Service Overview

SynAck Solutions' Managed SIEM & SOC service delivers 24/7 security monitoring, threat detection, and incident response through a dedicated Security Operations Centre. We ingest and correlate log data from across your environment — endpoints, networks, cloud platforms, and applications — applying MITRE ATT&CK-mapped detection rules and behavioural analytics. Every alert is triaged by experienced analysts; only validated incidents are escalated to your team.

Business Value

- Achieve 24/7 threat monitoring without building an in-house SOC
- Reduce alert fatigue — only analyst-validated incidents reach your team
- Detect advanced threats via ATT&CK-mapped rules and behavioural analytics
- Meet regulatory monitoring obligations under APRA CPS 234, SOCI Act, and ISO 27001
- Accelerate mean time to detect (MTTD) and respond (MTTR) for incidents
- Gain unified visibility across on-premises, cloud, and hybrid environments
- Reduce total cost of ownership compared to in-house SIEM deployment

What's Included

- Fully managed SIEM platform deployment, configuration, and ongoing tuning
- 24/7/365 monitoring by qualified SOC analysts (Tier 1, 2, and 3 escalation)
- Log source onboarding — endpoints, firewalls, cloud platforms, identity providers
- Detection rule development and maintenance mapped to MITRE ATT&CK techniques
- Behavioural analytics and UEBA for anomaly detection
- Threat intelligence feed integration for IOC matching
- Alert triage, investigation, and contextualised incident escalation
- Incident response coordination and containment guidance
- Monthly security posture report with detection metrics and trend analysis
- Compliance dashboards for APRA CPS 234, Essential 8, and ISO 27001
- Quarterly detection engineering review and rule tuning

Scope

The service covers log ingestion and monitoring across your agreed technology environment, defined during onboarding based on infrastructure, cloud footprint, and compliance requirements.

- On-premises infrastructure: firewalls, switches, routers, servers, domain controllers
- Cloud platforms: Microsoft 365, Azure, AWS, GCP log sources
- EDR platform integration — CrowdStrike, Microsoft Defender, SentinelOne
- Identity and access management: Active Directory, Entra ID, Okta, Duo
- Web application firewalls, proxy servers, and email security gateways
- Custom application logs where structured logging is available

What's Excluded

- SIEM platform licensing (we support BYO or can procure on your behalf)
- Hands-on incident response and forensics beyond containment guidance
- Endpoint agent deployment and management (available as Managed EDR)
- Network architecture redesign or firewall rule management
- Application-level vulnerability remediation

Methodology

Our SOC aligns with NIST CSF Detect and Respond functions and ISO 27035 for incident management. Detection rules are developed using the MITRE ATT&CK matrix to ensure coverage across all tactics. Alert triage follows structured playbooks aligned with NIST SP 800-61.

Engagement Timeline

Onboarding takes four to six weeks including platform deployment, log source integration, and initial tuning. Full 24/7 monitoring commences upon onboarding completion. The service operates on a twelve-month minimum term with monthly or annual billing and quarterly service reviews.

Get Started

Contact SynAck Solutions to schedule a Managed SIEM & SOC scoping consultation. We'll assess your logging maturity and design a service tailored to your environment and compliance obligations.

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

ABN 88 667 784 956