SUCCESS STORY

UK MDR Provider Socura Scales Threat Intelligence To Protect Country's Biggest Business And Critical Public Services Providers

Why Dark Web Intelligence Is Now Essential for MDR Providers

Credential theft has emerged as one of the most pervasive and consequential threats facing organizations today. Rather than exploiting complex technical vulnerabilities, modern attackers increasingly take the path of least resistance: they prefer to log in rather than hack.

Infostealer malware silently harvests credentials from compromised devices, often without the victim's knowledge, with stolen data quickly appearing across Telegram channels, dark web forums, and illicit marketplaces. From there, threat actors can purchase access to enterprise environments at minimal cost, enabling account takeovers, ransomware deployment, and large-scale data breaches.

As part of a joint marketing and research effort, Socura and Flare investigated the scale of credential theft across the FTSE 100, and found 460,000 instances of stolen employee credentials.

Customers increasingly expect their security partners to identify threats before they escalate into business-impacting events. It was this expectation, and the opportunity it represented, that led Socura to evaluate and ultimately integrate Flare into its security operations.

The Partner

UK-based Managed Detection and Response (MDR) provider protecting some of the country's largest businesses and providers of critical public services, spanning industries including financial services, healthcare, and the public sector

Recognized by Megabuyte as one of the UK's best-performing scale-up companies

Delivers round-the-clock security monitoring as an embedded extension of clients' in-house teams, combining threat intelligence, incident response, and threat exposure monitoring

Flare is an excellent technology partner to Socura. Their intelligence, technology, and team are fantastic to work with, adding real value to our MDR service offering whilst helping us generate additional revenue.

– Nigel Howarth,
Head of Partnerships and Alliances,
Socura

Challenge: Augmenting Threat Intelligence to Deliver More Proactive Customer Protection

Socura's in-house threat intelligence team drew on a wide range of commercial feeds and open-source intelligence (OSINT) sources to support their 24/7 MDR service. However, as the threat landscape evolved and customer expectations grew, Socura recognized an opportunity to go further.

Feedback from customers across industries made the need explicit: organizations wanted Socura to help them become even more proactive in their approach to security. To meet this demand, Socura sought to:

- **Rapidly identify leaked or stolen credentials** belonging to their customers that had surfaced on the dark web or within illicit Telegram channels
- **Conduct highly specific, targeted searches** based on identifiers such as domains, IP addresses, and product names, moving beyond broad monitoring to precise, actionable intelligence
- **Detect evidence of targeting** by specific threat actors, both against individual customers and organizations with a similar threat profile

Socura's existing range of threat intelligence sources couldn't provide the dark web insights it needed. It was also looking for a platform that integrated seamlessly with its incident management portal to streamline workflows across its security operations center. Ultimately, that search led to Flare for three reasons:

1. **Data and intelligence depth:** The ingested threat intelligence is accurate and up-to-date, enabling proactiveness in mitigating risks for customers.
2. **Flexibility to scale:** Continuous improvements such as the industry-specific reports help keep up with certain sectors closely, such as finance.
3. **The people:** As Socura works collaboratively with their partners, it mattered to find a team with a similar ethos.

Implementation: Fully Operational in a Matter of Weeks

Socura became one of Flare's earliest channel partners in the UK, and from the outset the onboarding process was built for speed. The partnership was up and running in just a matter of weeks, enabling Socura to begin delivering enhanced threat intelligence capabilities to customers quickly and with minimal disruption.

Critically, Flare integrated directly with Socura's existing incident management portal, meaning the threat intelligence team could immediately begin leveraging Flare's intelligence within the workflows they already used, with no significant operational overhaul required. From day one, Socura's analysts were equipped to monitor for customer-specific identifiers across Flare's extensive data sources and receive automated alerts whenever relevant data surfaced. The platform's intuitive interface meant the team could begin conducting targeted searches and generating customer value almost immediately.

> **Working with Flare has enabled us to improve the outcomes we deliver to our customers, ensuring they can keep pace with threats and preempt attacks before they become business impacting events.**
>
> – Nigel Howarth, Head of Partnerships and Alliances, Socura

Benefits: Proactive Protection, a New Revenue Stream, and Streamlined Operations

Expanding Service Capabilities Across the SOC

Flare now supports Socura's threat intelligence team across a broad range of day-to-day activities, including:

- **Threat profiling** to build a detailed understanding of the specific threat actors relevant to each customer's industry and risk profile
- **Continuous threat intelligence reports** that give customers specific, ongoing insight into a shifting threat landscape, so they can keep improving their defenses.
- **Takedown support** for instances where a customer's domain has been spoofed by threat actors
- **Automated alerting** for leaked credentials, enabling rapid account resets and IP blocking on customers' behalf

By supplementing threat intelligence data from other sources and enabling precise searches across Flare's vast dataset, the platform has sharpened the quality and speed of intelligence Socura delivers across its entire customer base.

Generating Six-Figure ARR in Year One

Flare has not only enhanced the quality of outcomes Socura delivers, but it has also created a significant new revenue stream. In their first year as a Flare partner, Socura onboarded **over 25 customers** onto their Flare-powered identity-focused cyber threat intelligence service.

Socura offers this capability in two ways. It works as an add-on to their core MDR service, and as a standalone product for organizations looking to independently address their identity exposure monitoring needs. This broadens Socura's total addressable market while reinforcing the value of their flagship service.

Detecting Threats Before They Escalate

The real-world impact of Flare's intelligence was demonstrated clearly and early.

In one notable incident, Flare alerted Socura's SOC team to sensitive information belonging to a customer's employee that had been leaked on Telegram.

1

The compromised data included passwords tied to the individual's bank account and NHS login, exactly the type of high-value credentials threat actors can rapidly exploit for financial fraud or further network access.

2

Flare identified the exact infostealer file responsible, giving the team a concrete lead instead of a generic alert.

3

Armed with this precise intelligence, Socura's SOC team was able to:

- Identify an isolated malicious file on the employee's device
- Reset the user's Windows login credentials to prevent further exploitation of any compromised access

This rapid, targeted response, enabled by Flare's intelligence, exemplifies the proactive, outcome-driven protection Socura's customers had been asking for.

What's Next: Staying Ahead of a Faster Threat Landscape

As AI-driven attack techniques simplify and accelerate the pace of an already fast-moving threat landscape, Socura sees the need to adapt to new threats more quickly as an increasingly essential pillar of enterprise security. Over the next twelve months, Socura plans to deepen its partnership with Flare. The team is particularly excited about the platform's expanding reporting capabilities, including industry-level reports already available and threat actor reports coming soon. This intelligence will further equip them to understand and anticipate the latest attacker tactics, techniques, and procedures.

With Flare embedded in their SOC, a growing customer base benefiting from proactive dark web intelligence, and a collaborative partnership continuing to generate both market awareness and tangible revenue, Socura is well-positioned to empower UK businesses and critical public service providers to stay ahead of the threats that matter most.