Service Overview

SynAck Solutions maps every internet-facing asset your organisation exposes before an attacker does. We perform deep subdomain enumeration, passive DNS analysis, port scanning, service fingerprinting, and shadow IT discovery across cloud providers and SaaS platforms. The result is a living inventory of your external risk surface — including assets your own teams may not know exist.

Business Value

- Discover unknown subdomains, IPs, and cloud resources expanding your attack surface
- Identify shadow IT and orphaned infrastructure before threat actors exploit them
- Correlate certificate transparency logs with DNS records to reveal hidden services
- Benchmark external exposure against industry peers and best-practice baselines
- Receive continuous monitoring recommendations to catch new assets as they appear
- Prioritise remediation based on exploitability scoring, not just asset count
- Gain board-ready visibility into your organisation's true digital footprint

What's Included

- Passive reconnaissance: subdomain harvesting, certificate transparency, DNS records
- Active enumeration of all discovered assets for exposed services and versions
- Cloud asset discovery across AWS, Azure, GCP, and major SaaS platforms
- Shadow IT identification — infrastructure outside IT's known inventory
- Port and service fingerprinting with version detection across all targets
- Default credential and exposed management interface checks
- Risk-prioritised asset inventory with ownership mapping
- Branded report with executive summary, findings, and remediation roadmap
- Delivery in four formats: Word, PDF, interactive HTML, and Google Doc
- Post-engagement debrief with your security and infrastructure teams

Scope

The engagement covers all externally discoverable assets associated with your organisation, including but not limited to:

- Primary and subsidiary domain names and all subdomains
- Public IP address ranges and cloud-hosted infrastructure
- Certificate transparency records and SSL/TLS certificates
- DNS records including MX, NS, TXT, CNAME, and SPF entries
- SaaS and third-party hosted services linked to your domains
- Publicly accessible APIs, portals, and management interfaces

Scope boundaries are defined collaboratively during pre-engagement. Testing windows and escalation contacts are agreed in advance.

What's Excluded

- Exploitation of discovered vulnerabilities (available as a separate penetration test)
- Internal network scanning or assessment
- Social engineering, phishing, or vishing campaigns
- Denial-of-service or destructive testing of any kind
- Third-party hosted assets without explicit written authorisation
- Continuous monitoring deployment (recommendations provided)

Methodology

Our methodology combines passive OSINT collection with active enumeration, aligned to the PTES reconnaissance phase. Each discovered asset is validated, fingerprinted, and risk-scored. Findings are mapped to MITRE ATT&CK Reconnaissance techniques (TA0043).

Engagement Timeline

A typical external attack surface discovery runs 5-10 business days depending on organisational size and domain complexity. Final report delivery within 5 business days of assessment completion. Follow-up reassessment available quarterly to track attack surface changes over time.

Get Started

Contact us to discuss your requirements and receive a tailored proposal. We will map your digital footprint, identify unknown assets, and deliver actionable intelligence on your external exposure.

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

ABN 88 667 784 956