Service Overview

Effective penetration testing demands clear scoping, sound methodology, and strategic integration with your broader security programme. SynAck Solutions offers vendor-neutral consulting to help organisations design, scope, manage, and interpret penetration testing programmes — from defining test objectives and rules of engagement through to evaluating vendor proposals, reviewing third-party reports for quality, and translating findings into actionable remediation strategies.

Business Value

- Ensure testing engagements target the assets and attack vectors that matter most
- Evaluate third-party pentest vendor proposals objectively and avoid underscoped assessments
- Improve finding quality by setting clear methodology, evidence, and reporting standards
- Translate technical vulnerability data into business risk language for board reporting
- Develop a multi-year testing strategy covering your full attack surface
- Reduce remediation costs by prioritising on exploitability and threat relevance
- Demonstrate a mature, auditable testing programme to regulators and certifiers

What's Included

- Testing programme strategy with annual calendars, scope rotation, and coverage planning
- Scoping workshops to define objectives, targets, threat scenarios, and rules of engagement
- Vendor assessment and selection support including RFP development and proposal evaluation
- Third-party pentest report quality review for methodology, evidence, and rating calibration
- Remediation strategy translating findings into prioritised, resourced plans
- Compliance mapping of testing activities to APRA CPS 234, ISO 27001, PCI DSS, Essential 8
- Executive and board-level reporting distilling results into strategic risk communication
- Methodology advisory against PTES, OWASP, and NIST SP 800-115 standards
- Remediation verification framework design for confirming findings are addressed
- Stakeholder communication templates for technical and non-technical audiences

Scope

Penetration testing consulting covers the advisory and programme management aspects of your security testing activities.

- Strategic planning across infrastructure, application, cloud, and mobile domains
- Scoping and rules of engagement development for individual engagements
- Vendor management and evaluation of external testing providers
- Report review and quality assurance for third-party assessments
- Remediation planning and prioritisation based on pentest findings
- Regulatory and compliance alignment of testing documentation

What's Excluded

- Hands-on penetration testing execution (covered under dedicated Pentest services)
- Vulnerability scanning or automated security tool operation
- Remediation implementation (covered under Remediation Assistance)
- Ongoing vulnerability management or continuous scanning
- Legal review of contracts or rules of engagement

Methodology

Our consulting draws on PTES for engagement lifecycle, OWASP Testing Guide for application standards, NIST SP 800-115 for technical testing, and ISO 27001 for security management integration. We apply risk-based prioritisation aligned with ISO 31000 and threat-informed scoping using MITRE ATT&CK.

Engagement Timeline

Programme strategy engagements typically run two to four weeks including stakeholder workshops. Individual scoping or report reviews complete in three to five business days. Ongoing advisory retainers available for year-round consulting support. All deliverables provided within agreed timeframes.

Get Started

Contact SynAck Solutions to discuss strengthening your penetration testing programme. Whether you need scoping support, vendor evaluation, or a multi-year testing strategy, we bring deep technical expertise to every engagement.

info@synack.au | https://www.synack.au

ABN 88 667 784 956