RelianceCyber

Proactive Cyber Security Professional Services

Service Definition

G-Cloud 15

Lot 3: Cloud Support

Contact Details

Email: tenders@reliancecyber.com

Contact Number: +44 (0) 845 519 2946

Contents

1 What are Proactive Professional Services?

This document defines Reliance Cyber's Proactive Professional Services, designed to support Public Sector organisations in the end-to-end management, optimisation and evolution of their cloud environments.

Unlike traditional reactive support models, our proactive approach focuses on preventative maintenance, continuous value realisation and strategic foresight. We operate as an integrated extension of your team, utilising data-driven insights to mitigate risks, control costs, and ensure that cloud infrastructure evolves in alignment with departmental goals.

Anticipate, Don't Just Respond

Modern public services require 99.9% uptime and absolute security. Achieving this requires a shift from "reactive troubleshooting" to "proactive stewardship." Our services are built on three core pillars:

- **Preventative Governance**: Continuous monitoring of security posture and compliance to prevent incidents before they occur.
- **Operational Efficiency**: Regular rightsizing and security reviews to eliminate waste and ensure every pound of public spending is maximised.
- **Futureproofing**: Iterative roadmap planning that prepares your organisation for emerging technologies, such as AI and serverless architectures, ensuring you remain prepared for the ever changing cyber security innovations.

All service pricing will be based on the scope of the service delivery. A scoping call will be conducted prior to sharing of estimated days required for completion of works alongside the relevant consultant job role within the pricing document.

2 Reliance Cyber's Proactive Professional Services

Our proactive cybersecurity services are designed to help organisations stay ahead of emerging threats through identifying areas of weakness before an incident happens, providing targeted recommendations and support to close gaps to make our clients more resistant to cyberattacks and more resilient should one occur.

Through regular assessments, hands-on testing and expert-led simulations, we provide clarity on your current security posture and practical guidance to strengthen it. These services support strategic decision-making, reduce the likelihood of breaches, and ensure your teams are better prepared to respond if the worst happens. Whether it's your infrastructure, cloud environment, or internal response capabilities, our approach focuses on continuous improvement and resilience.

2.1 Security Posture Review

Description

A Security Posture Review is designed to assess the maturity of an organisation's security controls, both from a technical and compliance perspective, and establish any gaps in capability. The service combines strategic governance interviews, technical configuration verification, and formal compliance mapping to establish a robust baseline. The review combines manual and automated analysis to analyse a range of cybersecurity domains, including identity management, data protection, network security, and monitoring practices.

The goal is to identify vulnerabilities, validate best practices and provide actionable, targeted recommendations for improvement with the option of developing a cyber roadmap.

Scope

- Review of key security controls across a number of cyber domains.
- Assessment of cybersecurity strategy, policies and procedures, tying them to industry standards and frameworks and checking alignment with overall business goals and risk appetite
- Workshops with key stakeholders to assess governance and risk management.
- Technical deep dives, including automated tooling, to assess the effectiveness of key security controls, including configurations.
- Establishing maturity scores and a baseline for cybersecurity going forward.

Deliverables

- Granular technical and compliance reports outlining findings in detail.

- A detailed report outlining findings, risks, and prioritised remediation actions.
- An interactive workshop to present results and recommendations to key stakeholders.
- A remediation plan with best practice guidance and training suggestions for IT teams.
- Final report summarising the review, improvements, and future recommendations.

2.2 Infrastructure Security

Description

Our Infrastructure Security services focus on protecting your organisation's physical and digital infrastructure. We assess risks, identify weaknesses, and provide guidance on how to secure critical systems, both on-premises and in the cloud, from evolving threats.

Scope

- Risk assessment of on-premises and cloud-based infrastructure.
- Assessment of tooling and technologies.
- Vulnerability analysis of servers, storage, and network devices.
- Recommendations for infrastructure hardening and protection.
- Assistance with the implementation of security measures and controls.

Deliverables

- **Infrastructure Security Report**: Overview of the current security posture.
- **Vulnerability Assessment**: Identifying weaknesses and threats to infrastructure.
- **Recommendations**: Steps for hardening infrastructure and reducing exposure.
- **Security Plan**: Actionable steps for securing infrastructure from physical and digital threats.

