CyberRisk Fast Track – Sample Report

Sample Report: AcmeCorp (Simulated Data Only)
Prepared by: Keith Pelchat

External Risk Scan

Tools Used: Nmap, OpenVAS

Open Ports Detected: 22 (SSH), 80 (HTTP), 443 (HTTPS)

Detected Services:

- Apache 2.4.52

- OpenSSH 8.2

- nginx 1.18.0

OS Fingerprint: Linux 5.X (Ubuntu)

Credential Exposure Check

Checked email: ceo@acmecorp.com

Breached Accounts Found:

- LinkedIn (2016)

- Dropbox (2012)

Recommendation: Reset exposed credentials, implement MFA, audit for reuse.

SSL/TLS Configuration Audit (testssl.sh)

TLS Versions Supported: TLS 1.0, 1.2, 1.3

Weak Cipher Suites Detected: TLS_RSA_WITH_3DES_EDE_CBC_SHA

Certificate Expiry: Valid until 2025-09-01

Additional Findings: No HSTS configured, deprecated protocols accepted

🧰 System Configuration Audit (Simulated)

Windows Findings:

- Local Administrator accounts enabled

- Missing critical patches: KB5015807, KB5026361

Linux Findings:

- SSH root login allowed

- Outdated Apache version 2.4.38 in use

📅 Prioritized 30-Day Action Plan (Sample)

Week 1: Close unused ports, update SSH and Apache configurations

Week 2: Reset compromised credentials, enforce MFA

Week 3: Patch all outdated systems (Windows & Linux)

Week 4: Implement recurring monthly scans + breach monitoring

📄 Executive Summary

This simulated report highlights common vulnerabilities small and mid-sized businesses face when lacking internal cybersecurity support. Issues found include exposed services, outdated SSL/TLS protocols, credential leaks, and system misconfigurations. Our CyberRisk Fast Track process identifies these risks and provides a clear, actionable plan for remediation.

👉 Book your own scan at: https://keithpelchat.com/fasttrack

Contact: keith@keithpelchat.com