Service Overview

SynAck Solutions' Remediation Assistance service provides hands-on support to close the gap between assessment findings and a genuinely hardened environment. Our consultants work alongside your teams to implement fixes across infrastructure, applications, and cloud environments — translating vulnerabilities into prioritised remediation plans and verifying every change through independent re-testing to confirm effective closure.

Business Value

- Reduce mean-time-to-remediate for critical and high-severity vulnerabilities
- Verify remediation through independent re-testing, not assumption
- Free internal IT teams to focus on operations while specialists address findings
- Satisfy regulatory requirements for documented remediation under APRA CPS 234
- Minimise risk of introducing new vulnerabilities during the patching process
- Accelerate closure of findings from penetration tests and audit reports
- Access specialist knowledge for complex scenarios like legacy system hardening

What's Included

- Review and triage of assessment findings from SynAck or third-party reports
- Prioritised remediation plan with effort estimates and risk ratings
- Hands-on vulnerability patching for operating systems, applications, and firmware
- Configuration hardening aligned to CIS Benchmarks and vendor best practices
- Active Directory and identity platform hardening (GPO, privilege reduction)
- Cloud remediation across AWS, Azure, and GCP (IAM, security groups, storage)
- Web application remediation guidance for development teams (OWASP Top 10)
- Targeted re-testing of remediated vulnerabilities to confirm closure
- Remediation evidence pack with before/after documentation and sign-off
- Knowledge transfer sessions with internal teams on root cause and prevention
- Post-remediation summary report with residual risk assessment

Scope

Engagements are scoped based on the volume and complexity of findings, tailored to the specific technologies where vulnerabilities were identified:

- Server and workstation operating systems (Windows, Linux, macOS)
- Network infrastructure: firewalls, switches, routers, and wireless controllers
- Cloud platforms (AWS, Azure, GCP) — IaaS, PaaS, and SaaS configurations
- Web applications, APIs, and supporting middleware
- Active Directory, Azure AD/Entra ID, and identity federation services
- Endpoint security tooling configuration (EDR, AV, host-based firewall)

What's Excluded

- Procurement or licensing of security products or software patches
- Remediation of findings in environments not included in agreed scope
- Ongoing managed security services beyond the engagement period
- Full application redevelopment or major code refactoring
- Hardware replacement or physical infrastructure upgrades
- Regulatory compliance certification or formal audit attestation

Methodology

Our approach follows NIST SP 800-40 and CIS Controls for prioritisation. Findings are triaged using CVSS scoring and contextual risk factors — asset criticality, exploitability, and regulatory exposure. Implementation follows change management best practices with documented rollback procedures. Re-testing uses the same tooling as the original assessment for consistent validation.

Engagement Timeline

Engagements typically span two to six weeks depending on finding volume and complexity. A prioritised remediation plan is delivered within three business days, with hands-on remediation and re-testing in agreed sprints. Final report with re-test results and residual risk assessment delivered within five business days of completion.

Get Started

Contact SynAck Solutions to discuss your assessment findings and remediation requirements. We will review your reports, scope the effort, and provide a tailored proposal for your environment and timeline.

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

ABN 88 667 784 956