2.3 Platform and Host Review

Description

A security assessment of the build standards was conducted against industry benchmarks. Our build review test will review a selected or a selection of build images used across your organisation's devices to ensure there are no misconfigurations or vulnerabilities that have not been found.

Scope

- Conduct white-box security assessments of host systems using both automated and manual techniques.
- Evaluate host configurations against industry-recognised standards such as CIS benchmarks.
- Audit patch levels, user permissions, password policies, and operating system hardening.
- Review third-party applications and their security posture.
- Inspect host-level policies and configurations for compliance and risk exposure.

Deliverables

- Detailed assessment report highlighting configuration gaps, vulnerabilities, and remediation recommendations.
- CIS benchmark alignment summary for each host assessed.
- Risk ratings and prioritised action plan for identified issues.
- Evidence logs and screenshots from manual inspections and tool outputs.
- Executive summary for stakeholders outlining key findings and strategic recommendations.

2.4 Cloud Security Assessment

Description

Our Cloud Security Assessment service evaluates the security of your cloud infrastructure to identify risks and vulnerabilities. We ensure that your cloud environment is protected against potential threats while aligning with industry best practices and regulatory requirements.

Scope

- Assessment of cloud architecture, security controls, and access management.
- Identification of potential security gaps and configuration weaknesses.
- Evaluation of cloud-specific threats and vulnerabilities.
- Recommendations for enhancing security and mitigating risks in the cloud environment.

Deliverables

- **Cloud Security Assessment Report:** Comprehensive analysis of cloud security posture.
- **Risk Assessment:** Evaluation of risks and threats to cloud resources.
- **Recommendations:** Steps to improve cloud security and reduce exposure to threats.

- **Compliance Checklist:** Review of compliance with cloud-specific security regulations.

2.5 Tabletop Exercise

Description

A tabletop exercise is a structured, discussion-based workshop where teams walk through a hypothetical scenario to evaluate plans, roles and decision-making in a low-pressure environment. The exercises are tailored to the organisation's specific risks and can be targeted at technical teams, executives, or board members to build awareness, decision-making skills, and operational resilience. Unlike a crisis simulation exercise, during a tabletop exercise it not about real-time execution – they address strategic thinking, policy reviews and collaborative discussion without the immediacy of a live scenario.

Scope

- 3-hour workshop simulating a real-world cyber incident.
- Delivered in-person or remotely.
- Tailored scenarios based on the organisation's specific risks, systems, and structure.
- Designed for different audiences: technical teams, executives, or board members.
- Escalating scenario injections to test decision-making and response coordination.

Deliverables

- Post-exercise report highlighting strengths, weaknesses, and recommendations.
- Enhanced readiness and operational resilience through experiential learning.
- Alignment with ISO 27001, NIST, GDPR, and other compliance frameworks.
- Demonstrable risk management for cyber insurance and regulatory purposes.
- Optional bespoke packages for unique threats (e.g. APTs, insider risks, supply chain attacks).

2.6 Incident Readiness Support

Description

Our Incident Readiness Support services provide businesses with tailored, actionable plans to quickly and effectively address incident response processes and obligations. We work with your team to understand gaps in capability and develop and refine incident response policies,

playbooks and procedures, ensuring that your organisation can respond effectively to a cyber-attack.

Scope

- Assessment of documentation and capability around incident response, including workshops.
- Development and refinement of incident response plans and other related documentation.
- Tabletop exercises and testing of incident response procedures (if requested).
- Coordination with internal teams and external stakeholders (e.g., legal, PR, regulators).

Deliverables

- Gap analysis: Assessment of incident response capability
- Incident Response Plan: Customisable and actionable steps for handling security incidents.
- Playbook Development: Specific instructions for managing various types of security incidents.
- Compliance and Legal Guidance: Ensuring proper regulatory and legal responses during incidents.

2.7 Compromise Assessment

Description

The compromise assessment leverages threat intelligence to uncover both current and historical threats across an entire environment. The objective is to identify active or dormant compromises, identify root cause, evaluate the organisation's exposure to broader threats, and provide actionable insights to enhance security defences and reduce risk. Our process is both measurable and repeatable, enabling continuous active defence and measurable improvements to your environment.

Note: If a breach is identified, we will switch to emergency response mode and respond accordingly.

