



Service Overview

SynAck Solutions delivers comprehensive Wireless (WiFi) Security Assessments that evaluate the security posture of your organisation's wireless network infrastructure. Our certified operators test corporate, guest, and IoT wireless networks using the same techniques employed by real-world attackers — from rogue access point deployment and WPA2/WPA3 cracking to evil twin attacks and wireless client manipulation.

Every engagement is conducted on-site using specialised wireless testing hardware and follows industry-standard methodology. We assess not only the technical security of your wireless infrastructure but also the effectiveness of network segmentation, client isolation, and monitoring controls that protect your wired network from wireless-originating threats.

Business Value

- Identify exploitable weaknesses in wireless infrastructure before attackers do
- Validate WPA2/WPA3 Enterprise configuration and certificate-based authentication
- Assess network segmentation between corporate, guest, and IoT wireless networks
- Detect rogue access points, misconfigured SSIDs, and shadow IT wireless devices
- Test wireless intrusion detection and prevention system (WIDS/WIPS) effectiveness
- Meet compliance obligations: ISO 27001, PCI DSS, Essential Eight, APRA CPS 234
- Receive actionable remediation guidance for wireless hardening and monitoring

What's Included

- Wireless reconnaissance: SSID enumeration, signal mapping, and access point fingerprinting
- WPA2/WPA3 security assessment: key management, authentication, and protocol configuration
- 802.1X/RADIUS and EAP configuration testing (PEAP, EAP-TLS, EAP-TTLS)
- Evil twin and rogue access point attack simulation
- Wireless client attack testing: deauthentication, disassociation, and credential harvesting
- Guest network isolation and segmentation validation
- IoT and operational wireless network assessment where in scope
- Rogue access point detection across assessed facilities
- Post-authentication lateral movement testing from wireless network segments
- Branded report: executive summary, findings, heatmap, remediation guidance
- Delivery in four formats: Word, PDF, interactive HTML, and Google Doc
- Post-engagement debrief and remediation guidance with your network team

Scope

The engagement covers wireless infrastructure across agreed physical locations:

- Corporate wireless networks (WPA2/WPA3 Enterprise, 802.1X)
- Guest and visitor wireless networks
- IoT and operational technology wireless segments
- Wireless access points, controllers, and management interfaces
- RADIUS/AAA infrastructure supporting wireless authentication
- Wireless intrusion detection/prevention systems (WIDS/WIPS)

Testing is conducted on-site at agreed facilities. Multiple sites can be assessed within a single engagement. RF coverage mapping and signal leakage assessment included for perimeter areas.

What's Excluded

- Internal wired network penetration testing (available separately)
- External infrastructure penetration testing (available separately)
- Social engineering or phishing campaigns
- Denial-of-service or sustained disruption of wireless services
- Bluetooth, Zigbee, or non-WiFi wireless protocol testing
- Physical security testing beyond wireless signal coverage assessment

Methodology

Our methodology aligns with the Wireless Penetration Testing Execution Standard and OWASP Wireless Security Testing Guide. Testing covers infrastructure configuration, authentication mechanisms, encryption strength, client-side attacks, and network segmentation. Each finding is scored using CVSS v3.1 with remediation guidance.

Engagement Timeline

A typical wireless assessment runs 2-5 business days on-site depending on the number of facilities and wireless network complexity. Final report delivery within 5 business days of testing completion. Re-test of remediated findings available within 30 days at 30% of initial engagement cost.

Get Started

Contact us to discuss your requirements and receive a tailored proposal. We will work with you to define site locations, wireless network scope, and schedule on-site testing at a time that suits your operations.

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

ABN 88 667 784 956