CAPABILITY OVERVIEW

Softcat

CYBER SECURITY
IN INTEGRATED CARE & GOVERNMENT

With healthcare systems more interconnected than ever and widespread use of medical IoT devices increasing complexity and attack surfaces, it's crucial to view cyber security as more than just compliance.

At Softcat, we focus not only on the fundamentals required by regulations, but also on understanding your entire organisation's landscape and identifying any gaps that could create problems in the future.

Softcat's Public Sector team have worked with NHS organisations for over 12 years and understand the importance of cyber security resilience, from protecting patient information, maintaining medical records' integrity, and ensuring critical medical devices function without interruption, to create a secure and safe environment for your patients and staff.

SOFTCAT ICG CYBER RESILIENCE FRAMEWORK

With so many different objectives at play when it comes to building out an effective strategy for cyber resiliency in your organisation, it can be challenging to see how they cross over. We've developed our ICG Cyber Resilience framework to support you in meeting your tactical, operational and strategic goals.

HOW TO IMPROVE CYBER RESILIENCE | **WHAT ARE THE DESIRED OUTCOMES?**

TACTICAL
- Secure your personal date
- Secure your Hybrid Platforms
- Secure your staff & clinicians
- Secure your Network

OPERATIONAL
- Economies of Scale & Collaboration across ICB procurement
- Reduced Cyber Risk & Improved Digital Maturity
- Collaboration of Threat Intelligence across ICB's
- Collaboration on more secure data sharing across regions

STRATEGIC
- Compliance: DSPT, CAF, Cyber Essentials, NIST

Tactical – involves practical steps using cyber security technology, tools and services to improve your cyber resilience, focussing on short to medium term outcomes.

Operational – the operational efficiencies that improved cyber resiliency can drive can also support the journey to achieving strategic goals in a single organisation or at an Integrated Care Board level.

Strategic – longer term goals that tactical and operational outcomes contribute towards and will support the long term success of your organisation from a cyber security perspective and beyond.

SECURE YOUR DATA

Securing cross-region collaboration: protecting personal identifiable data (PID) and personal data.

Facilitating secure collaboration among healthcare trusts across regions requires the ability to safeguard both PID and personal data effectively.

Softcat recommends:

IMPLEMENTING ROBUST SECURITY MEASURES FOR OFFICE 365
Treat your SaaS services, including M365, like your on-premise datacentre and ensure you can see all connections to and from them, including the context around those connections and the use of any SaaS platforms you weren't aware of.

MAINTAIN THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF DATA
Implement Data Security Posture Management to gain visibility of where sensitive data is, who has access, how it has been used, and what the security posture of the data stored is.

IMPLEMENTING A ROBUST DATA LOSS PREVENTION STRATEGY
Mitigate against accidental and targeted data loss by enforcing security policy for data at rest (encryption, classification), data in use (authentication and access), and data in motion (encryption, classification).

UTILISING THE RIGHT APPROACH TO DATA GOVERNANCE
Classification of data provides additional layers of security to data, ensuring that it can only be accessed by the right people and organisations, as well as maintaining data integrity.

MAINTAIN VISIBILITY OVER THE DATA IN YOUR CLOUD PLATFORMS
Softcat can help you gain full visibility of what is happening within your multi-cloud environment to ensure compliance and security through assessments and our Cloud Fundamentals which provides access to our industry leading Cloud Management Platform.

