweep

WHY Someone will schedule a report as themselves again.

WHERE Recipe R1

☐ Quarterly: stale users, stale computers, pwdLastSet=0, expiring vendor accounts

WHY Hygiene decays at the rate people are hired and devices are replaced.

WHERE Phase 7 queries

☐ Quarterly: RSOP user rights on a DC, a server and a workstation; Enforced link list

WHY GPO edits for one problem add rights for everyone.

WHERE Phase 0

☐ Semi-annually: krbtgt double reset; Seamless SSO key roll if applicable (monthly for the SSO key)

WHERE Phase 1, Phase 8

☐ Annually: restore test (one GPO from backup, one deleted user from the Recycle Bin, one DC from system state into an isolated network)

WHY A backup that has never been restored is a hypothesis.

- ❑ After every incident or outage: write down which of the above would have caught it earlier, and add that check

Recipes

R1: Inventory pass

```
# Effective user rights (run on each DC, one hypervisor, one server, one workstation)
Get-CimInstance -Namespace root\rsop\computer RSOP_UserPrivilegeRight |
    Select-Object UserRight, AccountList, GPOID | Sort-Object UserRight

# Domain-root and Enforced links
Get-GPInheritance -Target (Get-ADDomain).DistinguishedName | Select-Object -Expand
GpoLinks
Get-GPO -All | % { $r=[xml](Get-GPOReport $_.Id -ReportType Xml); $r.GPO.LinksTo | ?
NoOverride -eq 'true' | Select @{n='GPO';e={$r.GPO.Name}},SOMName }

# Privileged group membership with password age
foreach ($g in 'Domain Admins','Enterprise Admins','Schema Admins','Administrators',
    'Group Policy Creator Owners','Account Operators','Server Operators',
    'Backup Operators','Print Operators','DnsAdmins','Protected Users') {
    Get-ADGroupMember $g -Recursive -ErrorAction SilentlyContinue | Get-ADUser -Properties
    PasswordLastSet,LastLogonDate,Enabled,Description,adminCount |
        Select-Object @{n='Group';e=
    {$g}},SamAccountName,Enabled,PasswordLastSet,LastLogonDate,adminCount,Description
}

# Local Administrators, stored-credential tasks, domain-account services, patch level on
every server
$servers = (Get-ADComputer -Filter {OperatingSystem -like '*Server*' -and Enabled -eq
$true}).DNSHostName
Invoke-Command -ComputerName $servers -ErrorAction Continue {
    [pscustomobject]@{
        Host      = $env:COMPUTERNAME
        Admins     = (Get-LocalGroupMember Administrators).Name -join ';'
        Tasks      = (Get-ScheduledTask | ? { $_.Principal.LogonType -eq 'Password' -and
        $_.Principal.UserId -match '\\\' } |
            % { "$($_.TaskName)=$($_.Principal.UserId)" }) -join ';'
        Services  = (Get-CimInstance Win32_Service | ? StartName -match '^(?!LocalSystem|NT
        AUTHORITY|NT SERVICE|$)' |
            % { "$($_.Name)=$($_.StartName)" }) -join ';'
        Build      = (Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows
        NT\CurrentVersion').CurrentBuild + '.' +
            (Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows
        NT\CurrentVersion').UBR
        AU         = (Get-ItemProperty
        'HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU' -ErrorAction
        SilentlyContinue).AUOptions
    }
}
```

```

} | Export-Csv servers-inventory.csv -NoTypeInfoation

# Default containers
Get-ADComputer -SearchBase "CN=Computers,$((Get-ADDomain).DistinguishedName)" -Filter * -
Properties OperatingSystem,LastLogonDate
Get-ADUser -SearchBase "CN=Users,$((Get-ADDomain).DistinguishedName)" -Filter {Enabled -
eq $true} -Properties LastLogonDate

# SYSVOL / NETLOGON ACL and ownership, per DC
foreach ($dc in (Get-ADDomainController -Filter *).HostName) {
    icacls "\\$dc\SYSVOL\$env:USERDNSDOMAIN\scripts"
    Get-ChildItem "\\$dc\SYSVOL\$env:USERDNSDOMAIN\Policies" -Recurse | Get-Acl | Group-
Object Owner | Select Count,Name
}

# After removing an account from a protected group
Set-ADUser <sam> -Clear adminCount
$acl = Get-Acl "AD:\$((Get-ADUser <sam>).DistinguishedName)"
$acl.SetAccessRuleProtection($false, $true); Set-Acl "AD:\$((Get-ADUser
<sam>).DistinguishedName)" $acl

