South East Coast Ambulance Service significantly improves NHS Digital Cyber Alert management and takes greater control of its IT

ITHealth

The global ransomware attack, WannaCry, although not targeted at the NHS impacted the provision of services to patients. It highlighted many areas for security improvement both within individual NHS organisations and across the system as a whole - increasing the need for Trusts to demonstrate compliance to the sector-specific Cyber Alert (formerly 'CareCERT') advisories, as released by NHS Digital. Read how South East Coast Ambulance Service improved its Cyber Alert response, along with other security processes, through implementation of the ITHealth Assurance Dashboard.

Customer

South East Coast Ambulance Service NHS Foundation Trust (SECAmb).

Type of NHS Organisation

Ambulance Trust.

ITHealth Customer Since

2020.

Challenge

Poorly managed Cyber Alerts (formerly CareCERTs), limited asset visibility and no real ownership of patching drove the need for a solution to help better manage vulnerabilities across the Trust's IT estate.

Solution

The ITHealth Assurance Dashboard Solution simplifies and improves security for the Trust through automated Cyber Alert reporting, cybersecurity asset intelligence, and reliable and easy-to-access support.

South East Coast Ambulance Service covers a geographical area of 3,600 square miles including Brighton & Hove, East Sussex, West Sussex, Kent, Surrey, and North East Hampshire. The Trust has over 4,000 staff working across 110 sites in Kent, Surrey and Sussex. Almost 90 per cent of the workforce is made up of operational staff – those caring for patients either face to face, or over the phone at the Trust's emergency dispatch centre where they receive 999 calls. As well as a 999 service, the Trust also provides the NHS 111 service across the region.

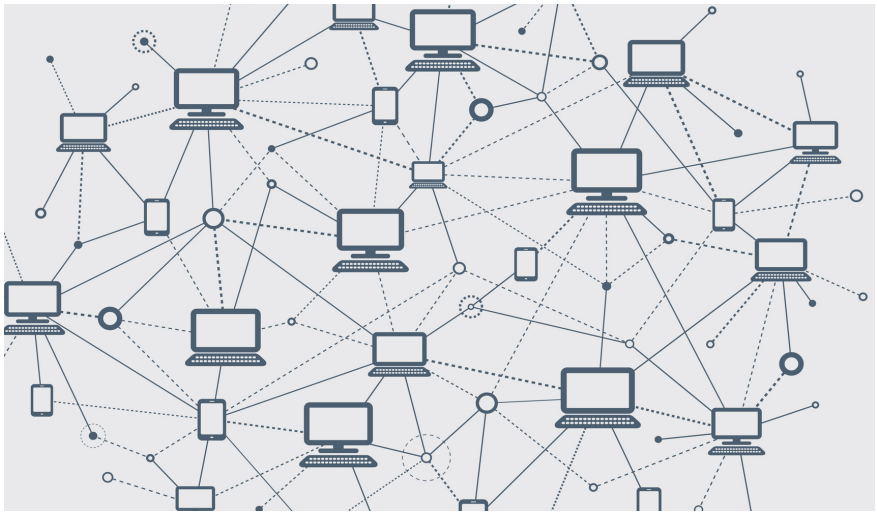
"In essence, we had no visibility of our assets – or, at least, not to the standard we wanted. We had no understanding as to what software was deployed on the assets or any real idea as to what patching vulnerabilities we had."

STEWART EDWARDS
IT Security Manager
South East Coast Service NHS Foundation Trust

The Challenge

WannaCry made clear the need for SECAmb to step up its efforts with cybersecurity so that every possible protection was being taken to defend against a future attack. SECAmb knew that it had limited visibility of its IT assets and that to protect something it must first know that it exists. It implemented Lansweeper, IT asset management software, to address this issue. 'How many endpoints do we have?' was soon no longer a mute question. Lansweeper also helped the Trust to identify what software required patching on the assets.

What the Trust lacked, however, was a robust process for its management of NHS Digital Cyber Alert advisories – and, naturally, NHS Digital was increasingly pushing Trusts to demonstrate compliance post WannaCry. According to Stewart Edwards, IT Security Manager at SECAmb, "The Trust's CareCERT process was poorly managed. CareCERTs would be manually logged in a spreadsheet and an email would be sent around the IT team to explain the issue to try and identify if the Trust was vulnerable to it. Often the answer would simply be, 'I'm not sure. I'll take a look.'" Resource constraints made it very difficult for the Trust's IT team to work out what remediation needed to be carried out and where.