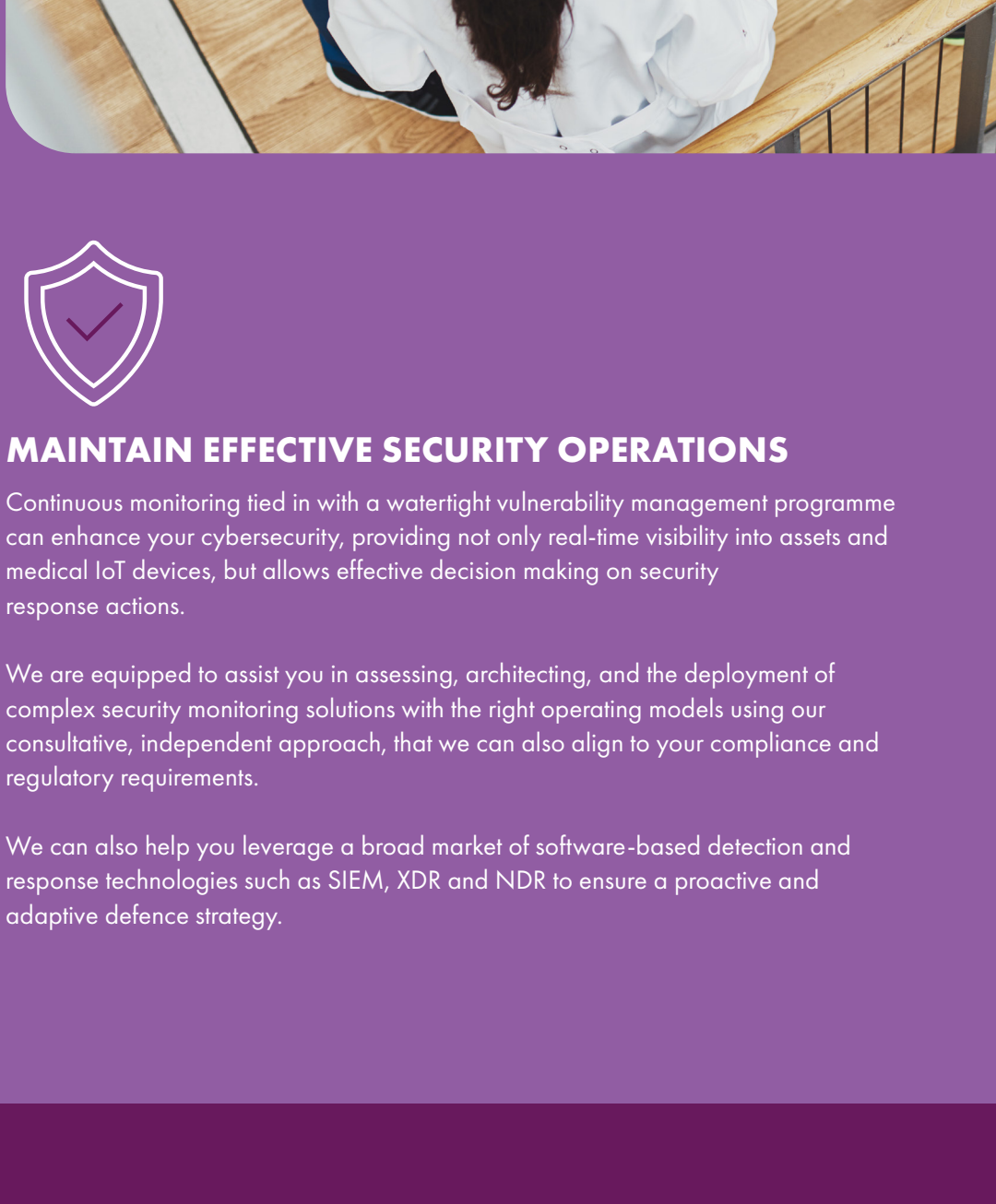
Softcat can consult and advise on security-specific monitoring and assurance tools your cloud, multi-cloud, hybrid and SaaS environments.

LEARN MORE ABOUT HOW WE CAN SUPPORT YOUR CLOUD PLATFORMS:

Taking action to prioritise your data security, you not only promote valuable research endeavours but also establish a foundation to safeguard patient identities and sensitive information, ensuring the integrity and privacy of your critical healthcare data.

FIND OUT MORE

SECURE YOUR NETWORK



Ensuring a proactive approach to threats on the network providing full visibility of assets and medical IOT devices.

Full visibility and a proactive approach to the security of network assets and medical IoT devices is vital for safeguarding patient data and maintaining the integrity of critical medical systems; improving reliability and mitigating against potential cyber threats for the continuous and secure delivery of healthcare services.

Softcat recommends:

UNDERSTAND WHAT DEVICES YOU HAVE IN YOUR ESTATE, INCLUDING MEDICAL IOT DEVICES
You can't protect what you can't see so it's crucial to take a modernised approach to asset management, utilising tools to automatically discover and document both network and medical IoT assets, providing comprehensive visibility into known and unknown assets.

Clinical devices and their interactions with IT can be unique, and at a bare minimum, it is vital that we understand when they last connected to the network and the level of firmware or software they are operating. This enable a holistic vulnerability and patch management programme, with an understanding of assets and their underlying context.

