Cyber Threat Intelligence Services

Enablement and enrichment services to improve threat awareness, prioritisation and response

Cyber Threat Intelligence Services provides specialist support to help organisations consume, operationalise and apply threat intelligence to improve cyber security decision-making. The service enables security teams to better understand emerging threats, prioritise risk, and enrich detection and response activities across on-premises, cloud and hybrid environments.

Buyers may select Threat Intelligence Enablement Services, Threat Intelligence Enrichment Services, or a combination of both under a single call-off.

Threat Intelligence Enablement Services

Enablement of threat intelligence capabilities to support proactive threat awareness and informed security operations.

Typical activities include:

- Threat intelligence architecture and integration design
- Configuration of threat intelligence ingestion and normalisation
- Alignment of intelligence feeds to organisational risk and use cases
- Enablement of dashboards, alerts and reporting
- Validation, documentation and operational handover

Threat Intelligence Enrichment Services

Enablement of threat intelligence enrichment to provide context to security events, alerts and investigations.

Typical activities include:

- Integration of threat intelligence with detection and analytics workflows
- Enrichment of alerts with indicators, reputation and context
- Correlation of intelligence with assets, vulnerabilities and activity
- Tuning of enrichment logic to reduce false positives
- Documentation and operational handover

Outcomes for Buyers

- Improved awareness of relevant cyber threats
- Better prioritisation of security alerts and risks
- Faster and more informed investigation and response
- Reduced noise through contextual enrichment
- Clear documentation and operational readiness