```

R2: Editing a GPO or SYSVOL directly (when the GroupPolicy module is unavailable or double-hops)

1. Back up: copy the GPO's SYSVOL folder and `Get-ADObject <gPC DN> -Properties *` to a dated folder.
2. Edit on the **PDC emulator**: `GptTmpl.inf` (UTF-16LE), `Registry.pol` (binary "PReg" format; use a proper writer), or GPP XML.
3. Bump `versionNumber` on the gPC object **and** in `GPT.INI` : +1 for a machine-side change, +65536 for a user-side change. Clients skip a GPO whose version did not change.
4. `repadmin /syncall <pdcc> <domain DN> /e /d /A /P` , then confirm the version and file contents on every other DC.
5. `gpupdate /target:computer /force` on a test machine; verify with RSOP (user rights) or `gpresult /h` .
6. For permission changes under SYSVOL: apply on each DC's UNC path and read back on each. Do not assume DFSR carried the ACL.
7. Deleting a GPO by hand: unlink from every `gPLink` , `Remove-ADObject -Recursive` on the gPC, then delete the SYSVOL folder on the PDC.

R3: Protected Users rollout

1. Inventory every use of each admin account (Recipe R1: tasks, services; plus application credential stores, RDP sessions via `query user /server:<host>`, 4768 source IPs via R13).
2. Move every task and service to a service account (R5). Give applications that authenticate over NTLM their own admin login. Give the backup product its own account.
3. Create the break-glass account (Before you start) and test it from the admin host.
4. Add **one** admin to Protected Users. Wait a day. Read the DC Security log for 4776 and 4625 with `0xC000006E` and 4771 with `0x18` for that account; each source host is something still using NTLM or an old password. Fix it (FQDN, SPN, service account, log off the stale session).
5. Repeat for each admin, including the built-in Administrator last.
6. Tell every admin: FQDN only; expect to re-authenticate every 4 hours in long sessions; never `klist purge`; a stale disconnected RDP session will generate pre-auth failures until it is logged off.
7. Set a disconnected-session time limit on servers (*Set time limit for disconnected sessions*, Remote Desktop Session Host > Session Time Limits) so stale sessions stop accumulating.

R4: Deny admin logon to workstations

1. New GPO, user configuration disabled. Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment: - *Deny log on locally*, *Deny log on through Remote Desktop Services*, *Deny log on as a batch job*, *Deny log on as a service* = Domain Admins, Enterprise Admins (add the `-adm` accounts' group if it is separate). - Leave *Deny access to this computer from the network* unset for these groups.
2. Link at the workstation OU only. Verify the link list does not include servers, DCs, or a parent of either.
3. Verify on one workstation (`RSOP_UserPrivilegeRight` shows four `SeDeny*` entries), one server and one DC (none).
4. Give each admin a non-privileged account in the workstation-admin group for hands-on work at a PC.

R5: Service account for a scheduled task

```
# AD side
New-ADUser svc-<purpose> -Path "OU=Service Accounts,<domain DN>" -AccountPassword (Read-Host -AsSecureString) `
    -Enabled $true -PasswordNeverExpires $true -CannotChangePassword $true -
KerberosEncryptionType AES256
Set-ADUser svc-<purpose> -LogonWorkstations '<host>'
# Host side (elevated)
icacls C:\Scripts\<purpose> /grant "DOMAIN\svc-<purpose>:(OI)(CI)M"
# Grant "Log on as a batch job": secedit export, add the SID to SeBatchLogonRight,
secedit import; or Local Security Policy GUI
# Task: Register-ScheduledTask ... -User DOMAIN\svc-<purpose> -Password <pw> (LogonType
Password)
```

Prefer a gMSA where the task is PowerShell or a service that supports it. Once per forest, a KDS root key must exist (`Add-KdsRootKey`). Then `New-ADServiceAccount gmsa-<purpose> -DNSHostName gmsa-<purpose>.<domain> -PrincipalsAllowedToRetrieveManagedPassword <host>$` (name 15 characters or fewer; `-DNSHostName` is the gMSA's own name, not the host's); grant it *Log on as a batch job* on the host; `Install-ADServiceAccount` on the host; task principal `DOMAIN\gmsa-<purpose>$` with no password.

