Cyber Operations & Analytics Services

Enablement services for advanced security analytics, automated response, and insider threat detection

Cyber Operations & Analytics Services provides specialist enablement to help organisations detect, investigate, and enable effective response to cyber threats using data-driven analytics and automation. The service supports the establishment or enhancement of cyber operations capabilities across on-premises, cloud, and hybrid environments, enabling security teams to improve visibility, reduce response times, and strengthen governance.

Security Analytics & Threat Detection Enablement Services

Enablement of SIEM and security analytics capabilities to identify threats, anomalous behaviour, and indicators of compromise using security, operational and machine data.

Typical activities include:

- Platform configuration for security analytics and threat detection
- Data source onboarding and normalisation
- Detection use-case development and tuning
- Alerting, dashboards, and investigative workflows
- Validation, documentation, and operational handover

Security Orchestration, Automation & Response (SOAR) Enablement Services

Enablement of orchestration and automation capabilities to streamline incident response and reduce manual effort.

Typical activities include:

- SOAR platform configuration and integration
- Playbook design and implementation
- Automation of triage, enrichment, and response actions

- Integration with existing security tools and processes
- Testing, tuning, and operational handover

Insider Threat Detection Enablement Services

Enablement of analytics to identify potential insider threat activity through behavioural analysis and contextual monitoring.

Typical activities include:

- Insider threat use-case definition and modelling
- Configuration of behavioural analytics and baselining
- Data correlation across identity, endpoint, and activity sources
- Alerting and investigation workflows
- Governance, documentation, and handover

Outcomes for Buyers

- Improved detection of external and internal threats
- Faster, more consistent incident response
- Reduced operational overhead through automation
- Better use of security data to support decision-making
- Clear documentation and operational readiness