Case Study:

Barrett Steel Limited

SOCURA

“Excellent customer service, combined with an effective XDR and XSOAR technology platform, have delivered us a great MDR solution that fits our business well.”

MICHAEL RATCLIFFE
HEAD OF INFORMATION SECURITY
BARRETT STEEL LIMITED

Overview

About the client

Barrett Steel Limited is an established Steel stockholder and supplier that consists of 44 companies operating from 30 sites nationwide.

Founded in 1866, Barrett Steel has grown both organically and by acquisition from a one-man company to the largest independent steel stockholder in the UK with 1,500 staff members and is now on a path to digitise their workforce.

Background

Barrett Steel is on a trajectory towards digitising their workforce, and within the next 12 months, all 1500 employees will be actively utilising technology. This digital transformation brings with it increased risk to the business.

Despite substantial investments in modern cyber security tools, Barrett Steel has recognised the need for specialist outsourced Security Operations support to defend their environment against modern threats that may bypass preventive controls and is actively pursuing the outsourcing of their Security Operations function to a partner who will seamlessly collaborate with their in-house team and offer support throughout this transformative journey.

The Project

Releasing proactive protection: Socura's MDR service ensures the protection of Barrett Steel against cyber threats.

Socura's Managed Detection and Response (MDR) service offered Barrett Steel Limited a proactive 24/7 threat detection, hunting, and response capability. The service identifies and contains cyber threats in near real-time, protecting Barrett 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 Barrett's existing and forthcoming toolsets, enhancing their features and leveraging Socura's expertise as an extension of the in-house team, supporting them on this journey.

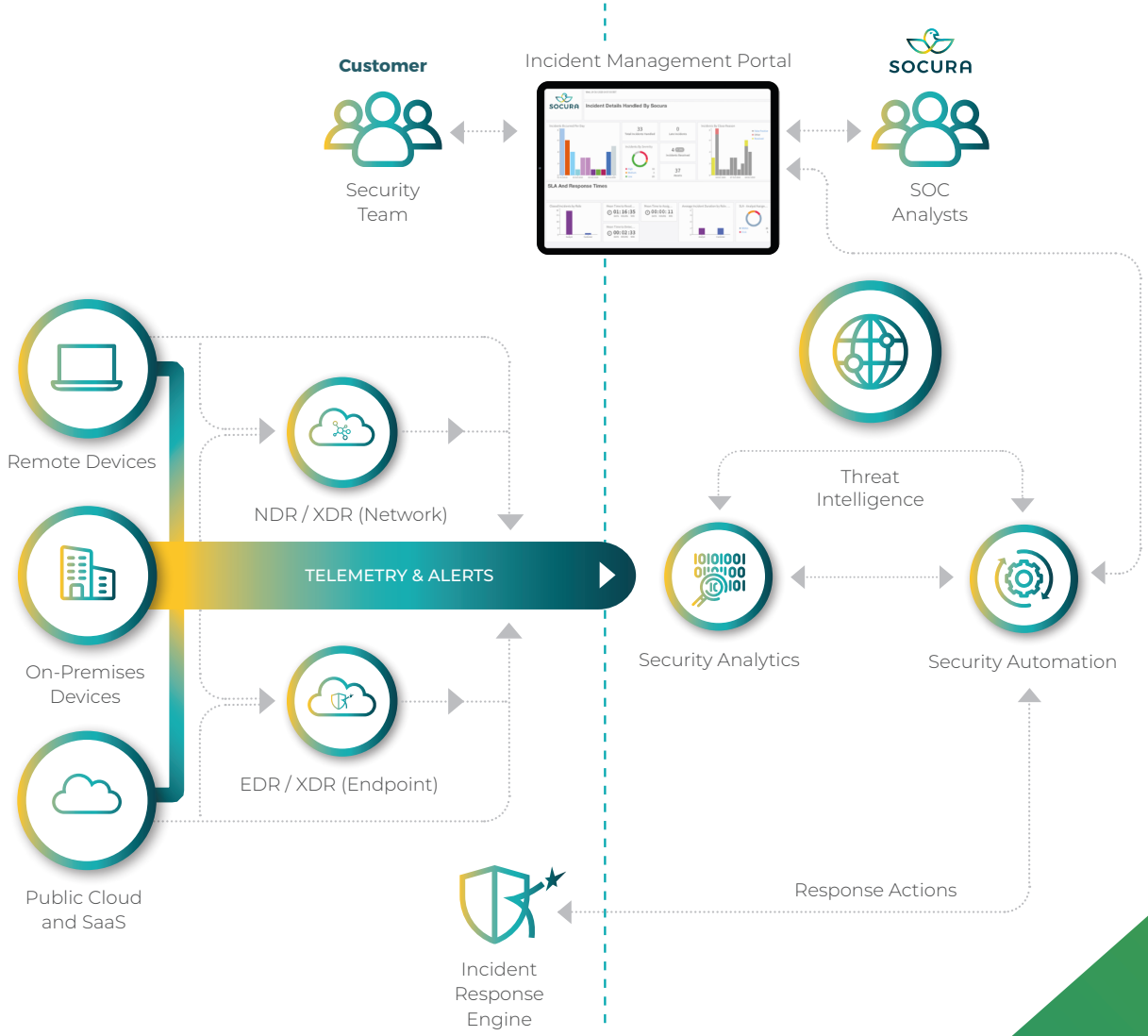
The Tech

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)



The Google Cloud Chronicle Advantage

Socura has partnered with Google Cloud Chronicle to allow us to ingest all the security data that Barrett'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.

Chronicle
part of Google Cloud

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 - Our journey commenced with the integration of our two teams. We conducted cooperative workshops, with a primary focus on gaining insight into the department's environment, business processes, and crucial information assets. Using this knowledge, we collectively crafted and agreed upon a deployment plan designed to accommodate the 28 unique log sources.

Deployment - Here the Socura team collaborated closely with the department to implement the technology necessary for monitoring, security telemetry, and proactive actions. This involved the deployment of five custom parsers and log source ingestion methods tailored to accommodate a diverse range of technologies.

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

Excellent customer service, combined with an effective XDR and XSOAR technology platform, have delivered us a great MDR solution that fits our business well. The onboarding service was an excellent process and a great introduction to the team and service.

We get regular reporting from Socura, which is really useful and detailed. The monthly service reviews also allow us to raise anything else we'd like to see if we want a follow-up on specific incidents and are really useful.

MICHAEL RATCLIFFE
HEAD OF INFORMATION SECURITY
BARRETT STEEL LIMITED

SOCURA

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