Essential Eight Configuration & Validation Report

Date: 06 Sep 2025

User ID/Session ID: Camille-Application-Control-Screenshot1-AC-01-03-04-02

1. Executive Summary

This EC&V scan analyses the evidence uploaded against the Essential 8 mitigation strategies.

It provides a maturity level estimate per detected strategy, recommendations for improvement, and an appendix of the original evidence for transparency.

Note: This is not a full audit. Results are based only on the uploaded evidence and may not reflect your complete security posture.

2. Definitions

Maturity Levels:
- ✓ **Level 0 (Initial)**: No or ad-hoc implementation
- ✓ **Level 1 (Baseline)**: All baseline criteria fully met
- ✓ **Level 2 (Maturity)**: Baseline + advanced criteria fully met
- ✓ **Level 3 (Target)**: Level 2 + continuous validation and automated enforcement

3. Detailed Findings & Recommendations

Summary Table:

Strategy	Test ID	Sub-Strategy	Detected Level	Target Level	Pass/Fail	Priority
Application Control	ML1-AC-03	Unauthorised Scripts must be blocked	Level 1	Level 3	Pass	High

Strategy: Application Control // **Test ID:** {Test_id} // **Sub-Strategy:** Unauthorised Scripts must be blocked

- **Description:**

- **Detected Maturity Level:** 1

- **Evidence Extract:**
  "script rules; re:\benforc(?:e|ed|ing)\b"

- **Recommendations:**

  (1) Ensure script files (SH, BASH, CSH, KSH, BAT, CMD, JS, VBS, PY, PS1, PL, PHP, SCPT, WSF, OSTS) cannot be run from user or temp folders by standard users (2) Use AppLocker or Windows Defender Application Control rules

4. Confidence & Limitations

OCR Match Confidence:

- Unauthorised Scripts must be blocked – %

Limitations:

- Evidence may be incomplete
- Some configurations require manual verification

5. Appendix – Uploaded Evidence

File: Screenshot1 AC-01 03 04.png

AppLocker Properties   x

1
Enforcement | Advanced

Specify whether AppLocker rules are enforced for each rule collection.

Executable rules:
☑ Configured

[Enforce rules   ▾]

Windows Installer rules:
☑ Configured

[Enforce rules   ▾]

Script rules:
☑ Configured

[Enforce rules   ▾]

Packaged app Rules:
☑ Configured

[Enforce rules   ▾]

More about rule enforcement

[OK]   [Cancel]   [Apply]