EFFECTIVE VULNERABILITY AND PATCH MANAGEMENT
Regularly scanning for vulnerabilities in critical Care certificates, using specialised tools for prioritised detection, and implementing strong patch management can ensure the swift and effective resolution of identified vulnerabilities, improving the network's overall security posture and safeguarding your medical IoT devices from potential exploits.

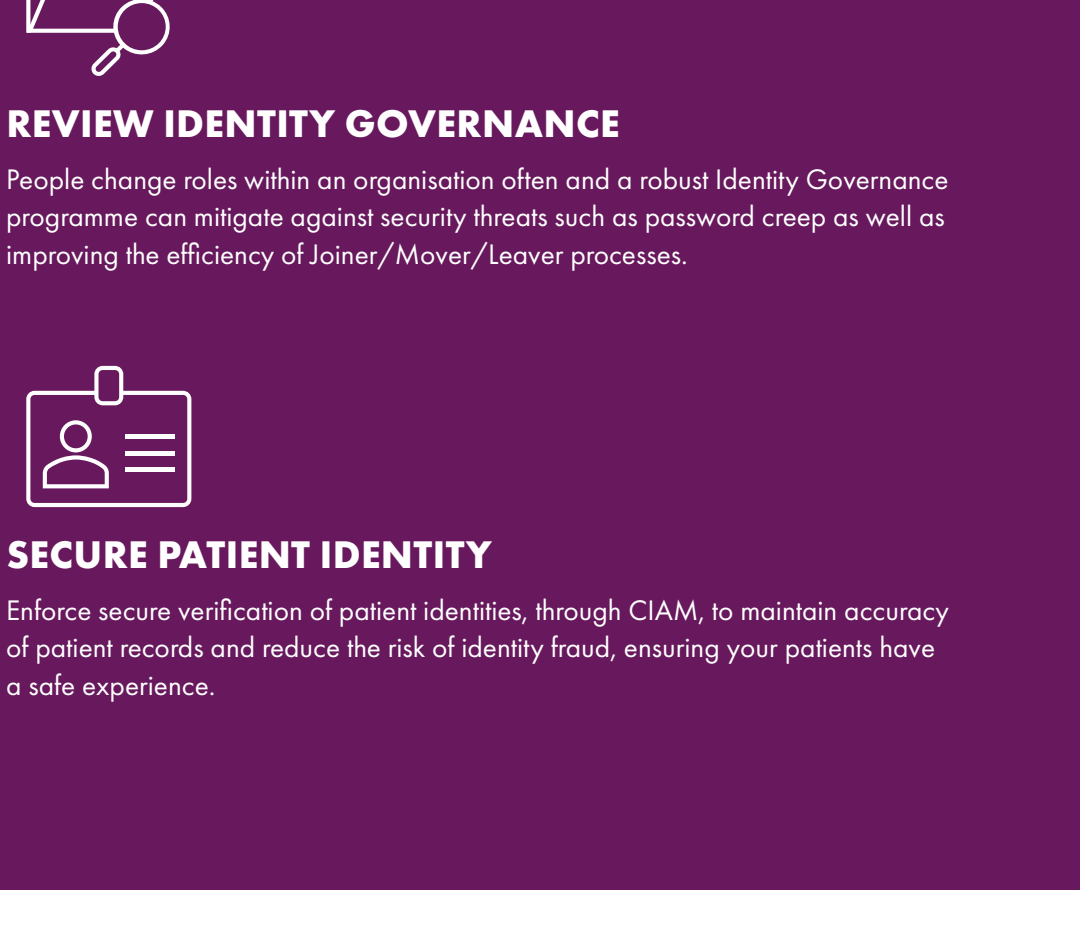
Our Vulnerability Management service helps you manage your vulnerabilities with a risk-based approach, using threat intelligence and machine learning.

MAINTAIN EFFECTIVE SECURITY OPERATIONS
Continuous monitoring tied in with a watertight vulnerability management programme can enhance your cybersecurity, providing not only real-time visibility into assets and medical IoT devices, but allows effective decision making on security response actions.

We are equipped to assist you in assessing, architecting, and the deployment of complex security monitoring solutions with the right operating models using our consultative, independent approach, that we can also align to your compliance and regulatory requirements.

