Cyber Resilience in Wales

Llywodraeth Cymru
Welsh Government

October 2025

Toby Grainger

Head of Wales Cyber Security Operations Centre (CymruSOC)
Welsh Government

Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE

Cyber Resilience Unit

Llywodraeth Cymru
Welsh Government

- Cyber exercising in Wales
- Cyber Assessment Framework (CAF)
- Cyber videos
- Supply Chain
- CymruSOC – the origins
  - Current state of play
- Looking to the future

Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE

Llywodraeth Cymru
Welsh Government

Cyber Resilience Unit

Our aim is to promote and improve cyber security and resilience for organisations and citizens in Wales.

Cyber Exercising Programme for Wales

Llywodraeth Cymru
Welsh Government

- Regular testing of Public Sector Cyber Incident Management Plans (CIMP) enhances preparedness.
- Table-Top exercises – 70% increase in CIMP improvement and user confidence.
- Senior Leadership training - covering cyber threats, risk management principles and SLT involvement.
- Virtual Cyber Simulation Exercise - provided real-life scenario experience for players.
- CIMP drafting sessions - supporting organisations in plan development and exercising.
- Future plans focus on expanding and deepening cyber resilience capabilities.
- Procurement exercise currently underway

"I recently attended Cyber UK and thought it was one of the most useful events I've been to, I place this exercise on the same level in terms of value to my organisation."

NSRD

DATBLYGU SEIBERWYDNWCH
BUILDING CYBER RESILIENCE

Cyber Assessment Framework (CAF)

Llywodraeth Cymru
Welsh Government

The CAF is a self-assessment tool to help organisations manage critical networks and systems to achieve and demonstrate cyber resilience across 4 key objectives; managing risk, prevention, detection and minimising impact.

- We have funded and work in partnership with the Welsh Local Government Association (WLGA) to implement the CAF in Local Authorities and Fire & Rescue Services in Wales.
- Relationship management. Delivery Group, Reference Group, CAF Board.
- Successful completion of CAF Objectives A and D (managing risk and minimising impact).Supported with ongoing feedback and workshops provided by the SME we funded
- Critical Systems Mapping has started to analyse key systems and support further objectives. Mapping these systems will inform the work on objectives B and C (prevention and detection).

NSRD

DATBLYGU SEIBERWYDNWCH
BUILDING CYBER RESILIENCE

Cyber Awareness Videos

Llywodraeth Cymru
Welsh Government

- Bilingual videos to improve cyber security understanding across Wales.
- Videos focus on threats like phishing, ransomware, and social engineering.
- Widely adopted by Welsh public sector and international banking platforms (over 170,000 views)
- Award nominations (National Cyber Awards)
- Future videos -
  - Docu-style video on Welsh Language Commissioner's office cyber attack
  - Upcoming videos focus on attack impact and organisational recovery efforts.
  - Completion of new video expected in autumn to raise further awareness.

