Red Team / Blue Team Readiness Checklist

Organisational Visibility

1. ☐ We know our exposed internet-facing assets.
2. ☐ We regularly review privileged account usage.
3. ☐ We monitor unusual login geography or timing.
4. ☐ We can identify suspicious cloud download behaviour.

Human Verification

5. ☐ Employees are trained to verify urgent requests.
6. ☐ Finance verifies vendor payment changes.
7. ☐ Helpdesk has strong password reset validation.
8. ☐ MFA prompts are treated carefully by users.

Red Team Thinking

9. ☐ We periodically ask how an attacker would enter.
10. ☐ We simulate phishing or impersonation attempts.
11. ☐ We pressure-test internal approval workflows.
12. ☐ We review vendor trust assumptions.

Blue Team Thinking

13. ☐ We have documented escalation procedures.
14. ☐ We can disable compromised accounts quickly.
15. ☐ We review suspicious mailbox forwarding or rules.
16. ☐ We preserve useful logs for investigation.

Purple Team Learning

17. ☐ We document lessons from every simulation.
18. ☐ We tune controls after identified failures.
19. ☐ We review whether alerts actually surfaced anomalies.
20. ☐ We involve leadership in resilience discussions.

Security Culture

21. ☐ Staff know how to report suspicious activity quickly.
22. ☐ Verification is encouraged over blind speed.
23. ☐ Managers reinforce cyber caution.

24. ☐ Security is discussed outside IT.
25. ☐ We treat cybersecurity as continuous readiness.

SCORING RESULTS

Strong Tactical Readiness (20–25 Checked)

Your organisation is developing meaningful adversarial resilience and tested defensive maturity.

Moderate Defensive Maturity (12–19 Checked)

You have useful controls, but several assumptions remain under-tested.

Reactive Security Exposure (0–11 Checked)

Your organisation is relying too heavily on static controls without enough practical resistance rehearsal.