Case Study:

NHS Foundation Trust

SOCURA

“Would I recommend Socura to other Trusts? Definitely, I have absolutely recommended them, and will again, they’re incredible.”

CYBER SECURITY MANAGER

NHS FOUNDATION TRUST

Overview

About the client

This NHS Trust is one of the top ranked and top performing hospital Trusts in the UK. With more than 6,000 staff, the Trust provides care to a community of over 1.5 million people.

In partnership with the hospital charity, the Trust builds and enhances clinical facilities to create an outstanding care environment for their patients and staff. Their growing portfolio of innovation projects and reputation in this field, has made them a national leader for innovation within the NHS.

This level of innovation, coupled with a rise in demand for digital services, meant that cyber security could no longer be seen as a bolt-on, but instead an imperative.

Background

The Trust decided it was time for a change, replacing their incumbent cyber partner with an in-house team, supplemented by an outsourced Security Operations Centre (SOC).

The SOC would deal with high and critical severity security incidents as they happen, allowing the in-house team to focus on the strategic work the Trust wanted to undertake to mature their cyber security posture.

Week 1 – May

- Requirements gathering
- Service design

Week 3 - May

- Deployment into client environment
- Tuning

Week 6 - June

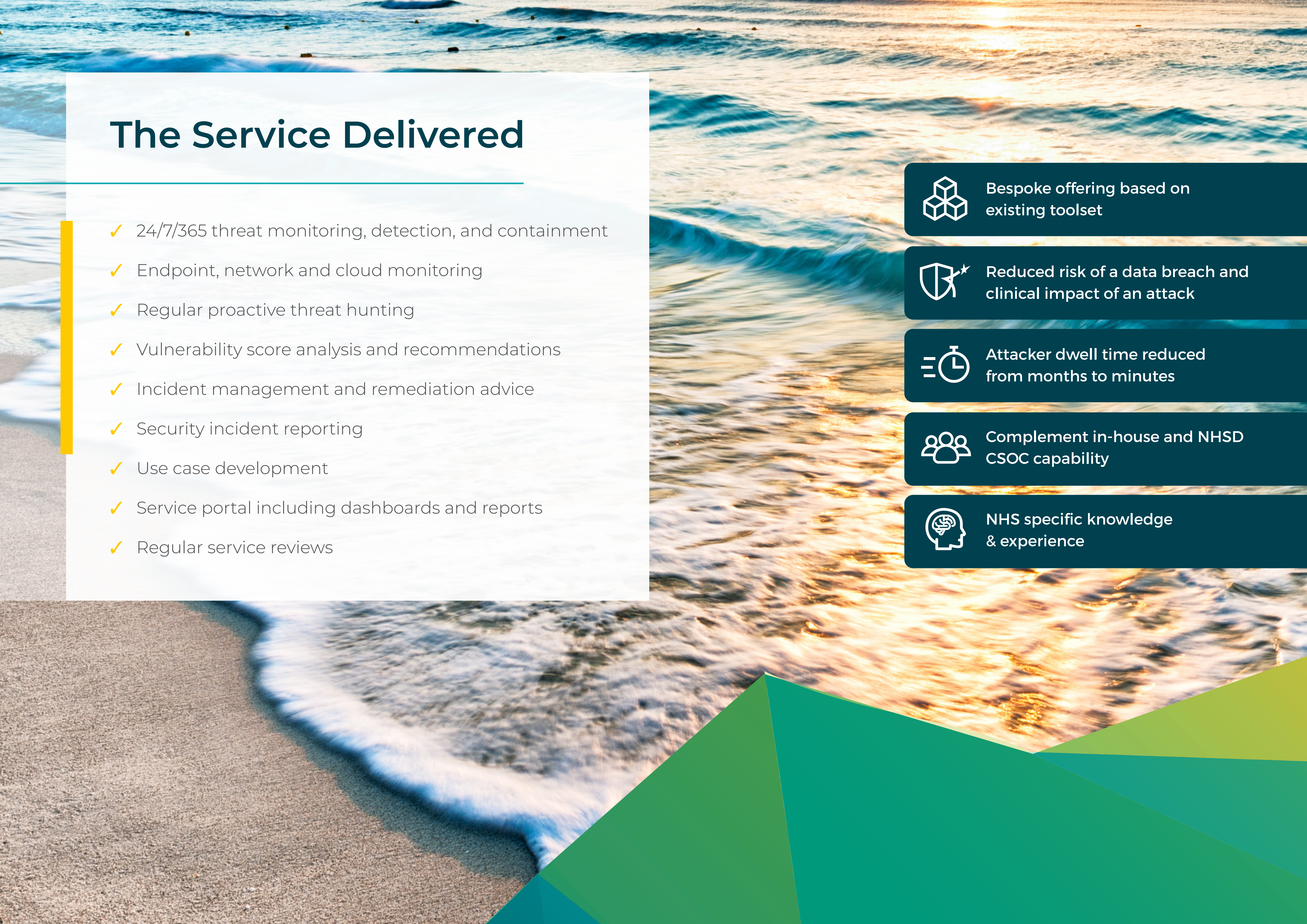
- Service acceptance meeting
- Go live

Aug - Nov

- Proving the value
- Stopped a number of ransomware attempts

December

- Service review
- Service uplifted to 24/7



The Service Delivered

- ✓ 24/7/365 threat monitoring, detection, and containment
- ✓ Endpoint, network and cloud monitoring
- ✓ Regular proactive threat hunting
- ✓ Vulnerability score analysis and recommendations
- ✓ Incident management and remediation advice
- ✓ Security incident reporting
- ✓ Use case development
- ✓ Service portal including dashboards and reports
- ✓ Regular service reviews

Bespoke offering based on existing toolset

Reduced risk of a data breach and clinical impact of an attack

Attacker dwell time reduced from months to minutes

Complement in-house and NHSD CSOC capability

NHS specific knowledge & experience

The Socura NHS service has been designed to meet NHS specific needs, allowing NHS organisations to benefit from world class protection delivered by highly skilled cyber security analysts, operating from a CREST accredited SOC.

We act as an extension of our clients own team, working with them in true partnership to augment their existing capability and providing 24/7 monitoring of their environment and the ability to act in minutes.

