THE PERIMETER EXPOSURE AUDIT

Proactive Vulnerability Identification & Threat Modeling

This document serves as a high-level diagnostic framework designed by **Quantum Xybernetics** to evaluate organizational resilience against common attack vectors.

Modern threats bypass traditional firewalls. Security today is defined by identity, patch velocity, and human vigilance.

IDENTITY & ACCESS MANAGEMENT (IAM)

- [ ] Is multi-factor authentication (MFA) enforced across all external-facing ingress points?
- [ ] Are privileged account credentials rotated monthly and stored in an encrypted vault?
- [ ] Do you perform quarterly user-access reviews to prune "ghost" accounts?

INFRASTRUCTURE & PERIMETER DEFENSE

- [ ] Is the mean time to remediate (MTTR) critical vulnerabilities under 72 hours?
- [ ] Are backups protected by immutable snapshots or physical air-gaps?
- [ ] Do you have visibility into all unmanaged devices (Shadow IT) on your network?

INCIDENT RESPONSE & HUMAN FACTOR

- [ ] Has your Incident Response plan been validated through a tabletop exercise this year?
- [ ] Do employees receive role-specific security awareness training (e.g., Finance vs Dev)?

RISK PROFILE BENCHMARKING

01 **OPTIMAL (7-8 SCORE)**
High maturity. Focus should shift to advanced behavioral analytics and Red Team adversary emulation.

02 **DEGRADED (4-6 SCORE)**
Structural weaknesses present. Attackers likely have multiple paths to escalate privileges within your domain.

03 **EXPOSED (0-3 SCORE)**
Critical failure points. Immediate intervention required to establish basic perimeter control and visibility.

STRATEGIC READINESS

Ready for a Deep-Tissue Audit?

Automated checks catch the noise. Our elite operators find the signal.
Schedule a 15-minute diagnostic brief with our team.

BOOK AUDIT BRIEF