Service Overview

SynAck Solutions conducts objective-based red team operations that replicate the tactics, techniques, and procedures (TTPs) of real-world threat actors. Our operators execute multi-phase campaigns — from OSINT and initial access through C2 establishment, lateral movement, and data exfiltration — testing your people, processes, and technology as an integrated defence system. Every technique is mapped to MITRE ATT&CK for structured reporting.

Business Value

- Test your entire defensive ecosystem against realistic adversary behaviour
- Identify detection and response gaps that penetration tests cannot surface
- Validate SOC effectiveness and incident response workflows under real pressure
- Map organisational resilience against industry-relevant threat actors
- Demonstrate security control validation for APRA CPS 234 and the SOCI Act
- Provide blue teams with high-fidelity IOCs for detection engineering
- Quantify MTTD and MTTR against specific ATT&CK techniques

What's Included

- Threat intelligence-informed adversary profile and TTP selection
- Comprehensive OSINT and reconnaissance of infrastructure and personnel
- Social engineering campaigns for initial access (email, voice, SMS, or physical)
- Custom C2 infrastructure with covert communication channels
- Privilege escalation and credential harvesting across AD and cloud identity
- Lateral movement through network segmentation boundaries
- Data exfiltration simulation without triggering detection alerts
- Persistence mechanism deployment and detection testing
- Full MITRE ATT&CK mapping with timestamped activity logs
- Technical report with attack narrative and detection gap analysis
- Executive summary with risk-rated findings and strategic recommendations
- Post-engagement purple team replay session with your SOC

Scope

Red team assessments are objective-driven, scoped to simulate realistic adversary campaigns:

- External attack surface including web applications, email, and VPN endpoints
- Internal network, data centre, and cloud infrastructure (AWS, Azure, GCP)
- Active Directory, Azure AD/Entra ID, and federated identity providers
- Human targets for social engineering within agreed ethical boundaries
- Physical security perimeter where included in rules of engagement
- Third-party integrations and supply chain access points as agreed

What's Excluded

- Denial-of-service attacks or intentional production service disruption
- Exploitation of systems explicitly excluded in the rules of engagement
- Testing against third-party systems without written authorisation
- Destructive actions such as data deletion or ransomware deployment
- Ongoing managed security services post-engagement
- Hands-on remediation implementation (available separately)

Methodology

Our methodology is built on MITRE ATT&CK for technique selection, PTES for engagement structure, and CBEST/TIBER-EU frameworks for adversary emulation. We operate under a trusted agent model with deconfliction protocols and emergency stop procedures. Campaign planning incorporates current threat intelligence to ensure realistic adversary simulation.

Engagement Timeline

Red team assessments typically span four to eight weeks. The first one to two weeks cover OSINT and adversary profile development. Active operations run two to four weeks with real-time deconfliction. Report delivery within ten business days, with a purple team replay session included.

Get Started

Contact SynAck Solutions to discuss your red team objectives and threat landscape. We will define realistic objectives, establish rules of engagement, and design a campaign that validates your organisation's resilience.

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

ABN 88 667 784 956