Case Study:

Builder's Merchant

SOCURA

“Excellent customer service, including a track record of meeting SLAs, combined with an effective XDR and XSOAR technology platform, have delivered a managed MDR partnership that is a very good fit for our company.”

GROUP INFORMATION TECHNOLOGY DIRECTOR
BUILDER’S MERCHANT

Overview

About the client

A well-established builder's merchant business operating across the UK, Ireland, The Netherlands, and Finland.

The organisation which is over 100 years old and is listed on the FTSE 250 index and has grown through acquisitions, encompassing various operating companies in the manufacturing, distribution, and retail sectors. As the business expanded, so did its IT environment, with each acquisition bringing in new IT systems, processes, and repositories of critical business data.

Background

As it's IT environment became increasingly complex, the organisation recognised the need to safeguard against potential cyber attacks that could disrupt their operations.

Ransomware, in particular, posed a significant concern. Despite making significant investments in modern cyber security tools and building an in-house cyber security team, they realised the importance of specialised Security Operations (SecOps/SOC) support to defend their environment against modern threats that could evade preventative controls.

The Project

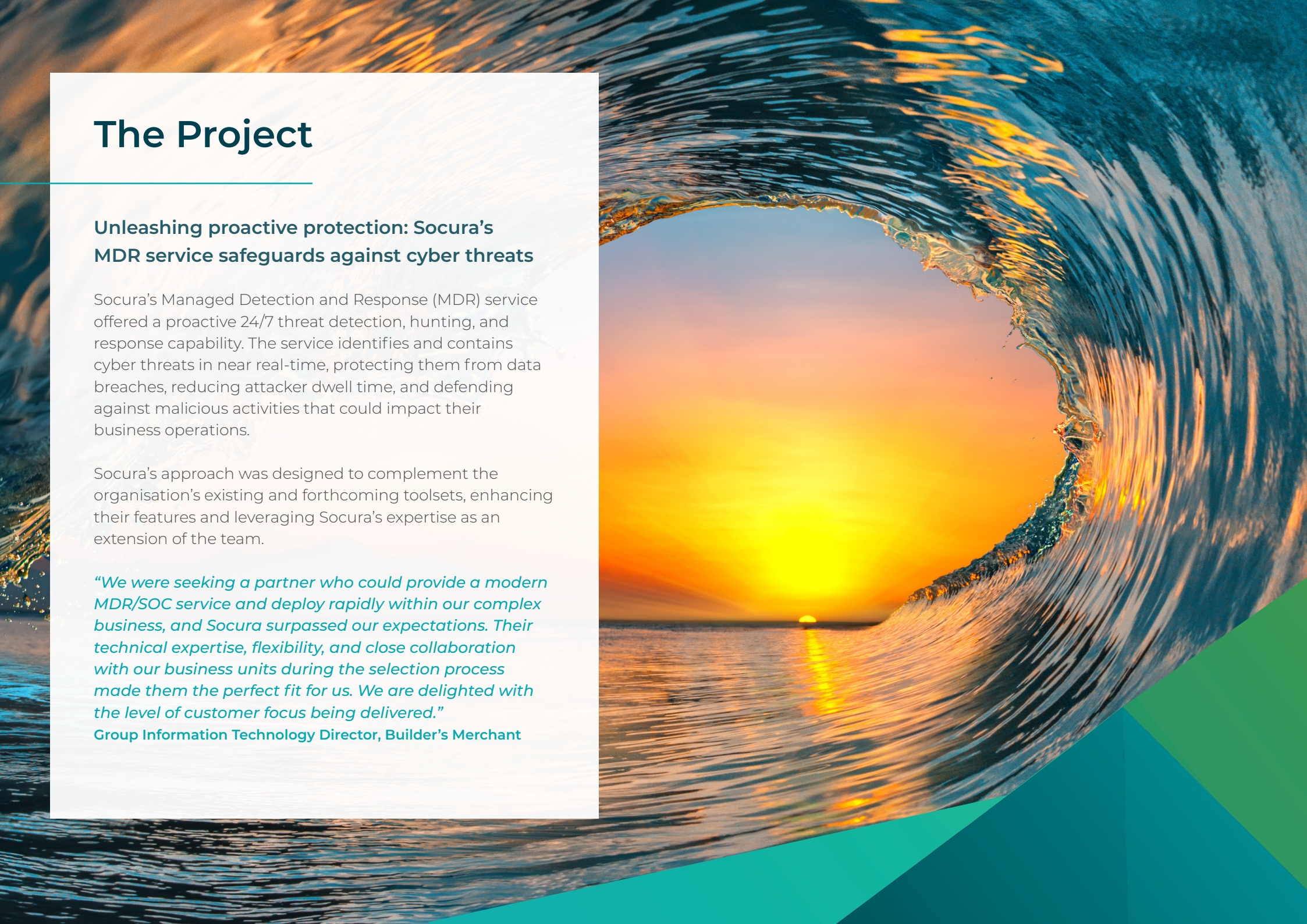
Unleashing proactive protection: Socura's MDR service safeguards against cyber threats

Socura's Managed Detection and Response (MDR) service offered a proactive 24/7 threat detection, hunting, and response capability. The service identifies and contains cyber threats in near real-time, protecting them from data breaches, reducing attacker dwell time, and defending against malicious activities that could impact their business operations.

Socura's approach was designed to complement the organisation's existing and forthcoming toolsets, enhancing their features and leveraging Socura's expertise as an extension of the team.

"We were seeking a partner who could provide a modern MDR/SOC service and deploy rapidly within our complex business, and Socura surpassed our expectations. Their technical expertise, flexibility, and close collaboration with our business units during the selection process made them the perfect fit for us. We are delighted with the level of customer focus being delivered."