Crown
Commercial
Service
Supplier

CREST

The Socura Difference

Relationship with the National SOC

The NHSD CSOC provides excellent coverage using Microsoft's Defender for Endpoint (MDE – formerly ATP) and the Secure Boundary service. The CSOC can monitor devices within organisations that have deployed MDE and/or Secure Boundary.

Whilst the CSOC does have first-rate visibility, understanding the nuance of each organisation's IT infrastructure, key personnel, and specific operating processes, is very difficult when you consider that the NHS is made up of more than 200 Trusts and 1.2 million employees. This means that the CSOC can only detect certain activity and notify a Trust of a potential risk. It does not currently take immediate preventative response actions to contain threats.

Socura has built a service to complement the CSOC, increasing visibility within NHS organisations by integrating with key security tooling and delivering the capability to react quickly to these threats using our team of dedicated cyber security analysts.

Sharing the Journey

All too often, we see cyber businesses fail to fully deliver on the outcomes that initiated them. Over time, those mission-critical benefits promised can become diluted, delivering only partially on what was sought – and nothing pains us more.

We're driven by a belief in better, we're determined to deliver faster time to value, and we're dedicated to making smarter technology work for our clients – as it can, as it should, and as they and their stakeholders deserve. That's why we've architected a proven approach that follows a series of steps with mutual obligations, providing absolute clarity on what's possible and how it will be achieved.

Planning - The first phase began by bringing our two teams together. Collaborative workshops ensued, focussed on understanding the Trust's environment, business processes and key information assets. With this information, we jointly developed, and agreed on a deployment plan.

Deployment - Here the Socura team worked closely with the Trust to deploy the technology that would allow the monitoring, security telemetry, and pro-active action to take place (more on that later). Remote delivery of the technology equalled speed, with the deployment taking little over a week.

Tuning - With the mission-critical nature of an NHS Trust's work, it was vitally important that there was no adverse effect to their detection capability, or any other negative impact. So, after deployment, the Socura and Trust teams worked together to continue to tune the environment and develop the required rulesets.

