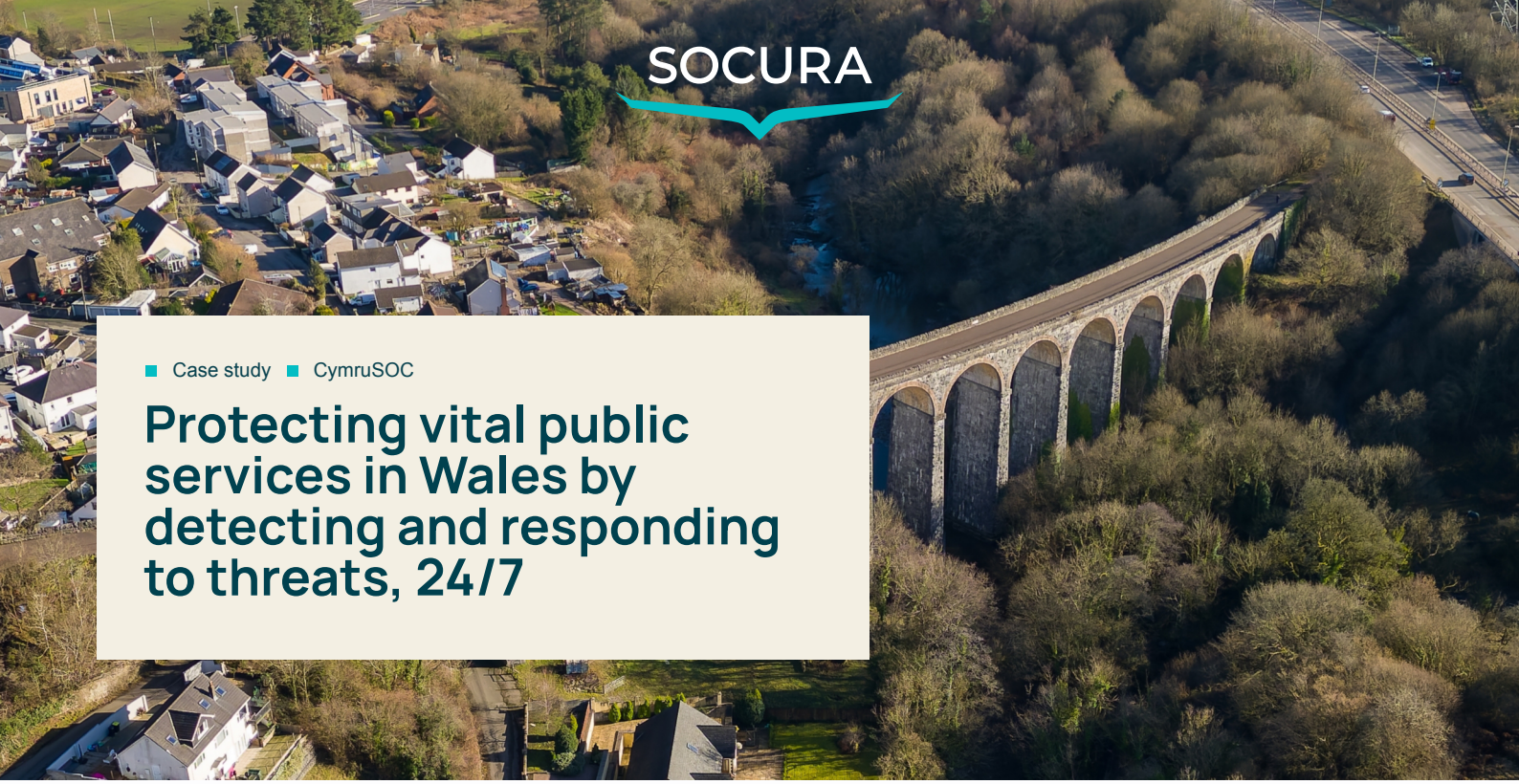

SOCURA

Case study ■ CymruSOC

Protecting vital public services in Wales by detecting and responding to threats, 24/7

Merthyr Tydfil County Borough Council, a local authority in South Wales, was concerned that a serious cyber incident could impact its ability to provide essential public services.

To minimise its risk and that of other public sector organisations across the country, the council helped establish CymruSOC, Wales' national security operations centre, and appointed Socura to deliver the service.

MERTHYR TYDFIL
County Borough Council
Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL

The security challenge

Serving over 60,000 people in Wales, Merthyr Tydfil County Borough Council was concerned that a serious cyber incident could impact its ability to provide essential public services.

However, the job of identifying and responding to threats around the clock was proving challenging for its IT and security teams. Ryan James, Chief Information Security Officer at the council, saw the benefit of seeking the help of threat detection specialists to ease the load and identify attacks as early as possible.