Scope

- Deployment of DFIR tools across the environment for data collection and analysis.
- Threat intelligence-driven analysis of realistic threats targeting your organisation to focus the assessment.
- Detection of current and historical compromises using IoCs, TTPs, and advanced forensic techniques.

- Comprehensive analysis of endpoints, servers, networks, and cloud infrastructure based upon specific threat profiles.
- Assessment of broader threats, including vulnerabilities, misconfigurations, and lateral movement risks.
- Integration of external and industry-specific threat intelligence to tailor the assessment.

Deliverables

- **Compromise Assessment Report**: Detailed findings, including evidence of compromises, threat actor activity, and risk analysis.
- **IoCs and Threat Intelligence Insights**: Comprehensive documentation of malicious indicators and adversary behaviours identified.
- **Risk and Exposure Analysis**: Identification of vulnerabilities, misconfigurations, and risks posed by identified threats.
- **Remediation Recommendations**: Actionable steps to resolve compromises, close security gaps, and reduce exposure to threats.
- **Strategic Threat Defence Plan**: Long-term recommendations for improving detection, response, and proactive threat mitigation capabilities.

2.8 Threat Hunt

Description

Threat Hunt aims to uncover unknown, stealthy, or emerging threats within an environment before they escalate into incidents. Unlike reactive investigations, it does not rely on a predefined hypothesis but instead uses threat intelligence, behavioural analysis, and expert-led hunting techniques to identify suspicious activity across cloud, endpoint, and network data sources. The goal is to detect hidden risks, improve visibility, and strengthen overall threat detection capabilities.

Scope

- Proactive, environment-wide hunt for unknown threats without a predefined hypothesis.
- Analysis of endpoint, cloud, and network telemetry using threat intelligence and behavioural detection.
- Identification of suspicious patterns, anomalies, and stealthy adversary techniques.

Deliverables

- Threat Hunt Report: Summary of methods, findings, and insights.
- Detection Gaps: Highlighted weaknesses in current monitoring.

- Recommendations: Actions to improve detection, response, and threat visibility.

2.9 Cyber Engineering Services

Our Cyber Engineering team provide comprehensive solutions for designing, implementing, managing, and optimising security systems to protect organisations from unauthorised access, threats, and vulnerabilities. These services support the enhancement of cyber resilience for an organisation's critical infrastructure and sensitive data.

2.9.1 Network & Security Infrastructure

Security Infrastructure Professional Services are designed to help organisations build, implement, and manage a robust and scalable security framework to safeguard their IT environments. This service focuses on protecting critical assets, ensuring regulatory compliance, and enabling secure business operations using client security systems and best practices. The Cyber Engineering Team can provide the end-to-end delivery of most security systems projects.

This includes, but is not limited to:

- Design and Planning
- Proof of Concept
- Implementation and Testing
- Migration

Scope

- Evaluate the current state of security infrastructure and identify vulnerabilities.
- Conduct network Security infrastructure reviews and performance tuning.
- Provide resilient security architecture tailored to organisational needs.
- Cloud environments and hybrid setups.
- Secure and controlled access to resources.
- Upgrades or migrations to modern security solutions
- Ensure optimal performance and scalability of security solutions.
- Provide post-implementation monitoring and troubleshooting.

Deliverables

- Provide a detailed gap analysis report with actionable recommendations.
- Optimise security policies and configurations.
- Provide professional support and recommendations.

- Carry out updates, patches, and maintenance of security systems.
- Design, plan and migration documentation as per client requirements.

These services are essential for organisations aiming to fortify their security systems while staying proactive in the face of evolving cyber threats.

2.9.2 Network Segmentation

Our Network Segmentation is a service that helps organisations to segregate a network into smaller, isolated segments to enhance security, control data flow and limit access. By separating critical systems from less secure or publicly accessible areas, network segmentation reduces the risk of unauthorised access, minimises the impact of cyberattacks, and improves compliance with regulatory requirements. It enables organisations to enforce tailored security policies for each segment, ensuring that sensitive data and operations remain protected. Also heavily used as a "kill switch" in case of cyber-attack breaches.

Scope

Workshops with client to identify business requirements to determine data flow and access requirements.

