celerity

Royal Papworth Hospital
NHS Foundation Trust

Care Without Compromise: Transforming Cybersecurity

HEALTHCARE

The Challenge

One of the most prestigious trusts focusing on high-quality, personalised care, Royal Papworth Hospital NHS Foundation Trust processes vast amounts of sensitive patient data daily. The increasing complexity of cyber threats, coupled with stringent compliance requirements like DSPT and NHS Cyber Alerts, made enhancing their cybersecurity infrastructure an urgent priority.

The hospital needed to address:

- Lack of real-time threat monitoring.
- Limited in-house expertise in managing advanced security tools.
- Difficulty meeting NHS compliance deadlines.
- Need for a scalable, proactive solution to combat emerging threats.
- Lack of staffing to monitor systems 24\7\365.

The Solution

Celerity deployed its fully managed SIEM service, integrating seamlessly with Royal Papworth's existing infrastructure. The service provided real-time threat detection, advanced analytics, and continuous monitoring to ensure rapid response to potential threats.

Cybersecurity is a constant challenge, but with Celerity’s round-the-clock team of experts, the hospital has implemented another level of protection that will ensure an increased cyber defense response every day of the year.

Key Features

- 24/7/365 security monitoring by a dedicated SOC. This continuous vigilance helps detect and respond to threats more quickly.
- Automated vulnerability assessments and reporting.
- Tailored dashboards for NHS-specific compliance tracking.
- Threat intelligence feeds to stay ahead of evolving risks.
- SOC team worked with Royal Papworth Cyber analyst to ensure all required log sourceswere setup and imported correctly as per their requirements.

Strengthening Patient Care with Secure, Compliant, and Cost-Efficient Outcome

Enhanced Cybersecurity

Real-time monitoring led to the early detection of 120 threats within the first 2 months, reducing potential breaches.

Improved Compliance

Streamlined reporting helped the hospital meet DSPT and NHS Cyber Alert requirements efficiently.

Operational Efficiency

The IT team is saving [18 hours/month] by outsourcing SIEM management, allowingthem to focus on patient-centric projects.

Cost-Effective

Operating an in-house SOC requires heavy investment in skilled personnel, technology, and training. Outsourcing to Celerity reduces costs while providing expert protection through our established infrastructure and industry experience.

> *Following the success of the Managed SIEM deployment, we plan to continue to expand our cybersecurity measures further with the planned implementation of an improved Privileged Access Management (PAM) solution and further investment into improving our Network Detection and Response (NDR) capability, as well as looking into the Internet of things (IOT) solutions to cover any holes we many encounter with the introduction of newer technologies. The managed SIEM solution is helping as part of our hybrid approach to cybersecurity.*
>
> *We understand the evolving nature of Cyber threats, but this solution helps increase our support enabling sensitive data to be more secure, and compliance has improved.*

Dept Head of ICT Operations (infrastructure)

Royal Papworth Hospital NHS Foundation Trust

For more information or to discuss how our Managed SIEM can be tailored to meet your specific needs, please get in touch today.

@CelerityLimited
marketing@celerity-uk.com
celerity-uk.com

celerity