Service Overview

When a security incident strikes, the speed and quality of response determines whether it remains contained or escalates into a full-scale breach. SynAck Solutions provides incident response through retainer-based and emergency on-call models, covering ransomware, business email compromise, data breaches, insider threats, and APT intrusions. Our retainer model ensures pre-negotiated response times, pre-positioned tooling, and a team that already understands your environment.

Business Value

- Minimise business impact through rapid, expert-led containment and eradication
- Reduce dwell time by deploying experienced responders who quickly scope compromises
- Preserve forensic evidence for regulatory notification and legal proceedings
- Satisfy incident reporting obligations under the Privacy Act, APRA CPS 234, and SOCI Act
- Identify root cause and attack vector to prevent recurrence
- Provide executive and board-level incident briefings with clear impact communication
- Maintain business continuity through coordinated response minimising disruption

What's Included

- Incident response retainer with SLAs for response initiation (two to four hours)
- 24/7 emergency hotline for critical incident escalation
- Initial triage and severity assessment to determine scope and priority
- Containment actions: network isolation, credential rotation, access revocation
- Digital forensic investigation across endpoints, servers, cloud, and email systems
- Malware analysis and reverse engineering of adversary tooling
- Eradication of persistence mechanisms, backdoors, and compromised accounts
- Recovery assistance including system restoration and security hardening
- Root cause analysis identifying initial access vector and exploitation chain
- Regulatory notification support including NDB assessment and OAIC drafts
- Post-incident report with timeline, findings, and strategic recommendations

Scope

Incident response services cover the full lifecycle of security incident management across your technology environment.

- Windows, Linux, and macOS endpoint forensics and response
- Cloud investigation and response across AWS, Azure, and GCP
- Email platform investigation for Microsoft 365 and Google Workspace
- Network traffic analysis and lateral movement detection
- Active Directory and identity provider compromise investigation
- Ransomware response including encryption assessment and recovery coordination

What's Excluded

- Legal advice or representation — we provide technical findings and evidence
- Insurance claim management or negotiation with threat actors
- Long-term managed detection and monitoring (covered under Managed SIEM/SOC)
- BCP activation and crisis communication — we coordinate with your BCP team
- Hardware replacement or physical infrastructure recovery

Methodology

Our methodology follows NIST SP 800-61 (Computer Security Incident Handling Guide): preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Forensic procedures align with ISO 27037 for evidentiary integrity. We use MITRE ATT&CK to characterise adversary behaviour and align with ACSC incident response guidance.

Engagement Timeline

Retainer clients receive response initiation within two to four hours. Active response typically runs one to four weeks depending on compromise scope. Post-incident report delivered within ten business days of completion, with a lessons learned workshop within 30 days. Non-retainer emergency engagements subject to availability.

Get Started

Contact SynAck Solutions to establish an incident response retainer. A retainer ensures guaranteed response times, pre-positioned capabilities, and a team ready to act when it matters most.

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

ABN 88 667 784 956