R6: Windows LAPS

1. On the schema master, as a member of Schema Admins (add yourself, get a fresh ticket by signing out and in, remove yourself afterwards): `Update-LapsADSchema` .
2. `Set-LapsADComputerSelfPermission -Identity "OU=Workstations,<domain DN>"` and the same for the server OU.
3. GPO (Computer Configuration > Administrative Templates > System > LAPS): *Configure password backup directory* = Active Directory; *Password Settings* = complexity 4, length 24, age 30; *Post-authentication actions* = Reset the password and log off the managed account, 24 hours; *Enable password encryption* = Enabled (2016 DFL+); *Configure authorized password decryptors* = Domain Admins or the helpdesk group.
4. Link to the pilot OU; `gpupdate` ; `Get-LapsADPassword <computer> -AsPlainText` from the admin host.
5. Delegate `Get-LapsADPassword` read to the helpdesk group with `Set-LapsADReadPasswordPermission` . With encryption on, the helpdesk must also be the authorized decryptor, which takes a single principal: use one group that holds both Domain Admins and the helpdesk.

R7: Point and Print, done in the right order

1. On the print server: `Get-PrinterDriver | Select Name, Manufacturer` and the driver package paths (`Get-PrinterDriver | Select InfPath`).
2. Push the packages to every PC in machine context: `pnputil /add-driver <inf> /install` then `Add-PrinterDriver -Name "<exact model name>"` for each name in step 1, via the endpoint tool or a SYSTEM startup task. Verify `Get-PrinterDriver` on a sample of PCs lists every name.
3. GPO: *Package Point and print - Approved servers* = print server FQDN; *Point and Print Restrictions* = Enabled, users can only point and print to these servers, *When installing drivers for a new connection* = Do not show warning or elevation prompt is **removed**, i.e. `NoWarningNoElevationOnInstall=0` , `UpdatePromptSettings=0` ; *Limits print driver installation to Administrators* = Enabled (`RestrictDriverInstallationToAdministrators=1`).
4. Link to one building OU for one week. Watch for "Printer driver software installation" UAC prompts and *Group Policy Printers* errors in the Application log.
5. Roll out. Keep a rollback copy of the GPO.
6. Independently (no user impact): *Allow Print Spooler to accept client connections* = Disabled on workstations and servers with a Deny-Apply ACE for the print server; spooler disabled on DCs, hypervisors and non-printing servers.

R8: DC backups

Tier 1: VM-level (the one you will restore from). 1. In the backup product, the DC VMs get application-aware (VSS) processing so the directory database is quiesced; verify the job log shows the VSS writer for NTDS succeeded. 2. Repository: immutable (object lock) or an offline/air-gapped copy; the backup service account is `svc-backup`, never a human admin (Phase 4). 3. Restore test annually into an isolated network. Never revert a DC VM to a hypervisor checkpoint.

Tier 2: system state (the authoritative-restore path). 4. On one DC (the PDC is fine): scheduled task as SYSTEM, `wbadmin start systemstatebackup -backupTarget:\\<tier0 share> -quiet`, weekly. Share and NTFS: SYSTEM and Domain Admins only; the DC's computer account Modify. 5. Confirm its last-success date monthly (`wbadmin get versions`). This is the job that silently stops.

