MARTELL CYBERTECH — DEVICE HARDENING ASSESSMENT

WindowsHardeningAssessment

DEMO-WIN-PC | 2026-05-12 08:14:49 | Windows 10.0.26200

38 TOTAL CHECKS

17 PASSED

16 FAILED

5 WARNINGS

Access Control 0/1 | Account Policy 2/5 | Antivirus 2/4 | Auditing 2/3 | Credential Protection 2/3 | Encryption 0/2 | Firewall 3/3 | Network 0/5 | PowerShell 1/3 | Remote Access 2/2 | System 1/3 | UAC 1/2 | Updates 1/2

CHECK RESULTS — SORTED BY SEVERITY & STATUS

16 REMEDIATIONS REQUIRED

CATEGORY	CHECK	SEVERITY	STATUS	DETAILS / REMEDIATION
Encryption	**BitLocker Drive Encryption**	CRITICAL	✗ FAIL	BitLocker on C: — Protection: OFF (drive unencrypted) **Remediation:** Enable BitLocker: Control Panel → BitLocker Drive Encryption → Turn On, or via Intune/GPO.
Network	**SMBv1 Disabled**	CRITICAL	✗ FAIL	SMBv1: ENABLED — legacy protocol, major attack surface (EternalBlue) **Remediation:** Disable: Set-SmbServerConfiguration -EnableSMB1Protocol $false, or via Windows Features.
Credential Protection	**LSA Protection Enabled (RunAsPPL)**	CRITICAL	✗ FAIL	LSA RunAsPPL = 0 (NOT protected) **Remediation:** Enable via: HKLM\SYSTEM\CurrentControlSet\Control\Lsa → RunAsPPL = 1, then reboot.
Encryption	**Secure Boot Enabled**	HIGH	✗ FAIL	Secure Boot: DISABLED **Remediation:** Enable Secure Boot in UEFI/BIOS firmware settings.
Antivirus	**Defender Tamper Protection**	HIGH	⚠ WARN	Could not determine Tamper Protection status: Get-MpPreference : Operation failed with the following error: 0x800106ba At line:1 char:2 + (Get-MpPreference).IsTamperProtected + ~~~~~~~~~~~~~~~~

				+ CategoryInfo : NotSpecified: (MSFT_MpPreference:root\Microsoft\...FT_MpPreference) [Get-MpPreference], CimException + FullyQualifiedErrorId : HRESULT 0x800106ba,Get-MpPreference **Remediation:** Enable via: Windows Security → Virus & threat protection settings → Tamper Protection ON.
UAC	**UAC Prompt on Secure Desktop**	HIGH	✗ FAIL	UAC prompt level = 5: Prompt for consent **Remediation:** Set ConsentPromptBehaviorAdmin to 1 or 2 via GPO or registry.
Account Policy	**Minimum Password Length >= 14**	HIGH	✗ FAIL	Minimum password length: 0 (recommended >= 14) **Remediation:** Set via: Local Security Policy → Account Policies → Password Policy → Minimum password length.
Account Policy	**Account Lockout Policy Set**	HIGH	✗ FAIL	Account lockout: NEVER (no lockout policy set) **Remediation:** Set via: Local Security Policy → Account Policies → Account Lockout Policy → Lockout threshold (recommended: 5–10).
Network	**SMB Signing Required**	HIGH	✗ FAIL	SMB RequireSecuritySignature = 0 (NOT required — relay attack risk) **Remediation:** Enable via GPO: Network server: Digitally sign communications (always), or registry RequireSecuritySignature = 1.
Network	**LLMNR Disabled**	HIGH	✗ FAIL	LLMNR: policy key not found — LLMNR likely ENABLED (poisoning risk) **Remediation:** Disable via GPO: Computer Config → Admin Templates → Network → DNS Client → Turn off multicast name resolution = Enabled.
Updates	**Automatic Updates Configured**	HIGH	⚠ WARN	AUOptions key not found — check Windows Update settings manually **Remediation:** Set Windows Update to auto-download and install (AUOptions = 3 or 4) via Settings or GPO.
Account Policy	**Built-in Administrator Renamed**	MEDIUM	✗ FAIL	Built-in admin account name: 'Administrator' (NOT renamed — default name in use) **Remediation:** Rename via GPO: Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → Accounts: Rename administrator account.
Network	**NetBIOS Disabled**	MEDIUM	✗ FAIL	NetBIOS: Adapter 0: Default/DHCP, Adapter 1: Default/DHCP **Remediation:** Disable via NIC properties → TCP/IP Properties → Advanced → WINS → Disable NetBIOS over TCP/IP.
Network	**WPAD Auto-Detect Disabled**	MEDIUM	✗ FAIL	WPAD: no machine policy found and WpadOverride not set — auto-detect proxy may be enabled (WPAD attack risk) **Remediation:** Disable WPAD via IE/Edge settings or set WpadOverride = 1 in registry.
PowerShell	**PowerShell Script Block Logging**	MEDIUM	✗ FAIL	Script Block Logging: NOT configured (key absent) **Remediation:** Enable via GPO: Computer Config → Admin Templates → Windows Components → Windows PowerShell → Turn on PowerShell Script Block Logging.
Auditing	**Security Event Log >= 32 MB**	MEDIUM	✗ FAIL	Security event log max size: 20 MB (recommended >= 32 MB) **Remediation:** Set via: Event Viewer → Windows Logs → Security → Properties → Maximum log size.