We can also help you leverage a broad market of software-based detection and response technologies such as SIEM, XDR and NDR to ensure a proactive and adaptive defence strategy.

SECURE YOUR PEOPLE



Facilitating secure collaboration for a diverse workforce across regions.

It is crucial to enable safe collaboration of the workforce when working across regions as well as securing hybrid workers, clinicians, contractors, and social workers, among others, to protect their professional identity and maintain appropriate access to critical resources.

Softcat recommends:

IMPLEMENT STRONG IDENTITY ACCESS CONTROLS AND POLICY
Provide simple access to productivity and clinical applications through a single solution, eliminating the need for multiple passwords.

Prevent unauthorised access to sensitive patient data and enhance security around medication dispensing and management.

REVIEW IDENTITY GOVERNANCE
People change roles within an organisation often and a robust Identity Governance programme can mitigate against security threats such as password creep as well as improving the efficiency of Joiner/Mover/Leaver processes.

MONITOR AND CONTROL THE ACCESS OF PRIVILEGED USERS
Effective tooling is recommended to limit common bad practices such as password sharing, or storing admin passwords in an unsecure manner.

Manage and monitor access for temporary and contract workers coming in and out of your organisation.

SECURE PATIENT IDENTITY
Enforce secure verification of patient identities, through CIAM, to maintain accuracy of patient records and reduce the risk of identity fraud, ensuring your patients have a safe experience.

SECURE YOUR PLATFORMS

Securing investments made into your Hybrid Environments.

As more and more data and systems move to public cloud, it is critical for NHS organisations to understand what can and can't be deployed in cloud.

We can work with you to ensure your cloud workloads are secured by extending the security controls that are in place for on-premises infrastructure, and legacy or medical systems that cannot be brought up to date through patching, or cannot be deployed in the cloud are secured appropriately.

Softcat recommends:

ENFORCING PROTECTING YOUR CLOUD WORKLOADS, AS YOU WOULD ON-PREMISE
Implementing Cloud Workload Protection ensures monitoring and securing diverse cloud workloads, safeguarding sensitive healthcare data with restricted access.

Understanding the shared responsibility model of cloud.

You and cloud service providers (CSPs) both have security responsibilities. CSPs handle cloud infrastructure security while you're accountable for securing your data, applications, and workloads.

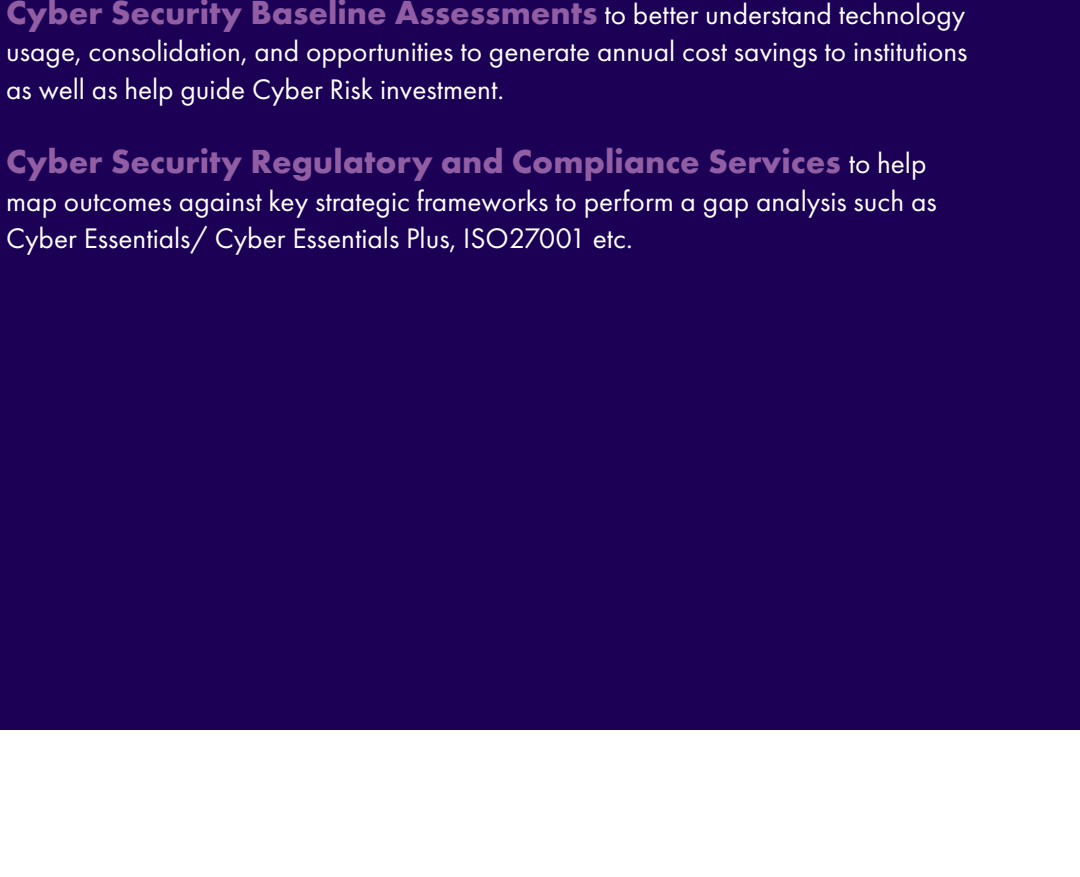
We can help you understand your shared responsibilities with your CSP. This way, you'll know what you need to take responsibility for and what your CSP takes care of.