Tier 3: object-level exports (restore one thing without touching the DC). 6. Weekly script on the PDC as SYSTEM: `Backup-GPO -All -Path <stage>\GPO ; Get-GPOReport -All -ReportType Html ; ldifde -f <stage>\domain.ldf -d "<domain DN>" -p subtree`; CSV exports of users, groups, memberships, computers, OUs; `INVENTORY.txt` with FSMO roles, sites, subnets, trusts, password policy, DNS zones, counts; SHA-256 manifest; README with restore steps; robocopy to a Tier 0 share; prune older than 60 days. 7. Allow the script's hash in application control **before** the first run. Monday after: read the log, confirm the folder exists and is the expected size.

Optional and not generally advised: IFM. 8. `ntdsutil "activate instance ntds" ifm "create sysvol full <stage>" quit quit` produces a full ntds.dit plus SYSTEM/SECURITY hives: every hash, as files. Only take it if you have a stated forensic need (offline mount with `dsamain -dbpath <copy> -ldapport 51389`, which exists only on a DC or AD LDS server), keep it on a DC or an encrypted Tier 0 volume, and delete it on a schedule. It satisfies the scanners' backup-age rule, but so do tiers 1 and 2, so that is not a reason.

R9: Retiring student accounts (or any bulk delete) safely

1. List every system that reads the OU: Entra Connect (OU filter), GCDS (config), print management, library, cafeteria, LMS, RADIUS/NPS, any script. For each: does it delete, suspend or disable on sync? Neutralise or re-scope **before** deleting.
2. Confirm Google student accounts are provisioned from the SIS, not from AD.
3. Confirm no NPS/RADIUS server exists that authenticates Wi-Fi against student AD accounts.
4. Confirm the only GPOs linked to the student OU affect nothing else.
5. Export: every user (DN, GUID, memberOf, attributes) to CSV; every BitLocker key under every computer to be deleted; `Backup-GPO -All` ; a system-state backup (R8 tier 2).
6. Confirm the Recycle Bin is on and `msDS-DeletedObjectLifetime` (blank means it equals `tombstoneLifetime`) is 180 days.
7. Delete in batches with `Remove-ADObject -Recursive` from the PDC; keep the result CSV (DN, GUID, status).
8. Keep OUs and groups unless nothing references them; remove the GPO links that now apply to nothing.
9. Expect: ntds.dit does not shrink until an offline defrag; Entra shows a large delete if the scope included the objects; sync tools re-scoped in step 1 do nothing.

R10: SPNs for host names over 15 characters

```
Get-ADComputer -Filter {Enabled -eq $true} -Properties DNSHostName,ServicePrincipalName |
? { ($_.DNSHostName -split '\.')[0].Length -gt 15 } | % {
    $c    = $_
    $full = ($c.DNSHostName -split '\.')[0]
    $add  = @("HOST/$full","RestrictedKrbHost/$full") | ? { $c.ServicePrincipalName -
notcontains $_ }
    if ($add) { Set-ADComputer $c -ServicePrincipalNames @{Add=[string[]]$add} }
}
```

Safe to re-run. Add to the weekly staging-OU check, or cap names at 15 characters at imaging.

R11: Finding plaintext credentials in script and export folders

```
# Files whose first line looks like a header with a password column
Get-ChildItem C:\Scripts,C:\Tools,C:\Automation -Recurse -Include
*.csv,*.txt,*.text,*.log -ErrorAction SilentlyContinue |
? { (Get-Content $_.FullName -First 1 -ErrorAction SilentlyContinue) -match '(?
i)pass(word|wd)' } |
Select-Object FullName, Length, LastWriteTime
# Who can read the folder
icacls C:\Scripts
# Service-account keys, DPAPI blobs, private keys
Get-ChildItem C:\Scripts -Recurse -Include *.json,*.cred,*.ppk,*.pem,*.key,.env* | Select
FullName
```

For each hit: is it still produced? (If the producer is dead, delete the archive.) Who reads it? (ACL to that account only.) Can the producer stop writing the column? (Usually yes.)

