Southern Mutual Bank

PowerShell and Process Creation Auditing Configuration Export — Windows Fleet

configuration export · settings read from the system of record · synthetic assessor-grade test document

Export ID	SOU-EXP-1240
System	Windows Fleet
Exported by	Mei-Lin Tan (IT Operations Manager)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A configuration export for Windows Fleet: the current settings as held by the system, section by section, with the compliance status against the applicable baseline. It reports state; it does not describe intent. Settings shown as non-compliant carry a remediation ticket.

2. Process creation and command-line logging

Setting	Value	Status
Audit process creation	On — success events on 1,244 workstations and 212 servers	Compliant
Include command line in process creation events	On	Compliant
Central collection	Forwarded to the SIEM; retention 12 months; 1,456 of 1,456 hosts reporting	Compliant

3. PowerShell

Setting	Value	Status
PowerShell script block logging	On — all hosts; events forwarded to the SIEM	Compliant
PowerShell module logging and transcription	On — transcripts written to a protected share	Compliant
PowerShell 2.0	Removed from all workstations and servers	Compliant
PowerShell language mode	Constrained language mode for non-administrators, enforced by application control	Compliant

4. Application hardening

Setting	Value	Status
.NET Framework 3.5 (includes .NET 2.0 and 3.0)	Removed from workstations and servers	Compliant
Microsoft Office — child processes, OLE package activation, content injection	Blocked by attack surface reduction rules	Compliant
PDF software — JavaScript and child process creation	Blocked by policy	Compliant
Vulnerable driver blocklist	Applied — Microsoft vulnerable driver blocklist in force	Compliant

Setting	Value	Status
Blocked events logged	Attack surface reduction and PowerShell blocks logged and forwarded to the SIEM	Compliant

5. Monitoring

Setting	Value	Status
SIEM detections	Encoded PowerShell, suspicious parent-child process chains and blocked-driver load attempts alert the security operations centre	Compliant
Review of logs	Detections triaged each shift; 11 triaged in the last 30 days, none escalated	Compliant

6. Control framework mapping

Framework	Indicative mapped controls
Essential Eight	ML2 target
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2

Exported from the management console; integrity hash recorded in the evidence register. Reviewed by the control owner and second-line risk.