PROTECTING MEDICAL IOT DEVICES
Utilise specialist tooling to protect medical devices that are not protected by traditional endpoint security solutions or patch management

PROTECTING YOUR LEGACY SYSTEMS THROUGH REGULAR PATCHING, VULNERABILITY MONITORING, AND UPDATES WHERE POSSIBLE
Employing intrusion detection systems and other security measures can help mitigate the risk of exploitation for legacy systems.

SECURE YOUR HYBRID PLATFORMS SO YOUR ORGANISATION IS PREPARED AS AND WHEN DISASTER RECOVERY IS NEEDED TO MAINTAIN BUSINESS CONTINUITY
Implement monitoring and alerting, and observability solutions to track the security and performance of both cloud services and on premises infrastructure. Real-time issue detection enables prompt responses, strengthening security and compliance during incidents.

COMPLIANCE & REGULATIONS



In order to drive your organisation towards your strategic goals, it's crucial to adopt a proactive cybersecurity approach to comply with DSPT, Cyber Assurance Framework, NIST cyber security framework, and CE+.

This safeguards patient information, ensures data integrity, and mitigates cyber threats, aligning with regulatory requirements for patient confidentiality.

It also establishes a strong cybersecurity foundation, enhancing strategic outcomes and fostering trust among patients and stakeholders.

Softcat can support you through this journey, whether it's in an advisory capacity, through our architecture and implementation capabilities, or across our support and managed services.

Key Services we can offer:

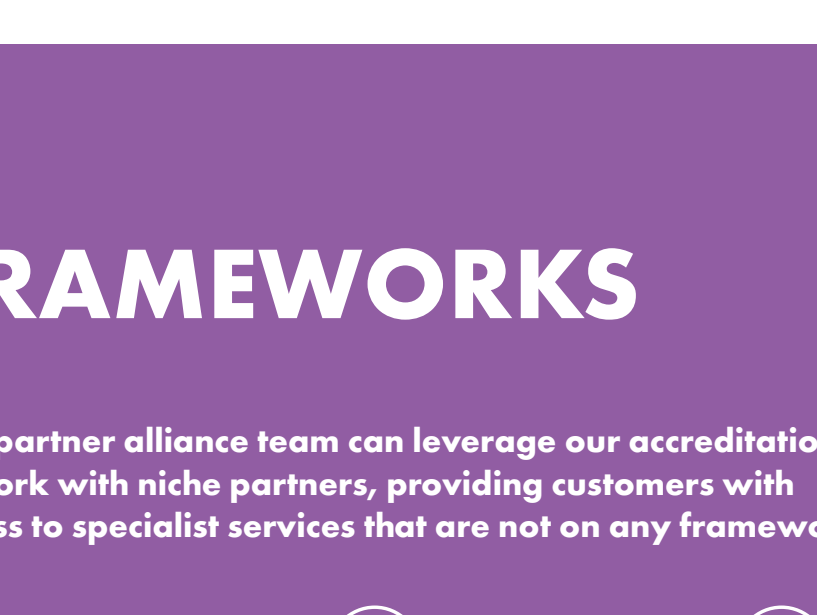
Managed Security Services
- **Managed SIEM Service** – Reduces your cyber risk by monitoring and detecting security threats, enabling you to respond quickly without disrupting services with guidance from our cyber analysts.
- **Managed Sentinel Service** – Helps you proactively defend yourself against threats and breaches by combining the threat protection, security intelligence and automation of the Sentinel security platform with expert monitoring and management by Softcat's Security Operation Centre.
- **Managed Firewall Service** - Provides continuous monitoring, updates, and expert technical support, reducing your cyber risks and protecting data by applying security best practices and swiftly addressing security incidents while easing the burden on your security team.

