Windows 11 v24H2 Security Baseline Gap Analysis Report

Prepared by: Michael Olayiwola

Date: February 2026

1. Executive Summary

This report presents the findings of a security gap analysis conducted on a Windows 11 v24H2 host system. The analysis compared the current system configuration against Microsoft's recommended Windows 11 Security Baseline using the Microsoft Security Compliance Toolkit and Policy Analyzer tool. The objective was to identify misconfigurations, assess associated risks, and recommend remediation steps to improve system hardening and reduce attack surface exposure.

2. Scope and Objectives

Scope: Local host configuration assessment only. No network-wide or domain-level policies were evaluated.

- Compare current system security settings against Microsoft Windows 11 Security Baseline.
- Identify configuration deviations (gaps).
- Assess potential security risks associated with deviations.
- Provide remediation recommendations.

3. Tools Used

- Windows 11 v24H2 Operating System
- Microsoft Security Compliance Toolkit
- Policy Analyzer
- Windows 11 Security Baseline Package

4. Key Findings

- Password minimum length set to 0 (Baseline recommendation: 14 characters).
- Password complexity disabled (Baseline recommendation: Enabled).
- Password history not enforced (Baseline recommendation: 24 previous passwords remembered).
- Certain service configurations deviated from baseline recommendations.
- Account lockout threshold validated and aligned with baseline.

5. Risk Analysis

Weak password policies significantly increase the risk of brute-force attacks, credential stuffing, and unauthorized access. Lack of password complexity and history enforcement enables attackers to reuse previously compromised credentials. Configuration drift from security baselines increases system exposure and weakens defense-in-depth strategy.

6. Remediation Recommendations

- Set minimum password length to 14 characters or higher.
- Enable password complexity requirements.
- Enforce password history of at least 24 remembered passwords.
- Review and align service configurations with baseline recommendations.
- Periodically re-run baseline comparison to ensure continued compliance.

7. Conclusion

The gap analysis revealed critical deviations from Microsoft's recommended Windows 11 Security Baseline, primarily in password policy configurations. Implementing the recommended remediations will significantly improve system security posture and reduce the risk of unauthorized access. Regular baseline validation is essential to maintaining a hardened and resilient operating environment.