- Audit client network, security systems to support design.
- Define objectives for the Network Segmentation project.
- Design logical and physical network segments as per business needs.
- Implement and support changes based on the network segmentation design
- Add access control policies and communication pathways between segments.
- Provide post-implementation monitoring and troubleshooting.
- Validate connectivity between segments to ensure functionality and compliance with policies.

Deliverables

- Network segmentation design document, including diagrams.
- Defined access control policies and security rules.
- Implementation, migration support plan.
- Configured network devices and tools.

2.9.3 Network Security

Description

Our Network Security services help safeguard your organisation's network infrastructure from cyber threats. Through comprehensive assessments, we identify vulnerabilities in your network and recommend measures to secure your environment from both external and internal threats.

Scope

- Network architecture review and security analysis.
- Identification of network vulnerabilities and exposure points.
- Review of configuration and implementation of network security controls.
- Recommendations for adjustments to maintain network security.

Deliverables

- Network Security Assessment Report: Identification of weaknesses and vulnerabilities.
- Risk Mitigation Plan: Recommendations for improving network defences.
- Remediation Support: Assistance in implementing security measures.
- Continuous Monitoring Plan: Strategies for ongoing security of the network.

2.9.4 ZTNA Deployment

Zero Trust Network Access (ZTNA) Deployment involves designing and implementing a security framework that enforces strict access controls where no user or device is trusted by default, even inside the network. ZTNA ensures secure access to applications and resources based on user identity, device security posture, and other contextual factors.

Scope

- Workshops with client to identify business and design.
- Design and plan suitable ZTNA solution (cloud-based or on-premises) that meets the organisation's requirements.
- Implement and integrate ZTNA solution with client existing security systems as per design (SSO, MFA, SIEM, etc).
- Configure access policies to resources based on client defined requirements. Such as:
- User identity and groups.
- Device security posture (managed, unmanaged devices, etc).
- User and device location.

Deliverables

- Assessment report, including identified resources and access requirements.
- Design documentation of the deployed solution.
- Deployment, migration and post implementation support plan.
- Configure ZTNA solution and integration with other Security systems.

2.9.5 Security Systems Health Checks and Audits

Reliance Cyber Security Systems Health Checks & Audits involve assessing the current state of an organisation's security infrastructure to identify vulnerabilities, ensure compliance and optimise performance. These services provide a comprehensive evaluation of security controls, policies, and systems to ensure they are effectively protecting the organisation against cyber threats.

Please note that this service covers Firewalls, load balancers, remote access, web proxies.

Scope

- Validate your security systems against vendors and industry standards.
- Evaluate the health and performance of security systems to identify gaps and vulnerabilities.
- Assess patch management practices and identify outdated or vulnerable systems.
- Review security and access control policies.
- Identify and categorise identified risks based on their potential impact.
- Provide recommendations for identified risks.

Deliverables

Detailed report of the current security systems including:

- Identified vulnerabilities and gaps.
- Prioritised list of risks with mitigation strategies.
- Summary of findings and recommendations.
- Workshop with client to present and discuss report.