Cyber Security Baseline Assessments to better understand technology usage, consolidation, and opportunities to generate annual cost savings to institutions as well as help guide Cyber Risk investment.

Cyber Security Regulatory and Compliance Services to help map outcomes against key strategic frameworks to perform a gap analysis such as Cyber Essentials/ Cyber Essentials Plus, ISO27001 etc.

WHERE WE HAVE DONE THIS BEFORE:

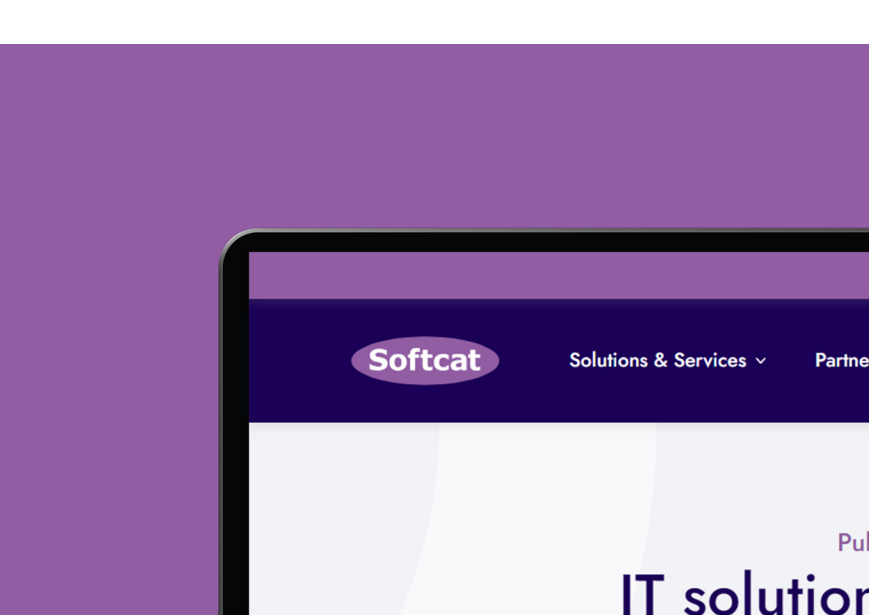
Durham County Council | NHS County Durham and Darlington NHS Foundation Trust



See how we delivered enhanced protection and capabilities for County Durham and Darlington NHS with a cutting-edge McAfee security solution.

