Service Overview

SynAck Solutions delivers Physical Attack Surface Assessments that evaluate the real-world effectiveness of your facility security controls. Our operators test physical access controls, surveillance systems, and personnel security awareness using the same techniques employed by sophisticated adversaries — including tailgating, badge cloning, lock bypass, and social engineering. Every engagement follows PTES methodology mapped to MITRE ATT&CK techniques.

Business Value

- Validate that physical access controls actually prevent unauthorised entry
- Identify gaps between documented security policies and real-world enforcement
- Test staff awareness and response to social engineering at the physical layer
- Meet compliance for physical security under ISO 27001, APRA CPS 234, SOCI Act
- Reduce risk of insider threat, corporate espionage, and supply chain compromise
- Gain evidence-based recommendations for security investment prioritisation
- Demonstrate due diligence to boards, regulators, and cyber insurance underwriters

What's Included

- Pre-engagement reconnaissance of facility layout, access points, and security posture
- Tailgating and piggybacking attempts at controlled entry points
- Badge cloning and RFID/NFC access card duplication testing
- Lock bypass assessment: picking, shimming, and bypass tool evaluation
- USB drop testing with instrumented payloads to measure plug-in rates
- Dumpster diving and waste disposal security assessment
- Pretexting and social engineering at reception, loading docks, and common areas
- Surveillance system coverage gap analysis (CCTV blind spots, camera angles)
- Server room and sensitive area physical access testing
- Photographic and video evidence capture of all successful access
- Branded report with findings, evidence, ATT&CK mapping, and remediation

Scope

The engagement covers all physical security controls at client-designated facilities:

- Building perimeter fencing, gates, and external access points
- Reception areas, lobby controls, and visitor management procedures
- Electronic access control systems (RFID, NFC, biometric, PIN)
- Mechanical locking systems on doors, cabinets, and server racks
- Staff security awareness and response to social engineering attempts
- Waste disposal practices and document destruction procedures
- Delivery and loading dock access procedures

What's Excluded

- Destructive entry or forced breach of doors, windows, or barriers
- Testing at facilities not explicitly listed in scope documentation
- Cyber exploitation of systems accessed during physical testing
- After-hours testing unless explicitly authorised and coordinated
- Testing that could endanger life, safety, or trigger emergency services
- Assessment of third-party or co-tenanted facilities without authorisation

Methodology

Our methodology aligns with PTES physical security testing guidelines and ASIS PSP standards. Each finding is scored for exploitability and business impact, mapped to MITRE ATT&CK techniques, and accompanied by tactical and strategic remediation guidance. Testing follows a graduated approach — passive observation first, then active testing as authorised.

Engagement Timeline

A typical physical assessment runs 3-5 business days depending on the number of facilities and scope complexity. Final report delivery within 5 business days of testing completion. Follow-up validation of remediated controls available within 30 days.

Get Started

Contact us to discuss your facilities, security concerns, and testing objectives. We will conduct a pre-engagement site review, define scope and rules of engagement, and schedule testing windows that align with your operations.

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

ABN 88 667 784 956