Case Study:

UK Government Department

SOCURA

“The Socura team are knowledgeable and easy to work with. They take the time to understand our processes and systems, and provide recommendations that make us a far stronger organisation.”

CYBER SECURITY MANAGER
UK GOVERNMENT DEPARTMENT

Overview

About the client

This Government department has risen admirably to the challenges posed over recent years, working tirelessly to support and steer the industry, and serve the public.

Employing over 4,000 staff around the UK, in roles as diverse as engineering, social research and law, the organisation plays a critical role in the UK's national infrastructure.

Strengthening the cyber resilience of the UK's most critical systems is vital if we are to guard our citizens personal information, and protect the functions and services on which we all depend.

Background

The department is striving to develop and mature a world-class cyber operations capability, and in 2022 decided to look for a partner who could help to develop their security operations.

They wanted a partner that they could collaborate with, to help provide security monitoring and detection, and leadership around the development, and continuous improvement of incident playbooks, helping to refine and tune monitoring and threat detection capabilities, whilst providing support and input into annual business continuity and disaster recovery planning.

The Project

The key to success

Our client had selected Microsoft Sentinel for their Security Information and Event Management (SIEM), allowing them to collect data at cloud scale, across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds. They were keen to work with a partner that could utilise this existing investment, and help to realise further value from it by ingesting data from more systems and incorporating it into the new MDR service.

Socura has significant experience working with Microsoft Sentinel, ingesting alerts from this, and numerous other technologies, into our Incident Management Portal, offered as a packaged service to further simplify security operations.

The client had identified three distinct phases for developing Sentinel platform and onboarding the new MDR service, with each phase integrating different data sources into either the Sentinel platform or, if there are no solutions to feed directly into Sentinel, directly into the Socura Incident Management Portal.

To ensure the client realised value from the project as quickly as possible, we were able to integrate the Socura MDR service into the existing Sentinel deployment and start monitoring within the first two weeks of project initiation. The three phases looked like this:

Phase 1 Integrations

- Azure Active Directory
- Microsoft 365
- SASE/SSE

Phase 2 Integrations

- Google Cloud Compute Engine and SCC
- Microsoft Defender for Endpoint
- NCSC Active Cyber Defence
- Vulnerability management
- Azure workloads
- Email security

Phase 3 Integrations

- Microsoft Defender for Cloud Apps
- Microsoft Data Loss Prevention
- Microsoft Intune

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.

The steps that took place at each phase

Planning - The first step began by bringing our two teams together. Collaborative workshops ensued, focussed on understanding the department'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 department to deploy the technology that would allow the monitoring, security telemetry, and pro-active action to take place. Remote delivery of the technology equalled speed, with the deployment taking around 6 weeks for each phase.

Tuning - With the mission-critical nature of government 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 internal 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. Happily both teams agreed that the acceptance criteria were successfully met and we could move into a live service state under the defined SLAs.

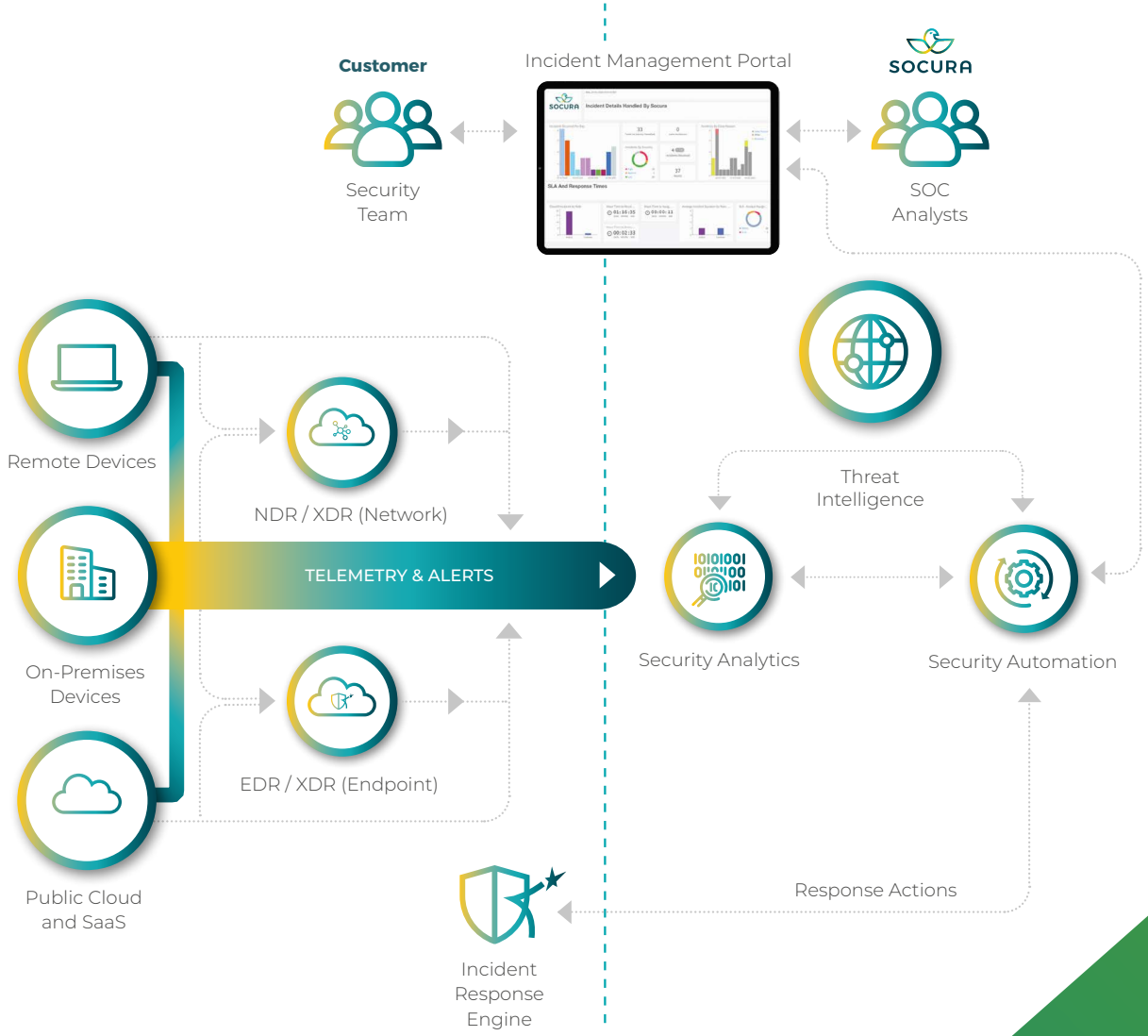
The Tech

The technical elements of Socura's Managed Detection and Response (MDR) service for the client 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 SIEM)



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, continually looking for different and better ways to do things, and always proactive in solving problems if they arise.

Continually improving cyber maturity

Every interaction between the client and the new managed SOC provides feedback on how things are working. A Socura Customer Success Manager (CSM) ensures these crucial learnings are developed into proper insights, and resulting actions that will continually improve the departments cyber resilience:

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

Review
security incidents

Analyse
data & trends

Measure
performance & SLAs

Identify
opportunities

We provide dashboards, data and user-friendly metrics, and the client 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 client is kept up to speed there too.