Service Overview

SynAck Solutions conducts structured purple team exercises that combine offensive tradecraft with defensive validation in a collaborative, iterative format. Using the MITRE ATT&CK framework as a common language, our operators execute specific techniques against your environment while your SOC team observes in real time. Each technique is scored for visibility, detection, and response — producing a quantified detection coverage matrix that drives targeted improvement.

Business Value

- Quantify detection coverage across the MITRE ATT&CK matrix with empirical testing
- Identify specific detection gaps and prioritise engineering effort accordingly
- Validate SOC alert fidelity — reduce false positives while catching real threats
- Uplift blue team capability through hands-on exposure to adversary tradecraft
- Accelerate detection rule development with real attack telemetry
- Demonstrate measurable improvement in security operations maturity
- Align defensive investment with techniques most relevant to your threat landscape

What's Included

- Pre-engagement threat profiling to select relevant ATT&CK techniques
- Collaborative exercise planning with SOC leadership and detection engineers
- Controlled execution of 30–60 ATT&CK techniques (scalable to scope)
- Real-time collaboration between SynAck operators and your blue team
- Per-technique scoring: visibility, detection, and response capability
- Detection coverage heatmap mapped to the full MITRE ATT&CK matrix
- Detection rule recommendations including Sigma, KQL, or SPL rule logic
- Telemetry source analysis identifying missing or misconfigured log sources
- Alert tuning recommendations for improved signal-to-noise ratio
- Response playbook validation and improvement recommendations
- Comprehensive report with per-technique results and remediation roadmap

Scope

Assessments are scoped to your security operations capability and monitored environments, defined collaboratively:

- EDR platforms and configured detection rules and behavioural analytics
- SIEM platforms, log correlation rules, and telemetry source coverage
- Network detection and response (NDR) tools and traffic analysis capabilities
- Active Directory and identity-based attack detection, including Entra ID
- Cloud workload protection and cloud-native security monitoring
- Incident response procedures, escalation workflows, and containment playbooks

What's Excluded

- Covert adversary simulation (covered under Red Team Assessment)
- Exploitation of zero-day or undisclosed vulnerabilities
- Remediation implementation — recommendations provided, engineering is separate
- Physical security testing or social engineering campaigns
- Ongoing SOC monitoring or managed detection services

Methodology

Our methodology is structured around MITRE ATT&CK, using ATT&CK Navigator for technique selection and coverage visualisation. Each technique is executed using documented procedures, scored against a standardised detection maturity model, and correlated with SIEM, EDR, and NDR telemetry in real time.

Engagement Timeline

Assessments typically run two to four weeks. The first week focuses on threat profiling and exercise coordination. Active purple team sessions run one to two weeks with daily collaborative sessions. A comprehensive report with detection heatmap is delivered within seven business days. Re-testing is available within 60 days.

Get Started

Contact SynAck Solutions to discuss your detection engineering priorities and SOC maturity goals. We will design a purple team programme that delivers measurable, repeatable improvement in detection and response capability.

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

ABN 88 667 784 956