R12: Helpdesk delegation groups

Helpdesk Password Reset	user objects under the staff OU	Extended right Reset Password; Write <code>pwdLastSet</code> , <code>lockoutTime</code> (and <code>pager</code> or whatever carries the badge number)	Same rights on the IT / admin / service-account OU
Helpdesk User Creation	staff OU and sub-OUs	CreateChild (user); GenericAll on descendant user objects	Both on the IT / admin / service-account OU
Helpdesk Computer Management	workstation OU	CreateChild + DeleteChild (computer); on descendant computers, Reset Password, validated writes to <code>dnsHostName</code> and SPN, and Write Account Restrictions (not GenericAll, which also exposes legacy LAPS passwords and RBCD)	Nothing on the server OUs or CN=Computers
Helpdesk Group Membership	the containers holding operational groups (printing, drive mapping, licensing)	Read + Write on the <code>member</code> attribute, <code>InheritedObjectType = group</code>	Explicit Deny on admin, delegation and infrastructure groups (AdminSDHolder-protected groups need none; SDProp resets their ACL hourly)

Apply with `Set-Acl` on an `AD:` drive pinned to one DC (`-Server`), then `repadmin /syncall` . Export each container's SDDL before and after. The technician signs out fully before testing; a reconnected session keeps the old token.

R13: DCSync rights and admin credential locations

```
# Who can replicate
$dn = (Get-ADDomain).DistinguishedName
(Get-Acl "AD:\$dn").Access | ? { $_.ObjectType -in '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2','1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' } |
    Select IdentityReference, ObjectType, AccessControlType
# AdminSDHolder write access (should be built-ins only)
(Get-Acl "AD:\CN=AdminSDHolder,CN=System,$dn").Access | ? { $_.ActiveDirectoryRights -match
'Write|GenericAll' } | Select IdentityReference,ActiveDirectoryRights

# Where admin passwords are typed (TGT requests by source IP), last 7 days, all DCs
$admins = (Get-ADGroupMember 'Domain Admins' -Recursive).SamAccountName
foreach ($dc in (Get-ADDomainController -Filter *).HostName) {
    Get-WinEvent -ComputerName $dc -FilterHashtable @{LogName='Security';Id=4768;StartTime=
(Get-Date).AddDays(-7)} |
        ? { $_.Properties[0].Value -in $admins } |
        Select @{n='User';e={$_.Properties[0].Value}}, @{n='IP';e={$_.Properties[9].Value}},
TimeCreated
} | Group User, IP | Select Count, Name

# NTLM refused by Protected Users (0xc000006E) by account and source
Get-WinEvent -FilterHashtable @{LogName='Security';Id=4776} -MaxEvents 5000 |
    ? { $_.Properties[-1].Value -eq '0xc000006e' } | Group { "$($_.Properties[1].Value) from
$($_.Properties[2].Value)" } | Select Count,Name
```

