CASE STUDY

MLCSU and Osirium Automation

How Midlands and Lancashire Commissioning Support Unit transform IT service delivery through automation

OSIRIUM

NHS
Midlands and Lancashire
Commissioning Support Unit

Midlands and Lancashire Commissioning Support Unit and Osirium Automation

The Challenge

The NHS Midlands and Lancashire Commissioning Support Unit (MLCSU) provides wide-ranging IT support services to Integrated Care Systems (ICS) groups across the Midlands, Lancashire and North-West England. Unlike Acute Trusts, which typically focus on a few large sites (usually hospitals), primary care is much more diverse. There are around 8,000 GP practices in the UK, many operating across multiple sites. This fragmentation leads to a wide range of technology, sites spread over a wide area, and surgeries with small teams with little or no IT skills. MLCSU provides a broad range of services to approximately 200 organisations and their services range from desktop deployment and clinical systems to Cyber Security.

A fundamental requirement for cyber security in the NHS is the Data Security and Protection (DSP) standards set by NHS Digital. MLCSU helps its clients conform and show conformity with DSP. A vital element of the service is using **ITHealth's Assurance Dashboard,** which provides a comprehensive inventory of an NHS organisation's IT estate, revealing the security state of IT systems, software and user accounts, and highlighting potential vulnerabilities.

DSP places specific requirements on healthcare organisations around user and administrator accounts management. Administrator accounts are particularly sensitive due to their elevated privileges when used with IT systems. These accounts can be used to exfiltrate sensitive patient data, interrupt services, or make it easy for ransomware attacks to strike (the NHS was one of the earliest high-profile ransomware victims when WannaCry struck in 2017). A significant part of the **DSP requirements** involves monitoring and managing how user accounts are created, maintained, and removed when no longer needed, especially those with elevated privileges.

When a new team member joins a practice team, the traditional process is to send a request to an IT Service Desk to provision the user's accounts, which may be in 4 or 5 systems, including Active Directory (AD), Office365, EMIS, and/or clinical systems. This places significant demand on the Service Desk and may introduce a delay before that new team member can start work.

When someone leaves, the reverse must happen: all those accounts must be removed quickly which is not always possible due to service demand spikes.

NHS
Midlands and Lancashire
Commissioning Support Unit

Company:	Midlands and Lancashire Commissioning Support Unit
Location:	UK
Industry:	Healthcare
Solution:	Osirium Automation and the ITHealth Assurance Dashboard

Challenge

- Address NHS DSPT cyber security requirements
- Transform IT Service Delivery for GP practices
- Reduce the load on the IT Service Desk

Solution

- Use Osirium Automation to delegate common user account management functions securely
- Use Osirium Privileged Access Management to increase the level of security on servers and domain controllers

> "A major transformation is possible if you can enable end-users to take care of account management tasks for themselves.

Glenn Hollywell, Senior Project Manager

In some situations, if a user needed an elevated account, a manual process would be used to create a temporary login and then remove the account when no longer needed. Across the integrated care system group, such account management tasks are happening every day. It's often an urgent demand for the IT Service Desk which impacts productivity at the GP Practice and opens potential security risks.

The Solution

MLCSU were looking for improvements in how IT systems are managed. Although there has been much focus on managing acute care trusts, the challenges of highly dispersed GP Practices remain. Glenn Hollywell, Senior Project Manager in the MLCSU Cyber Security Team, said, "It's about operational change, transforming how the end-user accesses services.

"A major transformation is possible if you can enable end-users to take care of account management tasks for themselves. It has to be done securely, of course, but it would allow us to free up Service Desk staff and could have a massive impact. We think automation will allow changes to be made very safely and reduce risk."

MLCSU drew up a series of functional and operational requirements and considered several potential vendors. MLCSU had a strong relationship with ITHealth through its Assurance Dashboard solution, and ITHealth introduced Osirium as a potential partner for automation and privileged access management (PAM).

Having reviewed **Osirium Automation (built on the company's Privileged Process Automation (PPA) platform)** in the context of the functional requirements, MLCSU moved forward with a Proof of Concept (PoC) with Hall Green Health in the Birmingham and Solihull (BSOL) CCG, the largest CCG in the country. The PoC allowed admin staff at Hall Green to perform standard account management functions such as create, enable, disable, and unlock accounts. The PoC identified ten tasks to test with: six were provided with PPA "out of the box," and Osirium helped create the remaining four within a week.

Feedback from the PoC was positive from the start. The users were happy and, in fact, reported missing the service when the PoC was completed, and the service taken down temporarily. The Osirium style of automation, which guides a non-specialist user through the process of making a change, ensures that admin credentials are protected, and the user can't do anything they shouldn't.

During the PoC, Hall Green found Osirium Automation extremely helpful for everyday tasks and was relieved when licenses were extended to ensure they could continue working until the formal rollout started.

Glenn continued, "Hall Green has been extremely enthusiastic and helping with demos for other practices and trusts. We're currently in the planning process for the rollout of Automation to over 200 sites within BSOL and then out across the MLCSU community. Our new challenge is that everyone wants it and wants it now!"

He continued, "We're currently evaluating whether to roll out using a cloud-based PPA environment on on-premises servers. Functionally there's no difference, but operational costs are important."

In parallel to the Automation rollout, MLCSU is deploying Osirium PAM to their data centre. They will be using PAM to protect access to shared servers and services. These controls are important for DSP and were highlighted by the National Cyber Security Centre (NCSC) as a priority, especially to protect backup systems.

Looking Forward

Working with ITHealth has been a very positive and productive project. “We’ve worked with ITHealth for two years, and it’s exciting that they’ve brought Osirium into the partnership. These products are really, really exciting for our technology roadmap.” Glenn also added, “It’s been a really good relationship with Osirium, and nothing was too much trouble. They’ve been very responsive and supportive.“

> It’s been a really good relationship with Osirium, and nothing was too much trouble. They’ve been very responsive and supportive.

Glenn Hollywell, Senior Project Manager

The initial engagement at BSOL is only the start. Glenn said, “I think automation will be a major transformational project, not just across MLCSU but also across the NHS nationally. We want to transform how we deliver IT services. In a world where end-users are used to the “Amazon experience” of self-service account management, they’re looking for the same in their work environment.”

> I think automation will be a major transformational project, not just across MLCSU but also across the NHS nationally.

Glenn Hollywell, Senior Project Manager

The provision of self-service solutions for end users at remote sites with little or no IT support occurs across many industries, including retail, hotels, and finance. Digital transformation through secure automation and empowering end-users will be a key aspect of many organisations’ technology roadmaps.

About Osirium

Osirium is the UK's innovator in Privileged Access Management. Founded in 2008 and with its HQ in the UK, near Reading, Osirium's management team has been helping thousands of organisations over the past 25 years protect and transform their IT security services.

The Osirium team have intelligently combined the latest generation of Cyber-Security and Automation technology to create the world's first, built-for-purpose, Privileged Protection and Task Automation solution.

Tried and tested by some of the world's biggest brands and public-sector bodies, Osirium helps organisations drive down Business Risks, Operational Costs and meet IT Compliance.

OSIRIUM

Theale Court, 11-13 High Street, Theale, Reading, Berkshire, RG7 5AH
+44 (0) 118 324 2444, info@osirium.com, **osirium.com**