Service Overview

SynAck Solutions' Dark Web & Breach Monitoring service provides continuous surveillance of underground forums, paste sites, dark web marketplaces, and breach repositories to detect exposed credentials and threat actor activity targeting your organisation. Our platform aggregates intelligence from Tor-based forums, Telegram channels, initial access broker listings, infostealer log marketplaces, and public breach databases — with analyst-triaged alerts to eliminate false positives.

Business Value

- Detect compromised employee and customer credentials before they are weaponised
- Reduce mean time to respond (MTTR) for credential-based threats
- Identify data leaks, IP exposure, and sensitive document exfiltration
- Support Notifiable Data Breaches (NDB) scheme obligations with breach awareness
- Monitor for brand impersonation, typosquatted domains, and identity fraud
- Provide board and executive leadership with regular threat exposure reporting
- Strengthen third-party risk management by monitoring supply chain exposures

What's Included

- Continuous monitoring of dark web forums, marketplaces, paste sites, and breach databases
- Monitoring of Telegram channels, Discord, and emerging threat actor platforms
- Credential exposure detection across organisational and specified personal domains
- Infostealer log analysis — session cookies, saved passwords, and auth tokens
- Initial access broker monitoring for listings referencing your infrastructure
- Automated alerting with analyst-triaged escalation
- Monthly threat intelligence digest with trend analysis
- Quarterly executive summary report with risk scoring and recommendations
- Domain and brand monitoring for typosquatting and phishing infrastructure
- Integration with your existing SIEM, SOAR, or ticketing platform
- Dedicated threat intelligence analyst for escalation and inquiries

Scope

Monitoring scope is defined by your organisation's digital footprint — domains, email patterns, IP ranges, brand names, and key personnel identifiers.

- All organisational email domains and specified subsidiary domains
- Executive and high-value target monitoring (C-suite, IT admins, finance)
- IP address ranges and autonomous system numbers (ASNs)
- Brand names, trading names, and common typosquats
- Specified third-party and supply chain partner domains
- Source coverage: Tor hidden services, I2P, Telegram, paste sites, breach compilations

What's Excluded

- Active engagement with threat actors (purchasing data or negotiating)
- Domain takedown or abuse reporting services
- Remediation of compromised accounts — guidance provided
- Endpoint monitoring for active infostealer infections (recommend EDR/MDR)
- Legal advice regarding breach notification obligations
- Customer-facing breach notification communications

Methodology

Our methodology aligns with NIST CSF Identify and Detect functions and MITRE ATT&CK Reconnaissance (TA0043) and Resource Development (TA0042) tactics. Intelligence collection follows the F3EAD cycle with automated collection complemented by human analyst review.

Engagement Timeline

Onboarding — including digital footprint definition and baseline exposure assessment — completes within one to two weeks. Continuous monitoring operates 24/7 with real-time alerting. Monthly digests and quarterly executive reports are included. The service operates on a twelve-month subscription.

Get Started

Contact SynAck Solutions to schedule a dark web exposure assessment. We'll map your digital footprint, conduct an initial sweep for existing exposures, and activate continuous monitoring.

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

ABN 88 667 784 956

Copyright © SynAck Solutions Pty Ltd — https://www.synack.au