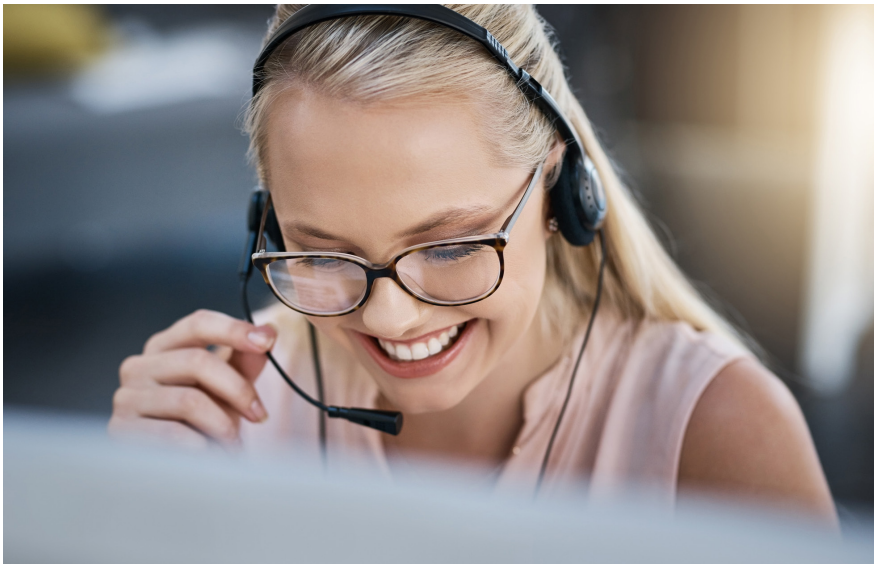
The Solution

SECAmb was aware that ITHealth was leveraging Lansweeper deep-scan technology and inventory data, and integrating it with other key data feeds to form a Dashboard designed specifically for NHS IT cybersecurity and compliance. The Trust requested a demonstration of the ITHealth Assurance Dashboard in February 2020 and could see immediately how its ability to automate CareCERT advisories would be beneficial. The following month, the Trust undertook a PoC (proof of concept) which lasted through to the end of May and by the summer, the Trust had fully procured the solution.

With the ITHealth Assurance Dashboard, the Trust's IT team could see at-a-glance the number of affected assets against a CareCERT and how this number of assets changed over time according to remediation efforts. "With ITHealth, it became very easy to understand our position with regards to CareCERTs", said Stewart.

Stewart explained how the Trust's digital team like how the ITHealth Assurance Dashboard also helps with patching verification and trending, understanding Windows 10 operating systems throughout the estate, software vulnerability management – including EOL software, plus how it gives a good view of Active Directory issues.

The Trust has been overwhelmingly impressed with the level of support that comes with the ITHealth solution. According to Stewart, "It's only a phone call away to get the support we need. We don't have to go through a call centre or be re-directed several times. What I love is the simplicity that ITHealth gives to answering our questions."



> "CareCERTs is the natural language of the NHS when it comes to IT. ITHealth reports against these. So, with ITHealth, it became very easy to turn around and show how compliant we are to CareCERTs and where affected assets remain outstanding."
>
> STEWART EDWARDS
> IT Security Manager, South East Coast Ambulance Services NHS FT

“

The ITHealth Dashboard was purchased initially purely for CareCERT management, though ITHealth support would have been a key purchasing driver if I knew then what I know now. For me, it’s as much about relationships as it is the product. ITHealth are always very responsive and straight talking, and we like that.”

STEWART EDWARDS, IT Security Manager, South East Coast Ambulance Service NHS Foundation Trust

The Results

Stewart highlighted particular benefits of the ITHealth Assurance Dashboard Solution for the Trust as follows:

▸ Increased security visibility

The ability to see key security information related to assets in a single place. Easy-to-understand reporting with issues clearly flagged and identified and the ability to monitor remediation over time.

▸ Ongoing assurance

Near real-time information means there’s always a genuine understanding of outstanding security issues and the Trust’s true security posture.

▸ Trustworthy and reliable support

Easy access to a team of highly skilled NHS IT specialists who remain on hand to assist with bespoke reports, queries and general cyber advice.

▸ Affordable, easy-to-use solution

According to Stewart: “It’s a good priced product, simple to use and relatively easily deployed”.

▸ Invaluable tool for the IT team

It’s a tool that is used daily to varying degrees throughout the IT team: the infrastructure team use it to validate that the patching they’ve done is correct, and the desktop team use it to identify non-compliant anomalies, e.g., unencrypted devices or uninstalled anti-virus, etc.

“I use the ITHealth Dashboard every day for around 30% of my day. In the main, I use it to delegate remediation tasks to the team. I also use it to provide assurance. I am very happy with how it helps me in my role as Security Manager for the Trust.” STEWART EDWARDS, IT Security Manager, South East Coast Ambulance Service NHS Foundation Trust

Find out more about the ITHealth Assurance Dashboard

Call: 0115 987 6339
Email: info@ithealth.co.uk
Visit: www.ithealth.co.uk

About ITHealth

ITHealth provide NHS organisations with proven and trusted IT security and access management solutions. Whether it’s providing fast, reliable, and secure access for NHS mobile workers, or finding effective ways to reduce threats while improving productivity and clinical workflows, ITHealth’s cost-effective solutions mean NHS systems and data are always secure, easy to access, and simple to manage.

Registered Office: ITHealth, 10 Churchill Park, Private Road, No 2, Colwick, Nottingham, NG4 2HF