Osirium Case Study

Company: NHS authority
Location: Scotland, UK
Industry: Healthcare
Osirium solution: Osirium PAM

Challenge

- Comply with government regulations
- Prevent the next WannaCry, and be ready for recovery following an attack
- Improve visibility and control of third-party suppliers

Solution

- Control internal and third-party supplier access to IT systems with Osirium PAM

The Challenge

NHS Lanarkshire is the third largest NHS authority in Scotland and cares for over 655,000 people. With three main acute care sites, 15 community hospitals, over 90 GP surgeries, and more than 14,500 staff, the trust's IT department is responsible for a complex and disparate IT estate. With over 14,000 Windows endpoints, 900+ servers, over 200 admin accounts, and more than 300 service accounts across their systems, it was impossible to safely manage all accounts and devices manually.

Following the WannaCry attack of 2017, the Scottish Government published its Public Sector Action Plan for Cyber Security that included a range of new standards which all critical infrastructure providers were required to meet, including Cyber Essentials accreditation, and NCSC baseline standards. NHS Lanarkshire were nominated as a "Cyber Catalyst" for the NHS in Scotland to pioneer the new requirements.

A key improvement was to be in privileged access for both internal staff and the many third-party suppliers that have access to internal systems. Lack of visibility and control of supplier access using these powerful accounts was identified as a significant risk.

> *"Selecting Osirium PAM wasn't just about the robustness of the solution and the competitive price. It was also the professionalism of their engagement and the excellence of their support."*

The Approach Taken

Having identified the need, especially to control and have visibility of the supply chain, NHS Lanarkshire created a plan to implement Privileged Access Management (PAM). From peer recommendations and research such as vendor webinars, NHS Lanarkshire created a short list of three PAM solutions which were trialed in a series of Proof of Concept (PoC) tests.

Following the PoCs, each solution was evaluated in terms of capability and cost analysis. Mark Grant, IT Infrastructure Operations Manager at NHS Lanarkshire summarised, "Selecting Osirium PAM wasn't just about the robustness of the solution and the competitive price. It was also the professionalism of their engagement and the excellence of their support."

NHS Lanarkshire took a phased approach to implementation of PAM starting with the third-party suppliers closest to the IT team for easier access and engagement, new suppliers, and key internal staff, especially Domain Admins and those with heightened privileges.

Because of their pivotal role in the IT infrastructure, the first wave also prioritised the systems to be protected with Domain Controllers, backup systems, SQL clusters, converged infrastructure and management systems

Benefits and Next Steps

NHS Lanarkshire has realised a significant improvement in visibility and management using Osirium PAM's Session Recording. Combined with integration into their SIEM tools, the IT team now have visibility into who is accessing which systems, when and what they are doing.

"We're now looking to delegate more IT operations to users," added Mark Grant. "For example, because we use PAM to protect or our Veeam backup systems, we've been able to safely allow users to restore their own backups without relying on the backup team."

Looking forward, NHS Lanarkshire plans to extend this ability to delegate work by using automation to allow GP practices to manage their own suppliers. They also intend to use automation with PAM to enable their service desk staff to assist users directly. From initial planning and implementation, the rollout continues.

> *"Osirium has helped us close the technology gap bringing control and oversight into an area where previously our only control was one of mutual trust."*