Gotchas: what breaks when you turn things on

CHANGE	WHAT BREAKS OR SURPRISES YOU	DO THIS FIRST
Protected Users (or any NTLM restriction)	RDP, SMB and WMI by IP fail (no SPN, NTLM fallback refused). DCOM to host names over 15 characters fails "Access is denied" (truncated SPN). 4-hour non-renewable TGT: long sessions lose every ticket. <code>klist purge</code> leaves the session with no tickets until lock/unlock or a fresh sign-in. Tasks running as the admin interactively fail overnight. Apps that validate logins over NTLM (print management web UI, some helpdesk tools) say "invalid password". Backup software with the admin's stored credential fails every job. Stale disconnected sessions log pre-auth failures every ~100 minutes.	FQDN everywhere; DNS records for every server; SPNs for long names (R10); tasks and services to service accounts (R5); app-specific admin logins; break-glass account outside the group; disconnected-session limit; one admin at a time (R3).
LmCompatibilityLevel=5	Copiers (scan-to-SMB), old NAS, some Linux Samba clients	Two weeks of 4624 <code>LmPackageName = NTLM V1</code> audit; do not test with a protected account
LDAP signing / channel binding	Firewall, VPN, wireless controller, copier and library LDAP binds in cleartext	Directory Service event 2889 audit; move each to LDAPS/636
SMB signing required on servers	SMB1-only scanners and copiers; some very old NAS	Replace the destination with SFTP/cloud drop or isolate
Kerberos AES only / RC4 removed	Old Macs, Linux boxes, appliances with RC4-only keytabs; service accounts without an AES key until their password is reset once	Watch 4769 <code>0x17</code> for a month; reset SPN account passwords after setting AES
Removing Authenticated Users from Pre-Windows 2000	Legacy NAS, RADIUS and LDAP browsers	Remove for a week on a test basis; have the rollback ready
Removing an account from an admin group	AdminSDHolder rule stays; account keeps protected ACL; helpdesk cannot reset its password	Clear <code>adminCount</code> , re-enable inheritance
Moving servers out of CN=Computers	Different GPOs apply (update policy, baseline); workstation GPOs stop (shutdown tasks, drive maps); helpdesk loses local admin and RDP	Review destination OU links; add helpdesk to Remote Desktop Users where needed
Deny admin logon to workstations	Admins cannot RDP or sign in to any staff PC	Non-privileged workstation-admin accounts; tell admins first; never link to server OUs
Authentication Policy Silo enforced	Every admin locked out at once if the computer list is wrong	Audit mode 2 to 4 weeks; break-glass outside the silo and tested
Kerberos armoring "fail unarmored"	Non-Windows clients and appliances cannot authenticate	Run in Supported mode first; leave fail-unarmored off
SYSVOL / NETLOGON ACL change	May not reach the other DC (replicated-folder root ACL, a broken DFSR, or a lagging DC)	Apply and read back on each DC
GPO edited directly in SYSVOL	Clients ignore it	Bump <code>versionNumber</code> in AD and GPT.INI (R2)
Redirecting new joins to a staging OU	Newly joined servers get workstation policy (shutdown task, Restricted Groups) until moved	Weekly staging-OU check; move servers at once
Point-and-Print restrictions on	District-wide UAC prompts for every printer the next morning; GPP printer items re-trigger it every refresh	Pre-stage every driver model as SYSTEM; pilot one building (R7)

CHANGE	WHAT BREAKS OR SURPRISES YOU	DO THIS FIRST
Spooler disabled on a server	Something on it printed (badge printer, label printer, report-to-PDF)	Check <code>Get-Printer</code> on the server first
AUOptions=4 on servers	Servers now reboot on the schedule; both DCs or both hypervisors on the same schedule reboot together	Stagger schedules; one DC and one host per window
Password change on an admin that runs a service	Service fails with 1069 at next restart, usually a weekend reboot	Move services off human accounts before the change
New export or backup task as SYSTEM on a DC	Application control blocks the script; "succeeded" in 1 second with exit 1	Allow the hash; read the log after the first run (R8)
IFM backup "for safety"	A second full copy of every password hash as plain files, usually on a server with helpdesk local admins	Prefer VM-level and system state; if IFM is truly needed, DC-only or encrypted, deleted on a schedule
Reverting a DC VM to a checkpoint	USN rollback: the DC silently stops replicating and nobody notices for weeks	Never checkpoint-revert a DC; restore from backup and verify <code>repadmin /showrepl</code>
Tightening the backup folder ACL	Your own non-elevated session can no longer read it; <code>icacls /reset /T</code> re-inherits the parent	Keep an explicit ACE for yourself; order the icacls steps (Phase 6)
Stale-computer sweep	Disables <code>AZUREADSSOACC</code> (breaks Seamless SSO) or the Entra Connect server; deletes BitLocker keys; list includes live machines	Exclude SSO and sync accounts; export <code>msFVE-RecoveryInformation</code> ; check LastLogon and 4768
Deleting student (or any bulk) AD accounts	A dormant directory-sync config suspends the matching Google accounts; print management or library deletes users; Entra deletes devices	R9 step 1: find and neutralise every sync first
Removing hybrid join	Already-joined PCs stay joined; Entra Connect still syncs computer objects	<code>dsregcmd /leave</code> ; change the connector scope
LAPS schema extension	Needs Schema Admins plus a fresh ticket; protected admins cannot <code>klist purge</code>	Sign out and in after adding yourself; remove yourself after
Bulk Google password reset keyed on <code>lastLoginTime</code>	Chromebook users were not locked out; now they are, and the device reports it days later	Use Reports API login events
Moving suspended Google users	OU-based licensing counts suspended users	Root-level Suspended Users OU
Application control on the admin host	DNS answers rewritten locally; "network is down" conclusions drawn from the wrong host; weekend lockdown policy blocks remediation	Test network problems from a second host; document the out-of-hours policy lift
15-character NetBIOS limit	Broken SPNs, broken secure channel, "clock is always wrong"	Naming standard; R10
Helpdesk delegation ACL added	Technician "still can't" until full sign-out	Sign out, not disconnect
Non-elevated admin session on a server	Cannot set owner, cannot grant logon rights, cannot read folders it just tightened	<code>Start-Process -Verb RunAs</code> for the elevated step
Disconnected-session time limit	Admins' long-running interactive jobs die when the session is reaped	Move long jobs to tasks under service accounts
Security log raised to 4 GB	Nothing; raising the size keeps the existing events (only shrinking needs a clear)	Raise it, don't shrink it