System	**Screensaver Password Lock**	MEDIUM	✗ FAIL	ScreenSaverIsSecure not set — screensaver may not require password **Remediation:** Enable via: Screen Saver Settings → 'On resume, display logon screen'.
System	**AppLocker / Application Control Configured**	MEDIUM	⚠ WARN	AppLocker not configured or could not be read **Remediation:** Configure AppLocker via GPO or use Windows Defender Application Control (WDAC).
Antivirus	**Microsoft Defender for Endpoint (ATP) Running**	MEDIUM	⚠ WARN	Microsoft Defender for Endpoint not detected (may not be licensed) **Remediation:** Ensure Microsoft Defender for Endpoint is licensed and the Sense service is running.
PowerShell	**PowerShell Transcription Enabled**	LOW	✗ FAIL	PowerShell Transcription: NOT configured **Remediation:** Enable via GPO: Windows PowerShell → Turn on PowerShell Transcription.
Access Control	**Windows Hello Policy Configured**	LOW	⚠ WARN	Windows Hello policy not configured (check manually) **Remediation:** Enable Windows Hello via GPO: Computer Config → Admin Templates → Windows Components → Windows Hello for Business.
Antivirus	**Windows Defender Real-Time Protection**	CRITICAL	✓ PASS	DisableRealtimeMonitoring key not present — real-time protection enabled (default)
Firewall	**Windows Firewall — Public Profile**	CRITICAL	✓ PASS	Public Firewall: ON (EnableFirewall = 1)
UAC	**User Account Control (UAC) Enabled**	CRITICAL	✓ PASS	UAC EnableLUA = 1 (enabled)
Credential Protection	**WDigest Authentication Disabled**	CRITICAL	✓ PASS	WDigest UseLogonCredential not set — disabled by default (Win8.1+)
Firewall	**Windows Firewall — Domain Profile**	HIGH	✓ PASS	Domain Firewall: ON (EnableFirewall = 1)
Firewall	**Windows Firewall — Private Profile**	HIGH	✓ PASS	Private Firewall: ON (EnableFirewall = 1)
Account Policy	**Guest Account Disabled**	HIGH	✓ PASS	Guest account: Disabled
Remote Access	**Remote Desktop (RDP) Disabled**	HIGH	✓ PASS	RDP fDenyTSConnections = 1 (RDP disabled)
Remote Access	**RDP Requires Network Level Authentication**	HIGH	✓ PASS	RDP NLA (UserAuthentication) = 1 (required)
Credential Protection	**Credential Guard Enabled**	HIGH	✓ PASS	Credential Guard SecurityServicesRunning: 2
Updates	**Automatic Updates Not Disabled by Policy**	HIGH	✓ PASS	NoAutoUpdate = 0 (updates allowed)
Auditing	**Logon Events Audited (Success & Failure)**	HIGH	✓ PASS	Logon auditing: System audit policy Category/Subcategory Setting Logon/Logoff

				Logon
Antivirus	**Defender Cloud Protection**	MEDIUM	✓ PASS	SpynetReporting = 2 (enabled)
Account Policy	**Maximum Password Age <= 90 Days**	MEDIUM	✓ PASS	Maximum password age: 42 days (recommended <= 90)
PowerShell	**PowerShell Execution Policy Restricted**	MEDIUM	✓ PASS	PowerShell ExecutionPolicy (LocalMachine) = RemoteSigned
Auditing	**Policy Change Audited**	MEDIUM	✓ PASS	Policy Change auditing: System audit policy Category/Subcategory Setting Policy Change Audit Policy Change
System	**AutoRun/AutoPlay Disabled**	MEDIUM	✓ PASS	NoDriveTypeAutoRun = 255 (all drives disabled)