

Service description document: Cyber security services

Cyber security services

eir business provides a comprehensive portfolio of cyber security and technology services designed to help organisations protect their systems, data, and users in an increasingly complex threat landscape. Our services support public sector and regulated organisations in improving cyber resilience, maintaining operational continuity, and meeting governance, compliance, and assurance requirements.

The services described in this document cover a broad range of security and technology capabilities, including security monitoring and detection, managed cyber security services, penetration testing, endpoint and device management, application services, and platform support. Each service is designed to be delivered independently or combined as part of a wider, integrated security and IT operating model.

eir business services are delivered using structured, best-practice approaches and industry-standard technologies. They are designed to be scalable, flexible, and aligned to customer requirements, supporting organisations of varying size, complexity, and maturity. Service scope, service levels, and delivery models are defined clearly to provide transparency and assurance at call-off.

This document provides a high-level description of each service, including service purpose, scope, and key characteristics. Commercial terms, pricing, and optional enhancements are defined separately within the applicable pricing documentation.

1. Security Operations Centre (SOC) / SIEM Service

Service overview

Our SOC SIEM Service provides continuous security monitoring, detection, and analysis of security events across an organisation's IT and cloud environments. The service is delivered using a centralised Security Information and Event Management (SIEM) platform that collects, normalises, and correlates security telemetry from agreed data sources. The service is designed to identify potential security incidents, suspicious activity, and policy violations through a combination of automated detection logic and analyst-led triage. It delivers timely, actionable security alerts to support investigation and informed decision-making, improving visibility of the organisation's overall security posture. This service focuses on monitoring, detection, and analysis. Incident containment or remediation activities are not included unless explicitly agreed as part of a separate service.

Scope of service

The SOC / SIEM Service includes:

- Onboarding and configuration of the SIEM platform
- Ingestion of security logs and telemetry from agreed data sources
- Normalisation and correlation of security events
- Configuration of detection rules and security use cases
- Continuous monitoring of in-scope telemetry
- Analyst triage and validation of security alerts
- Severity-based alerting and notification
- Support for security investigations through event analysis
- Regular security monitoring and trend reporting
- Ongoing tuning of detection logic to reduce false positives

Service outputs and deliverables

The service provides the following outputs:

- Security alerts aligned to agreed severity levels
- Incident and monitoring summary reports
- Event and log data to support investigation activities
- Documentation of onboarded data sources and detection use cases
- Service performance and activity summaries

Service characteristics

- Delivered on a continuous monitoring basis (24×7 unless otherwise agreed)
- Scoped to agreed data sources, environments, and log types
- Dependent on customer-provided access and log availability
- Analyst-supported detection and alerting model
- Scalable based on data volume and number of monitored sources
- Delivered using enterprise-grade SIEM technologies
- Does not guarantee detection of all security incidents
- Complements, but does not replace, incident response services

2. CyberGuard Lite – Managed Cyber Security Service

Service overview

CyberGuard Lite is a centrally managed cyber security service designed to provide essential, insurance-aligned protection for organisations requiring strong cyber hygiene without operational complexity. The service delivers continuous monitoring, proactive risk reduction, and user-focused security controls through a single, managed service.

The service combines endpoint monitoring, vulnerability management, patching, user awareness, email security, and cyber risk reporting to reduce exposure to common cyber threats such as malware, phishing, ransomware, and credential compromise. It is delivered as a fully managed service, removing the need for customers to deploy, integrate, or operate individual security tools.

CyberGuard Lite provides a pragmatic uplift in cyber resilience, supporting regulatory, audit, and cyber insurance requirements while remaining lightweight and operationally efficient.

Service scope and capabilities

The service includes the following core components:

- Managed Detection and Response (MDR): Continuous monitoring of endpoints with automated threat detection, investigation, and response.
- Vulnerability Management: Ongoing vulnerability scanning with prioritised remediation guidance and regular reporting.
- Patch Management: Operating system and application patching, validation, and compliance reporting.

- Security Awareness and Phishing Training: Employee cyber awareness training, phishing simulations, and user risk scoring.
- Email Security" Advanced filtering to protect against phishing, impersonation, malware, and malicious attachments.
- Cyber Risk Dashboard and Reporting: Centralised risk scoring and reporting aligned to cyber insurance and governance requirements.

Service levels and support

CyberGuard Lite is delivered as a managed, cloud-based security service with continuous operational monitoring.

