



Service Overview

SynAck Solutions provides continuous, managed vulnerability scanning, risk prioritisation, and remediation tracking across your infrastructure, applications, and cloud environments — powered by an enterprise scanning platform with integrated automated penetration testing validation. Unlike point-in-time assessments, our managed service operates continuously, identifying new vulnerabilities from software updates, configuration changes, and emerging threats. Discovered vulnerabilities are validated through automated exploitation, confirming real-world exploitability and eliminating false positives. Analysts prioritise confirmed findings by business impact and track remediation to closure against agreed SLAs.

Business Value

- Maintain continuous visibility into vulnerability posture across all environments
- Confirm exploitability through automated penetration testing — not just theoretical risk
- Prioritise remediation based on confirmed exploitation, asset criticality, and business impact
- Reduce mean time to remediate through structured tracking and SLA-driven workflows
- Satisfy patching and vulnerability management requirements under Essential 8, APRA CPS 234, and PCI DSS
- Free internal IT teams from scan management, triage, and reporting overhead
- Track remediation trends with integrated compliance reporting to demonstrate continuous improvement

What's Included

- Enterprise scanning platform deployment, configuration, and ongoing management
- Automated penetration testing validation confirming exploitability of discovered vulnerabilities
- Scheduled scanning — weekly, fortnightly, or monthly — tailored to your risk appetite
- Authenticated and unauthenticated scanning across internal and external surfaces
- Cloud-native scanning for AWS, Azure, and GCP workloads and configurations
- Exploitation-confirmed findings with false positive elimination and contextual scoring
- Risk prioritisation using CVSS, EPSS, exploitation status, and asset criticality
- Remediation tracking dashboard with SLA monitoring and integrated compliance reporting
- ITSM integration (ServiceNow, Jira, Freshservice) for ticket creation and tracking
- Monthly vulnerability posture report with trend analysis and SLA compliance
- Ad-hoc scanning for zero-day and emergency vulnerability disclosures

Scope

The service covers vulnerability identification and tracking across your agreed technology estate, defined during onboarding.

- External-facing assets: public IP ranges, web applications, DNS, email gateways
- Internal infrastructure: servers, workstations, network devices, databases
- Cloud environments: AWS, Azure, and GCP compute, storage, and managed services
- Container and Kubernetes environments where scanner agents are supported
- OT and IoT devices where safe scanning profiles are available
- Third-party hosted applications accessible via authenticated scanning

What's Excluded

- Remediation and patching of identified vulnerabilities (available separately)
- Penetration testing and manual exploitation (available via Penetration Testing)
- Application source code review or static analysis (SAST/DAST)
- Vulnerability scanner licensing where the client uses their own platform
- Network architecture redesign or firewall rule changes

Methodology

Our methodology aligns with NIST SP 800-40, ISO 27002 technical vulnerability management controls, and the ASD Essential 8 patching strategies. Prioritisation combines CVSS scores, EPSS exploit likelihood, automated exploitation confirmation, asset criticality, and environmental context. Remediation SLAs follow Essential 8 timeframes — critical within 48 hours, high within two weeks, moderate within one month.

Engagement Timeline

Onboarding — scanner deployment, asset discovery, policy configuration, and ITSM integration — completes within two to three weeks. First validated report delivered within four weeks. Ongoing scanning operates on agreed cadence with monthly reports within five business days of month-end. Twelve-month minimum term.

Get Started

Contact SynAck Solutions to schedule a vulnerability management scoping consultation. We'll assess your patching maturity, define scanning scope and SLAs, and establish a continuous programme to stay ahead of emerging threats.

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

ABN 88 667 784 956