Rollout order

Pilot (one server, one building OU) › Tier 0 servers › remaining servers › workstation
OUs by building

Each step waits for the previous step's gate.

1. **Before you start** and **Phase 0** (read, back up, break-glass, baseline PingCastle). One day.
2. **Phase 3 user rights and SYSVOL ACLs, Phase 1 admin group cleanup, Phase 6 dead stored-password tasks**: under an hour each, zero user impact, each closes a critical path. Do these the same week.
3. **Phase 4 tiering**: redircmp, servers into OUs, local admins on Tier 0, Entra Connect cleanup, patch policy and a patch window.
4. **Phase 6** service accounts for everything that runs as a human.
5. **Phase 1 Protected Users**, one admin at a time, after step 4.
6. **Phase 1 deny-logon GPO** and separate `-adm` accounts.
7. **Phase 4 backups**: VM-level with application-aware processing, system state on a DC, exports; confirm two runs of each; delete any IFM job nobody can justify.
8. **Phase 5**: LAPS, spooler inbound block, firewall; Point-and-Print only after driver pre-staging.
9. **Phase 2** protocol hardening with its audit periods (NTLM, LDAP, SMB, RC4), copiers and appliances fixed as they surface.
10. **Phase 7** hygiene and **Phase 8** sync boundaries; student retirement if applicable.
11. **Phase 9** detection, in parallel from step 3 so the retests themselves show up in the logs.
12. **Phase 1 Authentication Silos** and **Phase 2 armoring**, audit mode first, last of all.
13. **Phase 10** on the calendar.

DCs vs. servers vs. workstations at a glance

	DOMAIN CONTROLLERS	TIER 0 / MEMBER SERVERS	WORKSTATIONS
Local Administrators	Domain Admins (implicit)	Domain Admins + one <code>svc-</code> where required	LAPS account + workstation-admin group
Who may log on interactively	Domain Admins from the admin host	Domain Admins from the admin host; <code>svc-</code> as batch/service only	Users; Domain Admins denied
Patch policy	Scheduled install, staggered	Scheduled install, staggered	Endpoint tool / scheduled install
Print Spooler	Disabled	Disabled unless it is the print server	Running, inbound connections blocked
SMB signing	Required	Required	Required
LDAP signing / CBT	Required / Always	n/a	n/a
NTLM	Audit then restrict; admins never (Protected Users)	Same	Same
RDP	NLA, admin host only	NLA, admin host and documented vendors	NLA + Remote Desktop Users, or off
Credential Guard / LSA PPL	LSA PPL	LSA PPL (+ CG where supported)	Both
Security log	4 GB, forwarded	1 GB, forwarded (Tier 0)	Default, local
Firewall	On; management from admin host	On; management from admin host	On; 135/445/5985 from admin host only
Time source	External NTP on the PDC; VM IC provider off	Domain hierarchy	Domain hierarchy
Backup	VM-level (application-aware, immutable repo) + system state weekly; GPO/LDIF exports; IFM only with a stated need	Per role	None (data lives elsewhere)
OU	Domain Controllers	Servers / Tier0	Workstations by building; staging for new joins

Group Policy paths and PingCastle rule names move between releases. If one is wrong, open an issue or PR.