Red/Purple Team Report — Acme Pty Ltd — [CAMPAIGN]

Version: v1.0 · Date: 2025-02-15 · Confidential

Executive Summary

- Objective: [OBJECTIVE]
- Outcome: [OUTCOME]
- Business Impact: [IMPACT_SUMMARY]

Actions This Week

- [ ] [ACTION_1]
- [ ] [ACTION_2]
- [ ] [ACTION_3]

Rules of Engagement

- Threat Profile: [THREAT]
- ATT&CK focus: [ATTACK_TACTICS]
- Allowed Vectors: [VECTORS]
- Constraints: [CONSTRAINTS]

Campaign Timeline

- [TIME] — [EVENT]
- [TIME] — [EVENT]

Kill Chain Overview (MITRE ATT&CK)

Initial Access → Execution → Persistence → Priv Esc → Defense Evasion → Cred Access → Discovery → Lateral Movement → Collection → C2 → Exfil/Impact

Key Findings & Opportunities

- Detection Gaps: [GAPS]
- Response Gaps: [RESP_GAPS]

Detection Engineering Pack

- Rule: [RULE_NAME] — [RULE_SNIPPET_OR_LINK]
- Log Sources: [LOG_SOURCES]
- Tuning Notes: [TUNING]

Purple Team Outcomes (if run)

- Exercises: [EXERCISES]
- Capability Gains: [GAINS]

Technical Evidence

- Payload hashes, IOCs, transcripts, screenshots

Remediation & Roadmap

- 30/60/90-day Plan: [PLAN]

Sign-off & Appendix

- Tools/infrastructure used, legal/ethics, glossary