READ MORE

NHS Oxford Health NHS Foundation Trust



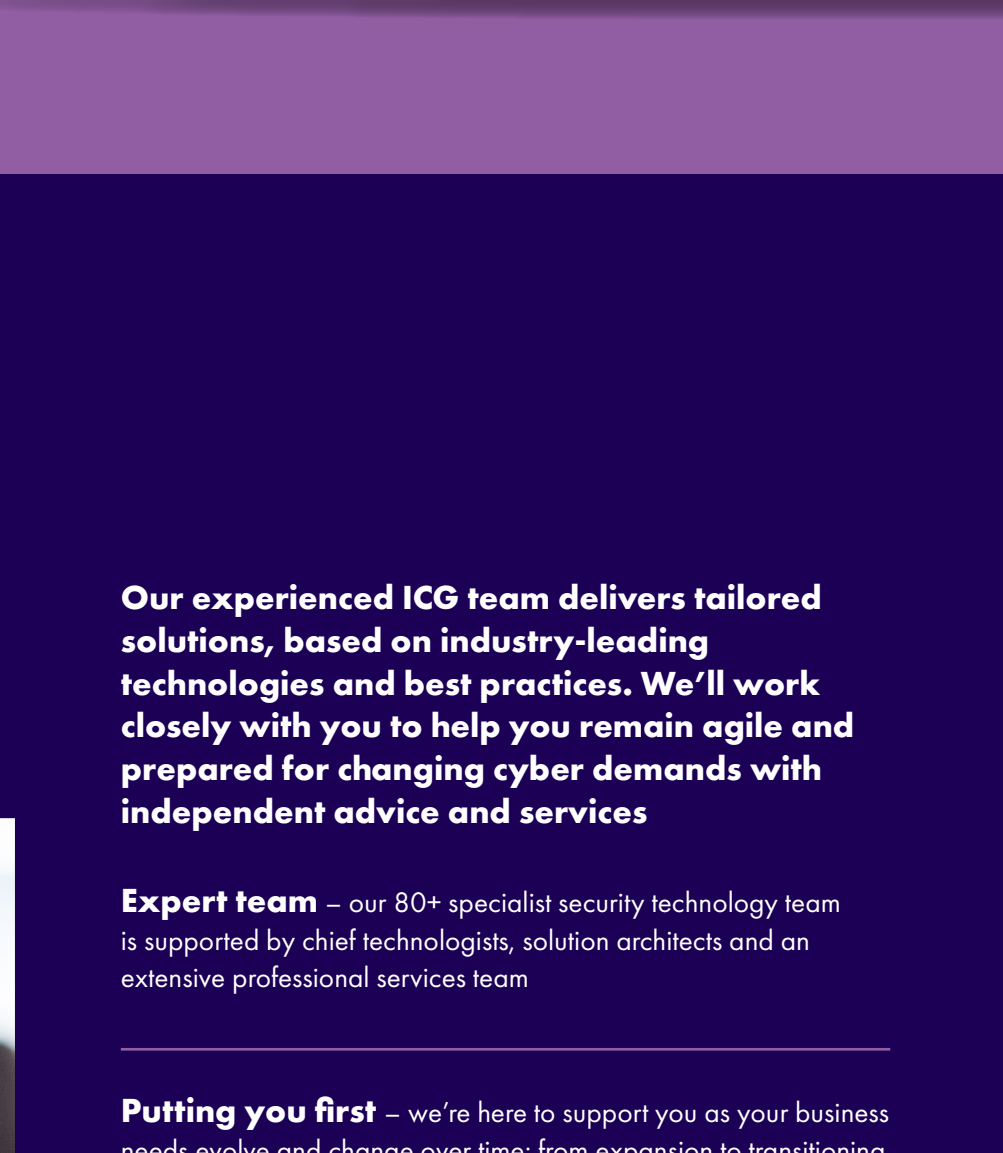
Discover how we harnessed the power of Mimecast to safeguard systems and staff – and reduce overall security issues – at Oxford Health.

READ MORE

FRAMEWORKS

Our partner alliance team can leverage our accreditations to work with niche partners, providing customers with access to specialist services that are not on any framework.

- **RM6098** CCS Technology Products & Associated Services 2
- **RM3764.3** CCS Cyber Security Services 3 (DPS)
- **NOE CPC** Total Technology Solutions
- **NHS SBS** Cyber Security Services
- **NHS SBS** Digital Workplace Solutions
- **KCS** Software Products & Associated Services
- **Health Trust Europe** ICT Solutions 3
- **META Procurement** IT Reseller



WHY SOFTCAT?

Our experienced ICG team delivers tailored solutions, based on industry-leading technologies and best practices. We'll work closely with you to help you remain agile and prepared for changing cyber demands with independent advice and services

Expert team – our 80+ specialist security technology team is supported by chief technologists, solution architects and an extensive professional services team

Putting you first – we're here to support you as your business needs evolve and change over time; from expansion to transitioning to the cloud, our services will adapt to suit you

Industry best practice – we keep up to date with the threat landscape, sharing a view of industry best knowledge, recent cyber threats, and recommended patches.

Top tier vendors – by working with innovative, industry-leading vendors, we're able to deliver best of breed, not best of brand; we offer bespoke solutions that are right for you

Holistic approach – by understanding each customer's unique needs, we're able to adopt a more holistic approach to business intelligence, powered by our transformation framework.

TAKE THE NEXT STEP

If you would like to find out more about how Softcat can support you on your cyber security journey, please contact your Softcat Account Manager today.

Copyright © Softcat 2024

Softcat