Cyber Extended Detection & Response (XDR) Services

Enablement services for unified threat detection, investigation and response across networks, endpoints and cloud

Cyber Extended Detection & Response (XDR) Services provides specialist enablement to help organisations detect, investigate and respond to cyber threats using correlated telemetry across multiple security domains. The service supports the establishment or enhancement of XDR capabilities to improve visibility, reduce alert fatigue, and accelerate response across on-premises, cloud and hybrid environments.

Buyers may select one or both enablement services under a single call-off, depending on their security architecture and maturity.

Security XDR Enablement Services

Enablement of XDR capabilities to correlate signals from endpoints, identity, cloud and security tooling into a unified detection and response workflow.

Typical activities include:

- XDR architecture design and platform configuration
- Data source onboarding and normalisation
- Detection use-case enablement and tuning
- Alerting, investigation workflows and response actions
- Testing, documentation and operational handover

Security NDR Enablement Services

Enablement of Network Detection & Response (NDR) capabilities to identify threats, anomalous behaviour and lateral movement within network traffic.

Typical activities include:

- NDR deployment and network telemetry integration
- Baseline creation and behavioural analytics configuration
- Detection use-case enablement and tuning
- Integration with investigation and response workflows
- Validation, documentation and operational handover

Outcomes for Buyers

- Improved detection of advanced and evasive threats
- Reduced alert noise through correlated analytics
- Faster investigation and response across security domains
- Enhanced visibility across endpoints, networks and cloud
- Clear documentation and operational readiness