G-Cloud 15 Service Description

Cyber Security Services

Cloud21

A Tegria Company

Table of Contents

1. PROPOSED SERVICES 2
2. ENGAGEMENT AND PLANNING 3
3. WHY CLOUD21 4
4. PRICING 5

1. Proposed Services

Our agile NHS focused Cyber Security solutions and services alleviate strain on clients' IT/Cyber teams by providing expert strategic advice, and hands on technical skills. We are experienced in delivering improvements across many NHS organisations helping them achieve compliance with Cyber Essentials and the DSPT, by delivering improvements to patch management, secure by default principles, security operations, risk management, subject matter expertise and wider cyber security programmes.

Cloud21 can support organisations with the following activities:

VCISO/Senior Leadership/Consultancy

- Provide a cyber incident escalation point.
- Review cyber security strategies.
- Review existing cyber security reports and create prioritised and actionable remediation plans.
- Work with the SIRO to understand current posture and support strategic aims.
- Continually review and benchmark Trusts cyber security compliance.
- Investigate current NHS Digital toolset to utilise free tools and services e.g. Phishing, technical audit, and reviews.
- Provide support and advice on how cyber security resilience could be improved.
- Review and provide assurance that technical work is being conducted appropriately.
- Support in the deployment of IT infrastructure hardening e.g. rogue file shares, security permissions etc.
- Support the Trust to produce detailed lists of IAO and IAA across all internal systems and reference with security compliance.
- Review and compile reports for meetings as required.
- Review current SOPs and identify potential policy gaps.
- Ensure that current security software tools are working as required.
- Attend meetings as required.
- Review options for hardening the IT infrastructure e.g. gold images, legacy operating systems.
- Support meeting the Cyber Assessment Framework.

Governance and compliance

- Mapping Data Flows and completion of RoPA.
- Data Protection Impact Assessment. o Cyber Security Impact Assessment.
- Resilience and disaster recovery.
- Monitoring use and compliance.
- Application Owners and Annual check List once in production.
- Governance and Risk Management.
- Support with meeting the Data Security and Protection Toolkit, Cyber Essentials Plus, ISO 27001, and the NCSC 10 Steps or Cyber Assessment Framework.
- vCISO.
- NHS and NCSC best practice.
- Tabletop scenario testing.
- Framework implementation.

Technical Design

- Integrations and API security.
- Secure by Design and best practice.
- Post installation security testing.
- Log monitoring.
- Encryption of data.
- Application Security.
- Microsoft Cyber Security Reference Architecture.
- Strategic reviews and Recommendations.

Service Features

- Real-time device monitoring through SIEM, and XDR technology products
- Patching and updates management service, end of support system upgrades
- CareCERT management, remediation, and compliance
- DSPT, ISO 27001, and Cyber Essentials compliance support
- Penetration test technical remediation assistance
- Vulnerability scanning, assessment and programme architecture and management
    - Including Medical IoT vulnerability scanning service via Cylera (Software not included)
- Assess and validate technical controls, processes, architecture and systems
- vCISO - Strategic Cyber guidance for OnPrem, Hybrid & Cloud
- Managed security infrastructure services, Firewall, Web, Anti-Virus
- 24x365 Security Operations Centre (SOC) plus Honeypot Service

Service Benefits

- Vendor agnostic. (SCCM, SolarWinds, Qualys, Lansweeper, Nessus, ManageEngine, Ivanti, Palo Alto Networks, Imprivata, Cylera, Thinkst etc)
- Responsive and agile SLAs to suit all customers' requirements
- Scalable, elastic service with on demand access to cyber professionals
- Expert advice from a leading IT consultancy in healthcare
- Proactive monitoring of systems and network infrastructure
- Allows customers to focus on their core business functions
- Achieving a proactive posture which is secure by default
- Extensive Security Operations knowledge and experience within the NHS and healthcare
- Improved ability detecting, remediating, and responding to a cyber-attack
- DSPT compliant, ISO 27001 and Cyber Essentials Plus accredited

2. Engagement and planning

We work with our customers initially hosting scoping workshops to understand the full scope of the services which need to be delivered.

This also allows us to fully understand the business, strategies, objectives and current position – and where the customer wants to get to. We can then align technically with the business

strategies and deliver the right outcomes and value. Our consultants will ensure that the design and delivery of any of our Managed IT Security Service meets the needs of our customers.

If required, we can provide a full cyber security assessment for commencement of any work.

The assessment is broken into the below 13 areas, and the scoring aligns with the NCSC 10 Steps to Cyber Security, the NCSC Cyber Assessment Framework, the NCSC Cloud Security Principles, the DSPT, and the Cyber Security Maturity Model. The 13 areas are explained in brief below.

- **Structure** (Organisational, board level engagement, strategy, leadership, responsibility, culture).
- **Controls** (Policies, procedures, frameworks).
- **Governance** (New technology implementations, DPIAs, Care Certs, governance groups, assurance groups. risk register, Data Security Protection Toolkit, third party audit assurance, training).
- **Domain** (Identity Access Management, Active Directory (AD), access controls, privileged access management (PAM), JML, certificate management).
- **Data** (Network attached storage (NAS), file shares, auditing, labelling, data loss prevention (DLP), data destruction).
- **Endpoint Protection** (Anti-virus, EDR, XDR, enrolment and build process, device lifecycle, posture/features, device health, OS versions, policies/exclusions, documentation).
- **Security Patching** (Process, targets/aims, compliance).
- **Cloud** (Providers, footprint, backups, Identity Access Management (IAM), data storage, assurance, assessment, policies, resilience).
- **Physical Security** (Datacentres/Comms Rooms and cabinets).
- **Network** (Network access controls (NAC), boundary controls, virtualisation, Wi-Fi, virtual private networks (VPNs), web application firewalls (WAFs), monitoring, legacy systems, telephony).
- **People, Toolsets and Technologies** (All related systems in use and their suitability, use of freely available tools, investment in existing cyber security staff).
- **Business Continuity Planning** (Organisational, Information technology and cyber security specific, technical, and documented, succession planning., backups).
- **Cyber Incident Response** (Process and procedures, documented approach, playbooks, escalation).

3. Why Cloud21

- **Independent and vendor-neutral** - advice focused solely on your requirements
- **Healthcare specialists** - extensive experience with NHS digital maturity frameworks and standards
- **Proven delivery** - supporting 200+ NHS trusts and public sector organisations
- **Quality assured** - ISO27001, ISO9001, ISO20000-1 and Cyber Essentials Plus accredited
- **Cost-effective** - identifying savings through contract optimization and licensing compliance

4. Pricing

We offer pricing that is engagement dependant, please do contact us to discuss but also please see our published rate card.