Case study ■ NHS Foundation Trust

Scaling detection and response to safeguard specialist patient care

In the face of unrelenting cyber threats, healthcare institutions must confront the dual challenge of protecting sensitive patient data while ensuring the uninterrupted delivery of critical services.

An NHS Foundation Trust, renowned for its global expertise in a highly specific field of medicine, recognised that its internal team needed additional support to maintain a resilient security posture. While the Trust benefited from the support of the NHS England National Cyber Security Operations Centre , selecting Socura as its partner for **Managed Detection and Response** (MDR) has enabled the Trust to successfully scale its defensive capabilities to proactively identify and shut down threats 24/7.

The continuous oversight provided by Socura MDR ensures cyber incidents are investigated and resolved within minutes, significantly increasing operational assurance and ensuring the Trust's information security meets the highest standards.

The security challenge

Operating across a large estate, this Trust provides highly specialised care. Any disruption to its services would not only delay life-altering treatments but also place immense pressure on the wider NHS network. Additionally, there was concern that cyber incidents could lead to the loss of ground-breaking research and damage the Trust's reputation for clinical and academic excellence.

The Trust's Information Security team, though highly skilled, functions as a multi-disciplinary unit responsible for a vast array of cyber security functions. Balancing such diverse responsibilities—including risk assessments, vulnerability management, and threat monitoring—was placing a heavy demand on their daily capacity.

Due to the team's workload, detecting and responding to threats at all hours of the day was proving especially (cont.) challenging. While the Trust benefited from the support of

Main security concerns

- **Protecting patient data, research and critical IT & medical systems**
- **Detecting and responding to threats at all times of the day**
- **Keeping pace with new attack tactics and techniques**
- **Meeting the latest industry information security requirements**

The security challenge (cont.)

the NHS England CSOC, the responsibility to attend to and investigate all alerts generated by its security controls put extra pressure on its internal staff—who struggled to maintain a consistent level of coverage while also keeping pace with other responsibilities.

Also mindful of the need to meet the requirements of national standards such as the NHS Data Security and Protection Toolkit (DSPT) and NCSC Cyber Assessment Framework (CAF), the Trust wanted to ensure it could evidence improvements to its security posture and take steps to be even more proactive in its approach to managing risks.

The solution

To address the challenges of continuously detecting and responding to threats, the Trust appointed Socura as its partner for MDR. Socura's team of analysts and engineers function as a 'security operations arm' of the Trust, working alongside its internal team to ensure coverage 24/7.

Socura MDR integrates seamlessly with the Trust's security controls and is responsible for not only monitoring and responding to alerts they generate but also for keeping them optimised based on the latest threat intelligence. Additionally, the service ingests, investigates, and responds to alerts generated by the NHS England National CSOC.

Crucially, Socura's analysts contain and disrupt threats by initiating pre-approved actions such as isolating endpoints and resetting user accounts—providing response capabilities that the NHS England National CSOC does not offer. The Socura team also performs regular threat hunts to uncover evidence of unknown attacks that controls may have missed.

Why Socura MDR

CREST certification

As a CREST-certified provider for Security Operations, Socura was able to demonstrate that its processes met the highest technical standards. Additional credentials—including a 'Standards Exceeded' DSPT assessment—also validated Socura as a trusted supply chain partner.

Technical approach

Socura demonstrated it could meet the Trust's technical needs by supporting a diverse range of security controls, seamlessly ingesting alerts from the NHS England National CSOC , and integrating directly with the Trust's IT Service Management system for a streamlined workflow.

Specialist expertise

The Trust required more than a service provider that simply triaged alerts. Socura's proficiency in both identifying and disrupting threats gave leadership the confidence that the partnership would significantly reduce the burden on their internal team. Socura's extensive experience working with other NHS trusts also demonstrated a deep understanding of the unique demands of working in a highly specialised environment.

Listing on G-Cloud

For streamlined procurement, the Trust sought a partner capable of transacting its services via G-Cloud—the government framework for cloud-based services.

> "The Socura team are experts in their field, so having them alongside us at all times gives us confidence that we can identify and respond to attacks early. Honestly, they help me to sleep better at night.

Head of Information Security
NHS Foundation Trust

SOCURA

hello@socura.co.uk
0800 640 4067
LinkedIn
Bluesky