Group Information Technology Director, Builder's Merchant



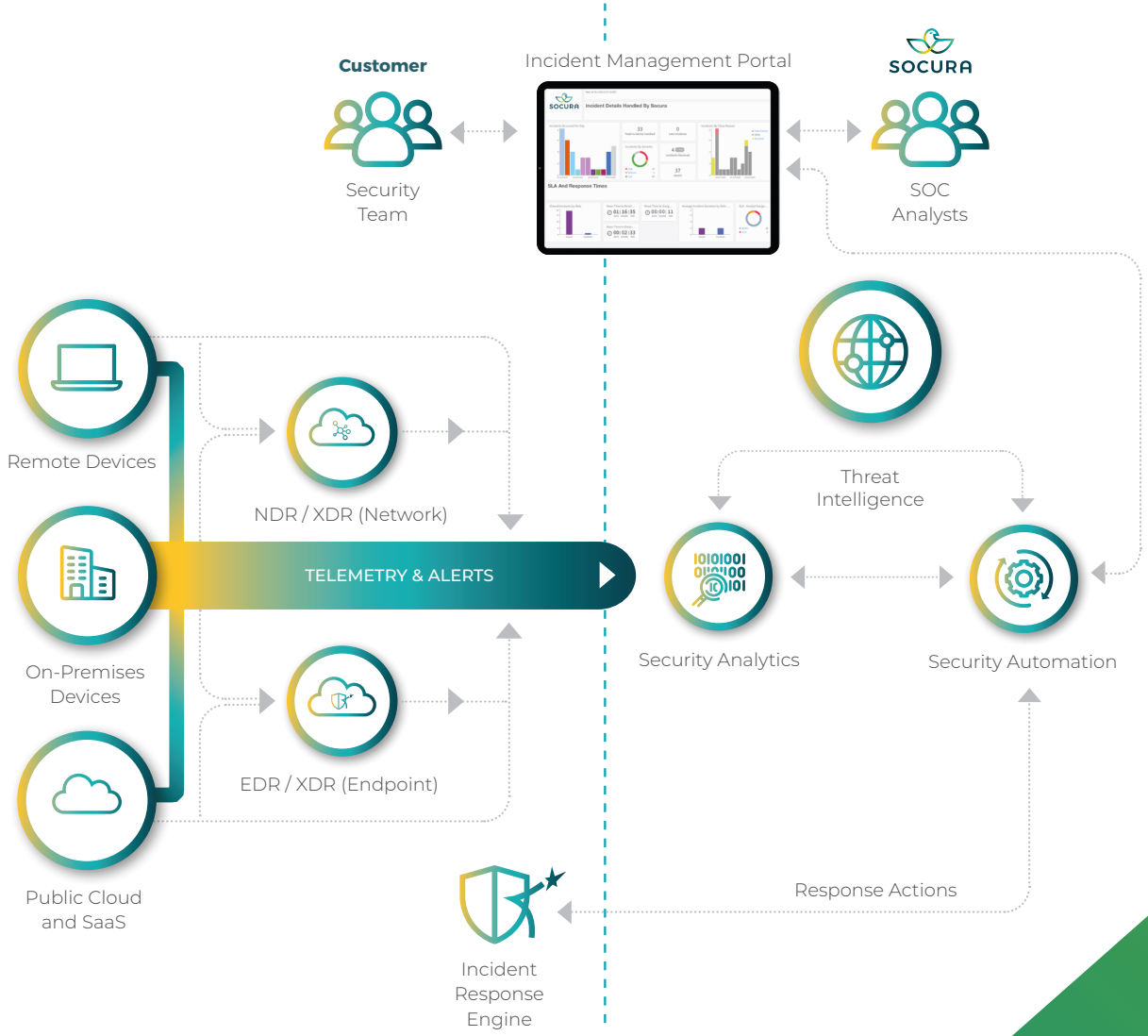
The Tech

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)



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 - 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.

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.

Making it Count

While Socura's innovative use of technology enables optimal risk management and response, it's their people-centric approach that truly sets them apart.

"Socura have worked very hard to get a deep understanding of our business and different subsidiaries, and have tailored their MDR service to ensure that every one of our companies is treated individually with an understanding of their specific environment and relationships developed with the individual business teams."

Telemetry and alerts from the existing network and security technologies are securely collected by Socura for correlation and matching against threat detection rules and intelligence sources. If a threat detection rule or threat intelligence match is found, Socura's Incident Management Portal (IMP) triggers a notification to the Socura analyst team. The analysts investigate the incident within the IMP, enriching related indicators with premium and open-source threat intelligence sources, and follow predefined playbooks specific to the incident type. If the incident is determined to be a false positive, detailed notes are added, and the incident is closed without customer notification to avoid unnecessary interruptions. Monthly reports include information about false positives.

"Socura endeavour to reduce the workload on the customer with a continual improvement approach to reduce false positives and deal with as many incidents themselves through tuning of the tooling and response playbooks, which has proven to be very effective."

If the investigation concludes with a true positive, response actions can be taken with customer authorisation or immediately if pre-approved. Socura orchestrates threat containment actions across endpoints, networks, and cloud environments using pre-approved playbooks.

"The Socura team work on a very collaborative basis and listen and respond to feedback. There have been several instances where we have improved the service in partnership by quickly implementing a tweak to a process or playbook after an incident."
Group Information Technology Director,
Builder's Merchant

SOCURA

Socura Limited Registered in England No. 12200836 I Email: hello@socura.co.uk I