Service support includes:

- 24×7 endpoint monitoring and threat response
- Incident detection, triage, and containment
- Defined escalation paths for high-severity incidents
- Monthly service reporting covering threats, vulnerabilities, patching, and user risk

3. CyberGuard – Managed Cyber Security Service

Service overview

CyberGuard is a fully managed cyber security service designed to provide organisations with essential, scalable cyber protection delivered through a flexible monthly service model. It enables customers to improve their cyber resilience, meet recognised best-practice security standards, and protect critical systems, users, and data without the need for in-house security resources.

The service is designed to address common cyber security challenges, including limited internal expertise, increasing threat exposure, regulatory pressure, and budget constraints. CyberGuard provides a structured, managed approach to cyber security, allowing organisations to focus on operational priorities while maintaining a strong security posture aligned to recognised UK guidance.

Key service components

CyberGuard combines multiple managed security capabilities into a single service, which may include:

- Security awareness training for end users
- Workstation and endpoint security review
- Managed endpoint detection and response (EDR/XDR/MDR)
- Vulnerability scanning and assessment
- Penetration testing
- DNS and dark web monitoring
- Backup and disaster recovery services (BaaS/DRaaS)
- Identity and access compliance controls
- Incident response support
- Cloud security and compliance support

- Certification and standards support, including Cyber Essentials and Cyber Essentials Plus
- ISO 27001 readiness and ongoing support

Service components are selected based on customer requirements and can be scaled as needs evolve.

Standards and alignment

CyberGuard aligns with recognised UK cyber security guidance and good practice, including National Cyber Security Centre (NCSC) principles for cyber hygiene. The service supports organisations in implementing controls across areas such as data protection, malware defence, access management, phishing prevention, and secure configuration.

Delivery model

The service is delivered as a managed, subscription-based offering, with continuous monitoring, review, and improvement. CyberGuard is designed to scale with organisational growth, enabling additional security capabilities to be introduced without disruption or significant upfront investment.

4. Penetration Testing Service

Service overview

Our Penetration Testing service provides manual, intelligence-led security testing designed to identify vulnerabilities across systems, applications, and infrastructure. The service simulates real-world attack techniques to assess the effectiveness of existing security controls and identify areas of risk before they can be exploited.

Testing is delivered by qualified penetration testers and is aligned to recognised industry standards and ethical testing methodologies, ensuring results are suitable for public sector assurance, compliance, and risk management requirements.

Scope of the service

Penetration testing is scoped and agreed in advance to align with organisational objectives, technical environments, and risk appetite. The service can include, but is not limited to:

- Internal and external infrastructure penetration testing
- Web application penetration testing
- API and service testing
- Cloud platform and configuration reviews
- Network and wireless security testing (where in scope)

A combination of manual testing techniques and supporting tools is used to identify, validate, and evidence vulnerabilities, with a focus on realistic attack paths and business impact.

Service delivery

Testing can be delivered remotely or on-site, depending on customer requirements and scope. All activity is conducted in a controlled and ethical manner, with clear engagement rules and minimal operational disruption.

Reporting and outputs

Customers receive a comprehensive penetration testing report, including:

- An executive summary suitable for senior and non-technical stakeholders
- Detailed technical findings with supporting evidence
- Risk-based vulnerability ratings
- Clear, practical remediation recommendations
- Post-test clarification and follow-up support where required

Benefits

- Independent validation of security controls
- Improved understanding of organisational risk exposure
- Support for compliance, assurance, and audit requirements
- Actionable insight to prioritise remediation activities
- Reduced likelihood of successful cyber attack

5. Application Development

Service overview

eir business Application Development provides the design, development, testing and delivery of bespoke software applications tailored to customer requirements. The service supports organisations in delivering secure, scalable and maintainable applications aligned to defined business objectives and technical standards.

Scope of service

The service covers the full application development lifecycle, from initial requirements definition through to delivery and handover. Engagements can be delivered on a project basis or through iterative development approaches, depending on customer needs.

Key service components

- Requirements analysis and solution design
- Application development and unit testing
- Secure coding practices and quality assurance
- Application deployment and handover
- Technical documentation and knowledge transfer

Deliverables

- Custom-developed application components or services
- Source code and supporting technical documentation
- Test evidence and release notes

Service characteristics

- Project-based or iterative delivery models
- Delivered using agreed development methodologies
- Secure development principles applied throughout
- Ongoing operational or managed support excluded unless explicitly agreed

6. Application Package Management

Service Description

eir business Application Package Management provides the creation, maintenance and lifecycle management of application installation packages for customer environments. The service enables consistent, secure and reliable deployment of applications across supported endpoint and platform technologies, using agreed standards, tooling and deployment methods.