Go live - It was then time to review the progress made in all of the previous stages, happily both teams agreed that the acceptance criteria was successfully met and we could move into a live service state under the defined SLAs. From here on out any security incidents could be raised with the Trust as they happen.

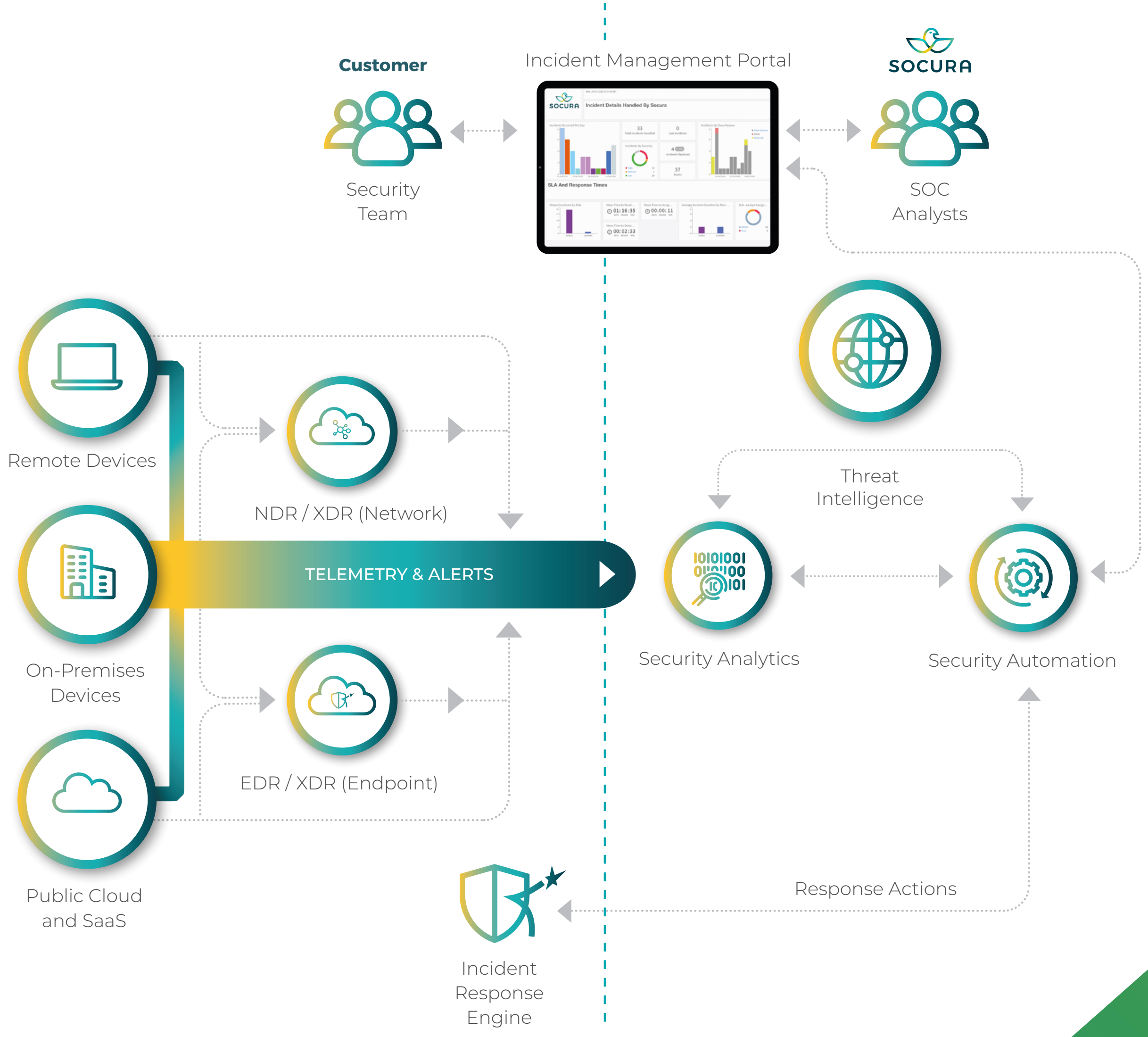
The Tech

The technical elements of Socura's Managed Detection and Response (MDR) service for the Trust include:

