Service Overview

SynAck Solutions performs controlled evasion testing that evaluates whether your EDR, antivirus, and endpoint protection can detect and prevent the techniques real adversaries use to bypass defences. Our consultants develop custom payloads, test bypass techniques against your deployed security stack, and provide actionable intelligence on detection gaps — all mapped to the MITRE ATT&CK Defence Evasion tactic (TA0005).

Business Value

- Validate true detection capability of your EDR/AV against real-world evasion techniques
- Identify blind spots in your security stack before adversaries exploit them
- Strengthen SOC detection engineering with concrete examples of missed alerts
- Demonstrate compliance with control validation under APRA CPS 234 and the SOCI Act
- Quantify which controls deliver genuine protection versus false confidence
- Reduce ransomware and advanced malware risk by testing common evasion techniques
- Uplift internal security team capability with adversary-grade tradecraft knowledge

What's Included

- Pre-engagement scoping of target EDR/AV platforms and security policy configurations
- Custom payload development for your endpoint protection stack
- AMSI bypass testing across PowerShell, .NET, VBScript, and JScript contexts
- ETW patching and log evasion assessment for telemetry pipeline visibility gaps
- Process injection testing: DLL injection, hollowing, thread hijacking, APC, syscalls
- In-memory execution and fileless malware simulation
- LOLBins testing using legitimate Windows binaries for payload execution
- User-mode and kernel-mode unhooking assessment against EDR hooks
- Obfuscation and encoding validation including custom crypters and packers
- Technical report with ATT&CK mapping and detection verdicts per technique
- Executive summary for board and senior leadership
- Post-engagement debrief with your SOC and security engineering teams

Scope

Testing is scoped to your endpoint security controls and host environments:

- Windows workstation and server endpoints with production EDR/AV configuration
- PowerShell, .NET, and native Windows scripting execution environments
- Application whitelisting and execution control policies (AppLocker, WDAC)
- Endpoint telemetry and logging pipelines (Sysmon, WEF, EDR telemetry)
- Network detection controls intersecting payload delivery (sandbox, proxy)
- macOS and Linux endpoints where EDR coverage extends to these platforms

What's Excluded

- Exploitation of application or OS vulnerabilities (covered under Penetration Testing)
- Social engineering or phishing for initial delivery (covered under Red Team/PhaaS)
- Physical access testing or hardware implant deployment
- Modification of production security tools — all testing is observational
- Ongoing managed detection or continuous monitoring

Methodology

Our methodology is grounded in MITRE ATT&CK Defence Evasion (TA0005) and PTES for engagement structure. Payload development follows NIST SP 800-115 guidance. Each technique is executed with real-time coordination with your security team to correlate detection events, alert fidelity, and telemetry coverage against the ATT&CK data sources matrix.

Engagement Timeline

A typical engagement runs two to four weeks. Custom payload development begins in week one, with active testing over one to two weeks. Technical report and executive summary delivered within five business days of testing completion. Re-testing of remediated controls available within 30 days at no additional cost.

Get Started

Contact SynAck Solutions to schedule a scoping call. We will review your endpoint protection stack, identify priority evasion techniques, and define a testing programme that delivers measurable assurance.

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

ABN 88 667 784 956