PENETRATION TESTING & ETHICAL HACKING

Find your weaknesses before someone else does

You can't secure what you can't see.

Our Penetration Testing services simulate real-world cyberattacks to uncover vulnerabilities in your systems, applications, and infrastructure — so you can fix them before attackers find them. All tests are scoped to your risk, sector, and compliance needs.

🔍 What Is Penetration Testing?

Penetration Testing (or ethical hacking) is a simulated cyberattack performed by security professionals to identify how an attacker could exploit weaknesses in your environment.

We offer manual and automated tests targeting:

- External infrastructure (internet-facing systems)
- Internal networks and devices (post-breach scenario)
- Web applications and APIs
- Microsoft 365 / cloud environments
- OT/SCADA networks (passive review or safe testing only)

You'll receive a detailed report, practical remediation advice, and — if needed — executive-level summaries for boards, vendors, or insurers.

🧰 Types of Testing We Offer

🌐 External Penetration Testing

- Test public-facing services (VPNs, email, websites)
- Identify common attack vectors (credential stuffing, brute force, outdated software)
- Includes DNS, SSL, firewall, and exposure review

🏢 Internal Penetration Testing

- Simulates a threat actor inside the network (e.g. rogue employee or breached device)
- Tests lateral movement, privilege escalation, and access to sensitive systems

🔐 Web Application & API Testing

- OWASP Top 10 testing (XSS, SQLi, IDOR, etc.)
- Authentication, session management, and access control flaws
- Logic testing and input validation

☁️ Cloud Security Testing

- Microsoft 365, Azure, Google Workspace
- Review of configurations, roles, MFA enforcement, and misused services
- Detection of mailbox rules, shadow IT, and account takeovers

29/97 Creek Street, Brisbane City QLD 4000 ☎ 1300 067 003 ✉ info@vciso.one 💻 vciso.one

PENETRATION TESTING & ETHICAL HACKING

Find your weaknesses before someone else does

👤💼 Who This Is For

- **Councils and NFPs** pursuing Essential Eight or ISO 27001 maturity
- **SMBs** preparing for cyber insurance, vendor assessments, or client audits
- **Infrastructure providers** under SoCI Act needing annual testing
- **Dev teams** building apps that require independent security validation
- **IT managers** needing external assurance on internal hardening efforts

---

💬 What Our Clients Say

"The pen test gave us exactly what we needed — a clear picture of where we were exposed and a plan to fix it. The report wasn't just a pile of jargon — it was actually useful."

— IT Operations Manager, Regional NFP

📋 Deliverables You'll Receive

- ✅ A plain-English executive summary
- ✅ Technical vulnerability report with risk ratings
- ✅ Screenshots and proof-of-concept where applicable
- ✅ Prioritised remediation plan
- ✅ Optional retesting to verify fixes

All tests are scoped carefully to **avoid disruption** to production environments, with options for passive OT testing or testing in dev environments.

🎯 Compliance & Standards Coverage

We perform tests aligned to:

- ACSC Essential Eight
- ISO/IEC 27001
- PCI-DSS
- OWASP Testing Guide
- SoCI / ISM guidance for critical infrastructure

Need support choosing what to test? We can help define the right scope based on your risk profile and regulatory needs.

📦 Optional Add-Ons

- Integration with managed detection & response (MDR)
- Staff phishing simulations and awareness training
- Policy development (IR, breach notification, escalation matrix)
- Executive cyber briefings or board simulations
- Secure cloud backup and recovery guidance

Ready to Test Your Defences?

We'll help you scope a responsible, risk-aligned test — and turn it into actionable insights that drive real improvements.

Schedule a FREE Security Discovery Call

vCISO.One cybersecurity consulting & advisory

29/97 Creek Street, Brisbane City QLD 4000 ☎ 1300 067 003 ✉ info@vciso.one 💻 vciso.one