"People and businesses rely on the Council for essential services such as social care, education and waste collection" says James. "If our websites, email systems, and telephone systems go down, that's going to prevent residents from accessing information, reporting issues, and seeking assistance."

Key security concerns of Merthyr Tydfil County

- **Preventing disruption to essential public services**
- **Protecting sensitive personal and financial data**
- **Mitigating the risks of phishing and human error**
- **Keeping security controls optimised to detect new threats**

The solution

As the partner chosen to deliver CymruSOC, Wales' national security operations centre, Socura now provides a Managed Detection and Response (MDR) service to Merthyr Tydfil County Borough Council.

Operating as an extension of the Council's security and IT teams, the service supplies a team of detection and response specialists, responsible for proactively identifying threats and eliminating them.

To provide extensive threat coverage and visibility, the MDR service uses the latest Security Orchestration, Automation and Response technology, fully integrated with the Council's Security Information and Event Management (SIEM) and other security controls. Available log sources are ingested as part of the service and Socura performs weekly threat hunting activities to look for evidence of historic attacks.

When malicious security events are identified, Socura's Security Operations Centre (SOC) analysts promptly investigate them and, where possible, automated response actions such as disabling user accounts are initiated. Should incidents need to be escalated, detailed information, including root cause analysis and remediation recommendations, is shared with the Council's teams.

Socura also regularly shares cyber threat intelligence, which is tailored to the threat profile of the Council and other local authorities in Wales.

Included as part of Socura MDR

- **Detection and response across networks, endpoints and clouds**
- **24/7 incident monitoring, analysis and triage**
- **Detection rule development and maintenance**
- **Proactive human-led threat hunting**
- **Automated threat containment and disruption**
- **Tailored threat intelligence for the public sector across Wales**
- **Monthly reporting and service reviews**

> With Socura monitoring and responding to threats 24/7, we get an early detection warning. The advanced detection coverage Socura provides means we are protected more comprehensively than ever.

Ryan James
Chief Information Security Officer

Key benefits

How Merthyr Tydfil County Borough Council benefits from CymruSOC.

01

Enhanced threat visibility

By replacing the Council's SIEM with a next-generation alternative offering unlimited data ingestion, Socura has increased visibility across the Council's environment. A larger dataset, which also includes cyber threat intelligence gathered by Socura across all participating members of CymruSOC, means that threat hunting activity is also performed more widely.

02

Reduced mean time to respond

Socura's MDR service doesn't just detect threats such as malware and phishing attacks. It also helps the Council respond to them, both swiftly and effectively. Automated incident response playbooks are triggered when specific behaviours are observed, meaning threats can be shut down in minutes. On average, it takes the Socura team just 6 minutes to assign a ticket and start investigating it.

"By initiating incident response processes, Socura's SOC team accelerates the time it takes us to respond to threats and minimise their potential impact," says James. "They also share root cause analysis and lessons learned so that we can continuously improve and adapt."

03

Genuine incident reporting

Because all security incidents are thoroughly investigated and triaged by Socura's SOC team, the Council's team is confident that when it receives a notification, it is usually a genuine incident that requires attention. No longer does the Council's team waste time investigating false positives.

6 minutes

On average, it takes the Socura team just 6 minutes to assign a ticket and start investigating it

04

Swift time to value

A phased approach to deployment means that the MDR service was operational within three months. “The service onboarding process meant that our service was up and running quickly,” says James. “Socura’s project management clearly outlines the tasks that need to be completed and is handled in a way that reduces any impact on our staff and operations.”

05

Instant access to experts

Operating as an extension of the Council, the Socura team is always on hand to provide support and advice when needed. This also includes responding to service requests.

“The Socura team are experts in their field, and we’ve already built great working relationships with their staff,” says James. “During the early discussions with Socura, you get the indication that they are very customer-centric, and this has been demonstrated in all aspects of the work they do for us. They also share their knowledge with us, which is great for helping to upskill our internal team.”

06

Regular service reviews

So the Council can track its security posture and identify ways to minimise risks, Socura shares monthly service reports. These are supplemented by regular reviews led by a dedicated Customer Success Manager.

“It used to be a manual exercise to go in and look at the security data and analytics that were available,” says James. “Now we get regular metrics from Socura and the information we need to continuously understand what our security posture looks like and make improvements.”

> “During the early discussions with Socura, you get the indication that they are very customer-centric, and this has been demonstrated in all aspects of the work they do for us.

Ryan James
Chief Information Security Officer

Talk to us about your detection and response challenges

SOCURA

hello@socura.co.uk
0800 640 4067
LinkedIn
Bluesky