3 Why Reliance Cyber?

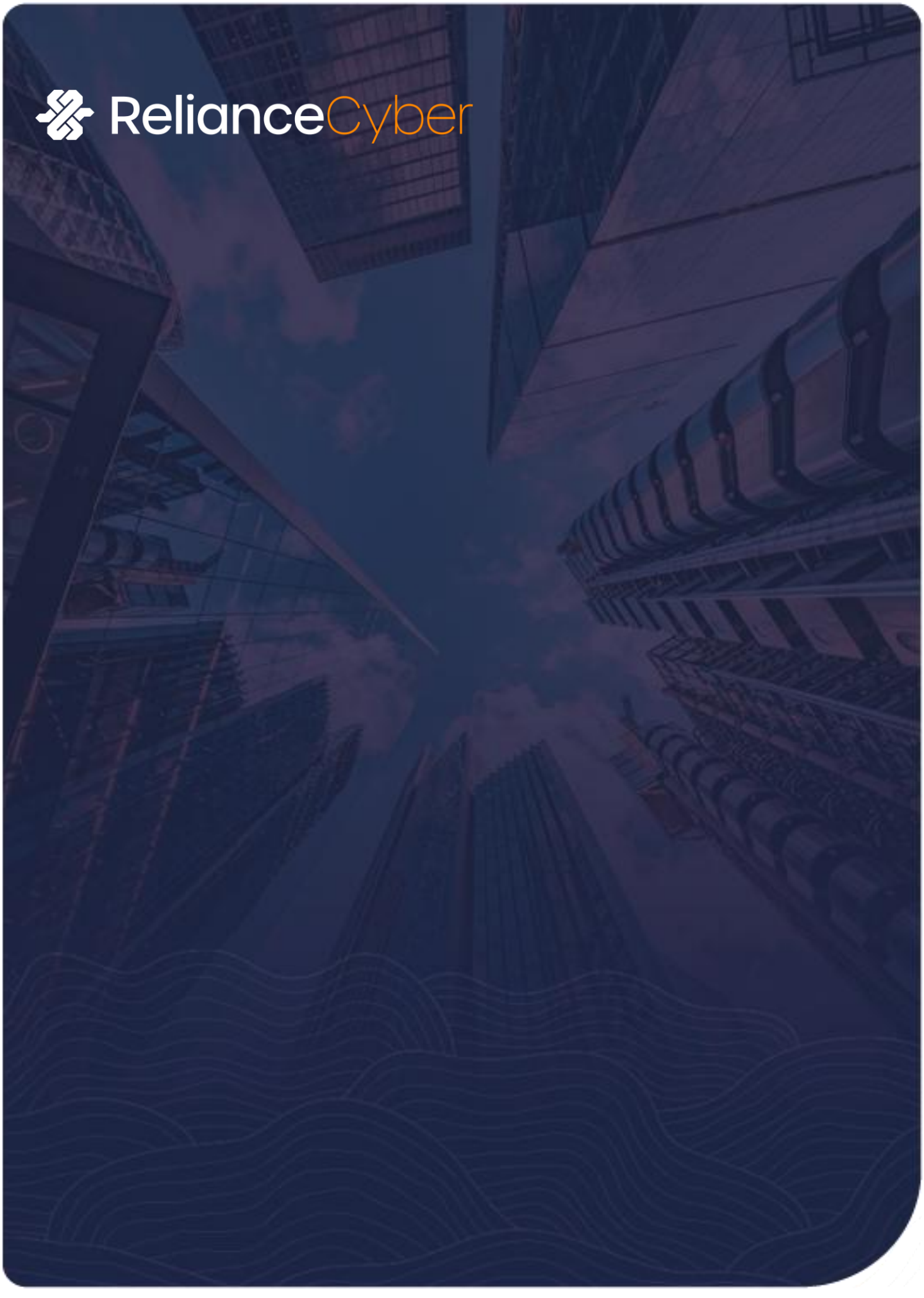
Reliance Cyber is a Managed Security Services Partner (MSSP), dedicated to fortifying our clients through cyber security. With a rich legacy spanning 20 years, Reliance Cyber has emerged as a trusted and innovative MSSP, continually reinvesting to ensure our clients receive the best security support on the market. This has enabled us to recruit the best SC specialists and develop market-leading capabilities focused solely on cyber security.

Operating 24x7x365, we prioritise collaboration, transparency and long-term trust-based relationships with clients to navigate the ever-evolving landscape of cyber threats.

3.1 Core Capabilities

Reliance Cyber's core services are structured around three strategic pillars, reflecting our holistic approach to cyber threat management across managed, proactive and reactive services.

- **Managed Services** – We deliver enhanced security operations through continuous monitoring, proactive threat detection, and rapid remediation. Operating 24x7 on our clients' behalf, our managed services include Managed Detection and Response (MDR), Managed Endpoint Detection and Response (EDR), Managed Secure Access Service Edge (SASE), Phishing Monitoring and Vulnerability Management.
- **Proactive Consulting Services** – We support clients in identifying and addressing vulnerabilities before threat actors can exploit them. Our proactive security offerings include Cyber Threat Intelligence, Crisis Simulations, Compromise Assessments and a range of bespoke solutions tailored to meet each client's unique risk landscape.
- **Reactive Consulting Services** – When incidents occur, we provide expert incident response and recovery support. Our services are delivered using methodologies certified by CREST and aligned with guidance from the National Cyber Security Centre (NCSC). Leveraging deep digital forensics expertise, we help clients contain, investigate, and recover from cyber incidents swiftly and effectively, minimising impact and enabling lessons learned to strengthen future defences.


RelianceCyber