NSRD

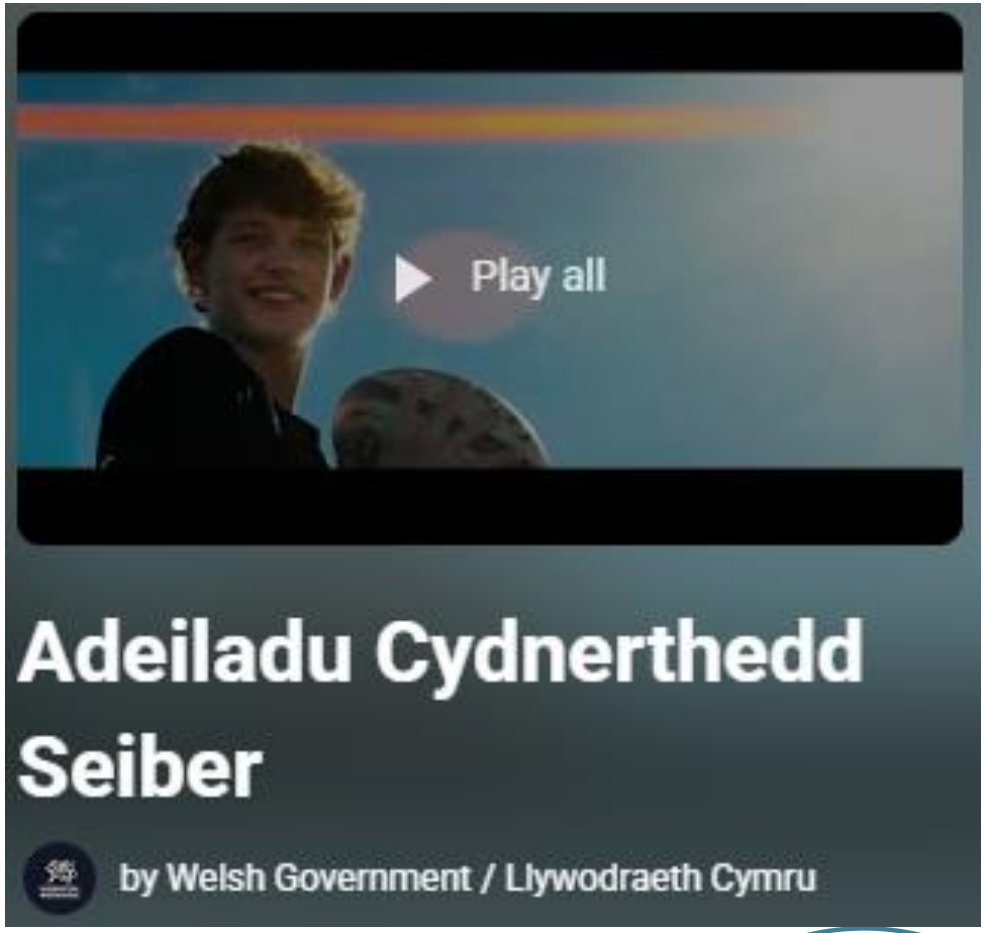
DATBLYGU SEIBERWYDNWCH
BUILDING CYBER RESILIENCE

Cyber Awareness Videos

Llywodraeth Cymru
Welsh Government

- **English version**

- **Fersiwn Gymraeg**



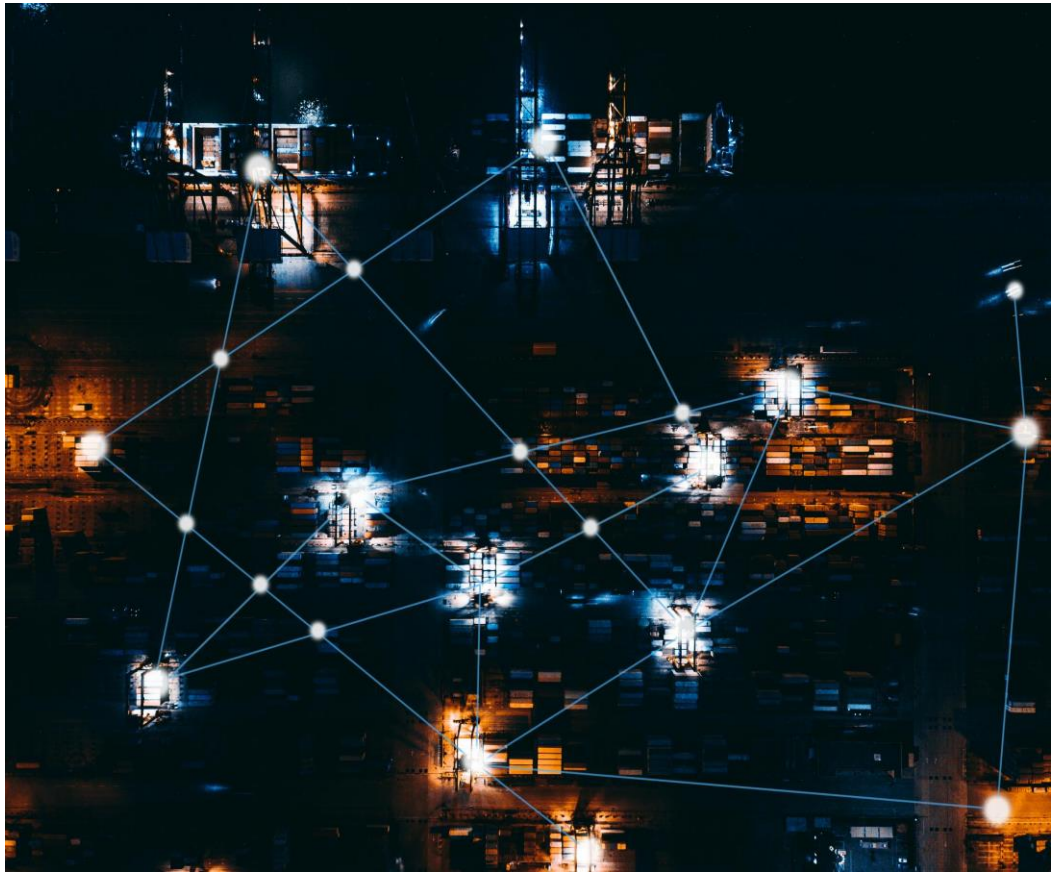
NSRD

DATBLYGU SEIBERWYDNWCH
BUILDING CYBER RESILIENCE

Cyber Supply Chain

Llywodraeth Cymru
Welsh Government

- Commissioned a research project to provide a report on supply chain cyber security across the public and private sectors.
- Delivered jointly by Actica Consulting and the Wales Cyber Resilience Centre, the research gathered insights from over 250 organisations and gauged current levels of cyber maturity across the sectors.
- This work aligns with Pillar 2 of the UK's National Cyber Strategy and the key findings and recommendations are being used by the CRU to shape future policy.
- Started looking at how to deliver on the recommendations and we're looking in the main at 'no cost' options given the current financial climate.