- ✓ Security Orchestration, Automation, and Response (SOAR)
- ✓ Cyber Threat Intelligence (CTI)
- ✓ SOC Visibility Triad

The SOC Visibility Triad describes the collection, correlation, and analysis of security telemetry and alerts from a combination of:

- ✓ Endpoint behaviour (Endpoint Detection and Response - EDR)
- ✓ Network behaviour (Network Detection and Response - NDR)
- ✓ Stitching together EDR + NDR + Identity + more (Extended Detection and Response – XDR)
- ✓ Security log sources (using Security Analytics or Security Information and Event Management - SIEM)



SOCURA INSIGHT

Telemetry should be collected from every asset/device, and across all parts of the IT infrastructure (including IaaS, PaaS, SaaS, endpoints, firewalls, email, directory services, DNS, Proxies, VPN, etc). Data should go back a year for maximum visibility.

More on this later ...

Being the Light

It's after go live that the Socura SOC team really shine. Agility is key here; we stay curious, open to new ideas and, continually looking for different and better ways to do things, and always proactive in solving problems if they arise.

Continually improving the Trust's cyber maturity

Every interaction between the Trust and the new managed SOC provides feedback on how things are working. A Socura Client Success Manager (CSM) works with the Trust to make sure these crucial learnings are developed into proper insights, and resulting actions that will continually improve the Trust's cyber resilience:

It's the role of the Socura CSM to act as a champion for the clients needs and objectives, working with the Trust to;

Review
security incidents

Analyse
data & trends

Measure
performance & SLAs

Identify
opportunities

We provide the Trust with dashboards, data and user-friendly metrics, and the Trust keeps us up to speed with any changes within their own operating environment. Areas such as automation, software features and the threat landscape are themselves in a constant state of development, so we ensure the Trust is kept up to speed there too.

The Google Cloud Chronicle Advantage

Socura has partnered with Google Cloud Chronicle to allow us to ingest all the security data that the Trust's systems generate, resulting in complete visibility across all data sources. This data is retained for 12 months, whilst remaining hot and searchable in milliseconds, meaning that we can also instantly and retroactively match newly discovered indicators of compromise against their entire historical telemetry dataset.

The elastic scale and speed of search that Google are renowned for can be brought to bear on the problem of hunting for malicious activity amongst vast amounts of data, whilst holding more data for longer, enabling us to see the bigger picture with no blind spots

[Read more about the Google Cloud Chronicle Advantage for the NHS >>]

Chronicle
part of Google Cloud

Making it Count

"Socura provides us with a really, really high-quality security service for operational needs, in terms of managing incidents like the day-to-day instance we get typically through ATP.

The Trust generally gets a handful of these every week or so and it's not just that Socura are really, really responsive to these, normally when something comes through, we'll get a response within a few minutes, but also they've got that background, they've got that insight, so they can advise us extremely well in terms of if it is a critical incident that needs immediate attention, and then my team and I have that background knowledge, allowing us to properly assess the threat, otherwise, it's very easy to get lots of alert fatigue.

Having that service gives us more reassurance that these incidents are going to be investigated in depth. Knowing that Socura has other NHS customers means they, and therefore we, are going to see all that's trending as well. It's so useful we've moved to Socura for out of hours support as well.

We get lots of regular reporting from Socura, which is very useful, really insightful. The regular service reviews also allow us to raise anything else we'd like to see, if there's any more statistics we'd like, if we want a follow up on specific incidents and that kind of thing, really, really useful. Would I recommend Socura to other Trusts? Definitely, I have absolutely recommended them, and will again, they're incredible."

CYBER SECURITY MANAGER
NHS FOUNDATION TRUST

> “Having the Socura service gives us that confidence that any incidents that do occur will be investigated in depth. Knowing that Socura has other NHS customers means they, and therefore we, are going to see all that’s trending too.”

CYBER SECURITY MANAGER

NHS FOUNDATION TRUST

SOCURA