Wk2

## 6  Future Patch Automation

# inside each new clone

Set-ExecutionPolicy RemoteSigned -Scope Process -Force

Install-PackageProvider NuGet -Force -Scope CurrentUser

Install-Module PSWindowsUpdate -Force -Scope CurrentUser

Import-Module PSWindowsUpdate

Get-WindowsUpdate -AcceptAll -Install -AutoReboot

Offline alternative: **WSUS Offline** or **WuPackage**; schedule monthly via Prefect (Week 15).

| **Layer** | **Hardening action** | **Exact command / setting** |
| --- | --- | --- |
| **1 Service integrity** | Lock service configuration so only Administrators can stop or reconfigure it. | powershell\n  sc.exe sdset SysmonDrv D:(A;;CCLCSWRPWPDTLOCRRC;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRC;;;SY)S:  \n  *(SY = SYSTEM full; BA = Built-in Admins full; everyone else = no control)* |
| **2 Executable integrity** | Set ACLs on Sysmon binaries and config so even Admins have *read-only* access during normal operation. | powershell\n  icacls \"C:\\Tools\\Sysmon\" /inheritance:r /grant:r \"SYSTEM:F\" \"Administrators:R\"  \n  # Break-write only when you intentionally update config  \n |
| **3 Config tamper alerts** | Tell Sysmon to log its own configuration changes to the Event Log. | The SwiftOnSecurity template already enables “Sysmon configuration change” (Event ID 16). Make sure you **forward ID 16** to ELK and alert on it. |
| **4 Centralised config control** | Keep the master sysmonconfig-gold.xml in your Git repo. Push updates via Ansible/WinRM and reload with Sysmon64.exe -c <file>. Never edit in-place on production hosts. |  |
| **5 Signed updates** | Get in the habit of verifying Microsoft’s SHA-256 and digital signature before replacing Sysmon64.exe. | powershell\nGet-FileHash Sysmon64.exe -Algorithm SHA256\nGet-AuthenticodeSignature Sysmon64.exe\n |
| **6 Event-log resilience** | Increase log size (you already did) **and** lock Security/EventLog ACLs so attackers can’t clear them. | powershell\nwevtutil sl \"Microsoft-Windows-Sysmon/Operational\" /ms:102400\nwevtutil sl Security /e:true\n# ACL lock via local policy → Security Options → Audit: Force audit policy subcategory settings\n |
| **7 Service recovery traps** | Configure service-recovery options to restart on failure and trigger a custom action. | powershell\nsc.exe failure SysmonDrv reset= 86400 actions= restart/60000\n |
| **8 AppLocker / WDAC** | Create a rule that **allows** the specific Sysmon path & hash, **denies** any other copy of Sysmon in %TEMP% or user folders. Blocks LOLBin-style replacements. | Add path + hash rules in AppLocker’s *Executable Rules* or WDAC policy. |
| **9 Defender Attack-Surface Reduction** | Enable the ASR rule “Block abuse of exploited vulnerable signed drivers” | Set-MpPreference -AttackSurfaceReductionRules\_Ids 56a863a9-875e-4185-98a7-b882c64b5ce5 -AttackSurfaceReductionRules\_Actions Enabled |
| **10 Continuous monitoring** | Alert if Event ID 255 (Sysmon service stopped) or if Sysmon event flow ceases for >N minutes in Grafana. | Prometheus exporter already collects event counts → set a *dead-man* alert. |

| **Task** | **Concrete actions** |
| --- | --- |
| **4 Git repo tasks** | Pre-commit hooks → .pre-commit-config.yamlCI skeleton → .github/workflows/ci.ymlgit add + commit + push. |
| **5 SICP 1.15 – 1.29** | Create sicp/ch1\_partB.scm, push after tests pass. |

### What goes into Git this week

docs/

└── auditpol\_backup\_benign-ws01\_2025-06-02.csv # tiny

.github/

└── workflows/ci.yml

.pre-commit-config.yaml

sicp/ch1\_partB.scm

Large VM disks stay in *vms/* (git-ignored).