NSRD

DATBLYGU SEIBERWYDNWCH
BUILDING CYBER RESILIENCE

Cyber Security and Resilience (Network and Information Systems) Bill

Llywodraeth Cymru
Welsh Government

- The Bill aims to:
  - Strengthen the UK's cyber defences
  - Enhance the resilience of essential services and infrastructure.
  - Address vulnerabilities in the current regulatory framework

- Cross-cutting across multiple Welsh Government policy areas, particularly those subject to NIS regulations

- CRU coordinating the WG response

- Bill will be laid to Parliament on before Christmas

NSRD

DATBLYGU SEIBERWYDNWCH
BUILDING CYBER RESILIENCE

Project Gwydion

Llywodraeth Cymru
Welsh Government

- A project to obtain an understanding of the cyber maturity on critical and significant infrastructures situated within Wales.
- To assure Welsh Ministers and Welsh Public Sector Bodies that CNI/SLI sites can effectively prepare, respond to and recover from cyber incidents.
- Given the secure nature of this work and the levels of security clearance needed, this has been a difficult area to access and engage with. However, the drive and determination of the project team has resulted in the project growing in momentum.
- A multi-layered engagement approach, including face to face meetings with officials, CNI Site Owners and Operators have taken place which have proven to be most insightful.

NSRD

DATBLYGU SEIBERWYDNWCH
BUILDING CYBER RESILIENCE

CymruSOC – what is it?

Llywodraeth Cymru
Welsh Government

- Defend as One
- Wales Cyber Action Plan
- Cabinet Office funded
- Fully funded SOC for 21 Member Bodies
- 3 year contract
- Optional SIEM

Cyngor Bwrdeistref Sirol Merthyr Tudful / Merthyr Tydfil County Borough Council
Cyngor Sir Gâr Carmarthenshire County Council
Cyngor Bwrdeistref Sirol Pen-y-bont ar Ogwr Bridgend County Borough Council
Cyngor Sir y Fflint Flintshire County Council
Cyngor Sir Ceredigion County Council
Cyngor Abertawe Swansea Council
Cyngor Sir Ynys Môn Isle of Anglesey County Council
Cyngor Bwrdeistref Sirol Castell-nedd Port Talbot Neath Port Talbot County Borough Council
Caerphilly County Borough Council / Cyngor Bwrdeistref Sirol Caerffili
Cardiff / Caerdydd
Cyngor Sir Ddinbych Denbighshire County Council
Vale of Glamorgan / Bro Morgannwg
Powys
Conwy County Borough Council / Cyngor Bwrdeistref Sirol Conwy
Cyngor Gwynedd
Wrexham County Borough Council / Cyngor Bwrdeistref Sirol Wrecsam
Rhondda Cynon Taf
Cyngor Sir Penfro / Pembrokeshire County Council
Gwasanaeth Tân ac Achub De Cymru / South Wales Fire and Rescue Service
Gwasanaeth Tân ac Achub Canolbarth a Gorllewin Cymru / Mid and West Wales Fire and Rescue Service
Gwasanaeth Tân ac Achub De Cymru / South Wales Fire and Rescue Service
CymruSOC – Canolfan Gweithrediadau Diogelwch / Security Operations Centre
Datblygu Seibergadernid / Building Cyber Resilience

NSRD – Yr adran Diogelwch a Gwydnwch Cenedlaethol / National Security and Resilience Division

CymruSOC – what is it?

Llywodraeth Cymru
Welsh Government

- Winning supplier – Socura
- Cardiff based
- True partnership
- Technical Consultants – Actica Consulting

SOCURA

Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL
MERTHYR TYDFIL
County Borough Council

ACTICA CONSULTING

NSRD

Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE

CymruSOC – current state of play

- We have 25 Member Bodies onboarded so far
- Totalling circa 610,000 users
- Increase to over 30Member Bodies by end of this year

CymruSOC – what are the benefits?

