Dukahn
Assess | Protect | Lead
www.cybersmithing.com

Essential Hardening Checklist

Operating System Hardening

- ❑ Remove bloatware and unused applications
- ❑ Enable automatic OS updates or centralized patching
- ❑ Configure host firewalls (Windows Firewall, ufw, iptables)
- ❑ Disable unnecessary default services (RDP, SMBv1, Telnet, FTP, etc.)

Application Hardening

- ❑ Patch all applications regularly
- ❑ Remove outdated or vulnerable software (e.g., old Java)
- ❑ Apply secure configuration guides (CIS benchmarks)
- ❑ Enforce application allowlisting (where possible)
- ❑ Enable automatic updates for browsers, PDF readers, etc.

Identity Hardening

- ❑ Enforce MFA across all systems
- ❑ Disable default accounts and rename admin accounts
- ❑ Restrict lateral movement (disable unnecessary local admin rights)
- ❑ Implement privileged access management (PAM)
- ❑ Enforce identity governance and lifecycle management

Network Hardening

- ❑ Disable unused network ports and protocols
- ❑ Enforce TLS 1.2+
- ❑ Use DNS filtering and secure DNS resolvers
- ❑ Implement network segmentation and micro-segmentation
- ❑ Deploy intrusion detection/prevention systems (IDS/IPS)

Cloud Security Hardening

- ❑ Enforce MFA and conditional access

- ❑ Monitor for misconfigurations (CSPM tools)
- ❑ Tighten IAM permissions—no wildcard * permissions
- ❑ Enable logging: CloudTrail, Azure Monitor, GCP Logging
- ❑ Set up alerting for unusual access patterns
- ❑ Encrypt all cloud storage buckets and block public access by default

Endpoint Hardening

- ❑ Enforce screen lock & inactivity timeouts
- ❑ Enable full disk encryption
- ❑ Disable local admin for standard users
- ❑ Harden BIOS/UEFI with a password
- ❑ Disable booting from external media

Logging & Monitoring Hardening

- ❑ Enable detailed audit logs systemwide
- ❑ Forward logs to a centralized SIEM
- ❑ Establish alert thresholds and triage workflows
- ❑ Monitor for brute-force attempts and privilege escalation
- ❑ Validate logging cannot be disabled by standard users

Email & Web Security Hardening

- ❑ Deploy anti-phishing protection
- ❑ Enable DMARC, SPF, and DKIM for domains
- ❑ Block macro-enabled Office docs by default
- ❑ Enable safe links and safe attachments
- ❑ Filter high-risk file types (EXE, JS, VBS, MSI)

Signature: _____

Name: _____

Date: _____