The service focuses on packaging commercially available or internally developed applications to support automated or managed deployment. It does not include application development, software vendor support, or end-user support unless explicitly agreed.

Service Scope

The service supports enterprise application packaging activities, including new application onboarding and updates to existing packages. Application packages are prepared to support silent, unattended and automated installation where required, and are aligned with customer deployment tools and standards.

Application Package Management is delivered as a scoped, request-based service and can be scaled based on application volume and complexity.

Typical Service Inclusions

- Creation of application installation packages for deployment
- Packaging of new applications and updates to existing packages
- Testing of application packages in agreed environments
- Alignment with agreed packaging standards and deployment tools
- Version control and maintenance of packaged applications
- Support for common installer types and packaging formats
- Documentation of packaging configurations and dependencies
- Packaging to support silent and automated installation
- Minor package updates following application version changes
- Handover of packaged applications to customer deployment teams

Deliverables

- Application installation packages ready for deployment
- Packaging documentation and installation instructions
- Test evidence or confirmation of successful package testing
- Versioned package artefacts for agreed applications
- Change records for updated or replaced packages

Service Characteristics

- Scoped per application and packaging request
- Delivered during agreed service hours
- Dependent on customer-provided installation media and licences
- Supports standard enterprise packaging and deployment tools
- Focused on repeatable and consistent application deployment
- Scalable based on application volume and complexity
- Does not include application remediation or deployment unless agreed

7. Device Monitoring

Service description

eir business Device Monitoring provides continuous, proactive monitoring of customer endpoints and network-connected devices to identify availability issues, security-related events, and abnormal behaviour. The service enables early detection of incidents and operational issues, supporting improved service reliability and faster investigation.

The service is designed to complement wider security monitoring and incident response services, providing visibility across supported devices through the collection and analysis of telemetry data.

Typical service inclusions

- Continuous collection and analysis of device telemetry
- Monitoring of device availability, performance, and security indicators
- Automated alerting based on defined thresholds and event types
- Analyst triage of alerts to reduce false positives
- Event correlation to support incident investigation
- Regular monitoring summaries and reporting at agreed intervals

Service deliverables

- Security and availability alerts
- Monitoring reports provided at agreed frequencies
- Incident-related event summaries to support investigation activities

Service characteristics

- Continuous monitoring of supported devices
- Near real-time alerting
- Dependent on device connectivity and correct configuration
- Complements, but does not replace, incident response services

8. Endpoint Management Service

Service overview

The Endpoint Management service provides centralised management and operational control of customer-owned endpoint devices to support security, compliance, and day-to-day IT operations across distributed environments.

The service enables organisations to maintain consistent configuration, enforce security baselines, manage software updates, and monitor endpoint health and compliance across supported operating systems and device types. It is designed to support modern, remote and hybrid working models while reducing operational overhead and improving visibility across the endpoint estate.

The service is delivered using industry-standard endpoint management tooling and is scalable based on the number and type of endpoints in scope.

Service scope and capabilities

The Endpoint Management service typically includes:

- Centralised endpoint configuration and policy management
- Software deployment, patching, and update management
- Security baseline enforcement and compliance monitoring
- Endpoint asset visibility and health status monitoring
- Support for device lifecycle activities, including onboarding and decommissioning
- Incident and exception notification where applicable

The service supports customer-owned devices and integrates with wider IT and security operations processes where required.

Service delivery model

The service is delivered as a proactive, policy-driven managed service, designed to operate continuously across distributed endpoint environments.

eir business provides service coordination, operational oversight, and customer engagement, ensuring consistent service delivery and alignment with customer requirements. The service can be delivered as a standalone capability or integrated with broader managed security and IT services.

Service levels and support

The Endpoint Management service is supported through defined service levels aligned to operational criticality.

Support typically includes:

- Access to service desk support via ticketing systems
- Incident logging, investigation, and escalation
- Monitoring of endpoint compliance and service health
- Reporting on endpoint status and policy adherence

Response times and escalation paths are aligned to incident severity and are defined within the applicable service schedule. Where underlying platform service levels apply, these are flowed through as part of the overall service commitment.

Commercial model

The service is provided on a subscription basis and is typically licensed according to the number of managed endpoints.
Commercial characteristics include:

- Subscription-based service aligned to an agreed contract term
- Licensing based on the number and type of endpoints under management
- Scalable service model allowing endpoints to be added or removed
- Optional professional services for onboarding, configuration, or optimisation


business
secure, managed solutions for all.