Security and Financial Assessment – DSM-MEMBER-SRV

Author: Joseph Knight
Date: 2025-12-30
System: DSM-MEMBER-SRV (Des Moines) – Windows Server 2025
Role: Tier 1/2 Member Server handling PII/PHI

Key Findings

- **Initial Drift:** 7 STIG deviations identified
  - High: 3
  - Medium: 4
- **Non-Compliant Areas:** Weak password policies, disabled auditing, unauthorized admin account
- **Post-Remediation:** 100% of drift corrected, auditing restored, unauthorized accounts removed
- **Daily Monitoring:** Automated script detects any future drift within 24 hours

---

Conclusion

Enforcing STIG controls ensures robust security standards, directly supporting VA and government business requirements. The lab demonstrates that **STIG enforcement significantly reduces risk**, corrects high-severity deviations, and provides measurable compliance metrics:

- **Compliance improvement:** 71% → 100%
- **High-risk findings resolved:** 100%
- **Detection latency for drift:** < 24 hours

Bottom line: The reward of maintaining STIG-aligned servers is clear — regulatory compliance, reduced risk, and readiness for government contracts.

Financial Security Assessment

- **Sensitive Data at Risk:** PII/PHI storage fully secured after remediation
- **Potential Impact if Compromised:** High — exposure of financial or health data could trigger regulatory penalties
- **Remediation Effectiveness:** 100% of identified vulnerabilities corrected
- **Ongoing Monitoring:** Automated daily checks ensure early detection of unauthorized changes, minimizing risk to financial and client data
- **Assessment Conclusion:** Maintaining STIG compliance directly protects sensitive financial and personal data, ensuring the organization meets government and regulatory security expectations