Llywodraeth Cymru
Welsh Government

Benefits of CymruSOC

- 24/7 eyes on glass
- Enhanced threat visibility
- Reduced mean time to respond to threats
- Genuine incident notification
- Full collaboration

NSRD

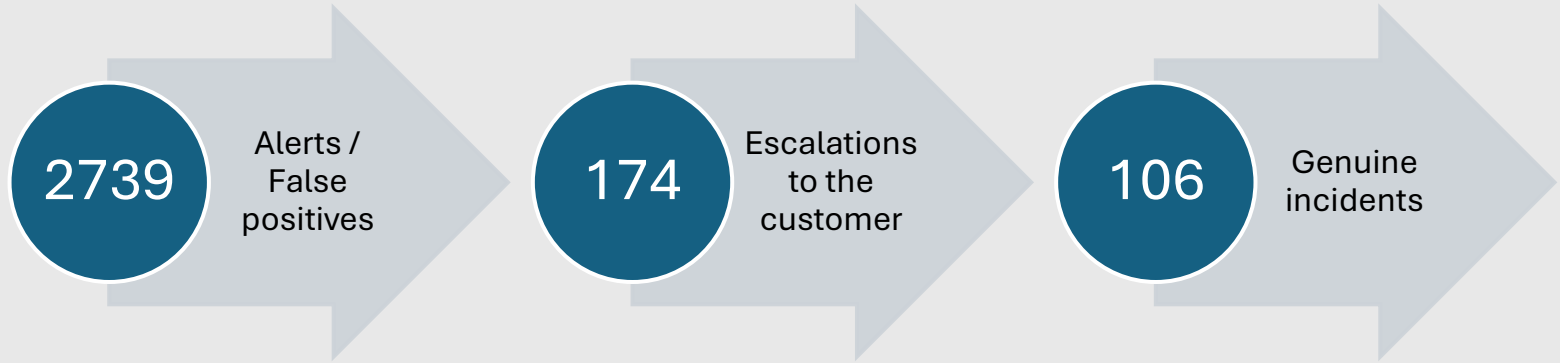
Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE

CymruSOC – operational performance

Llywodraeth Cymru
Welsh Government

Period – July -Feb



Average minutes to assign an alert - 5 mins

Average minutes to triage – 24 mins

NSRD

Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE

CymruSOC – Threat intelligence sharing

Llywodraeth Cymru
Welsh Government

- MISP
  - JISC
  - Scotland
  - GC3
  - MOD
  - Digital Health Care Wales (NHS in Wales)

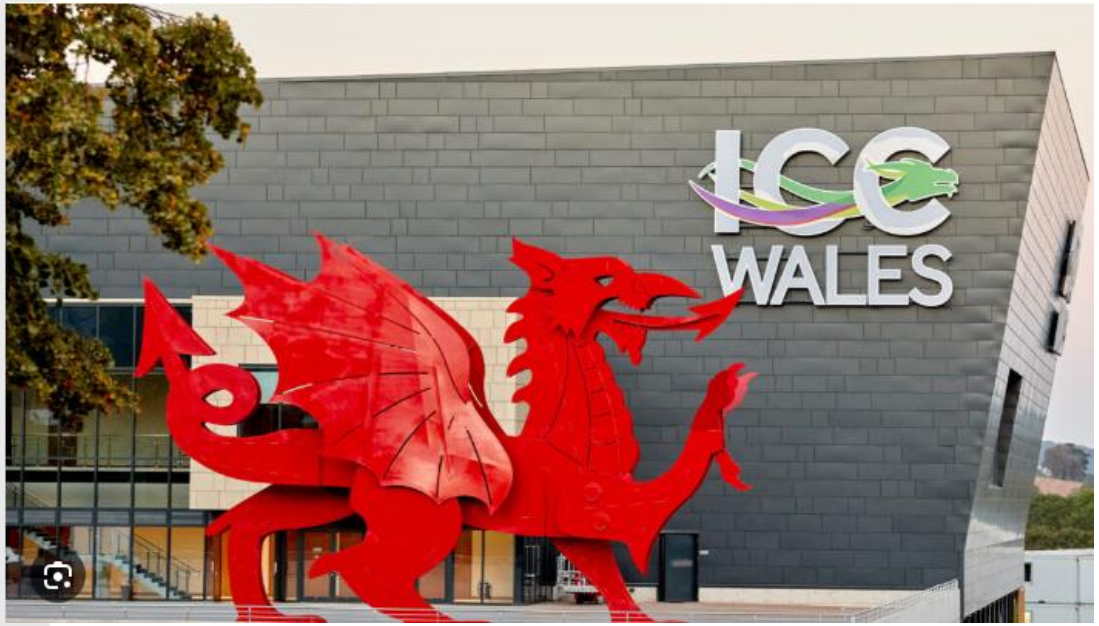
NSRD

Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE

CymruSOC events

- Virtual
- CISOs / IT Managers
- Flagship event – May 1st – Newport International Conference Centre (ICC)
  - Over 120 people attended (CISOs, SIROs
  - Shared best practice for incident response via CymruSOC
- Bigger event planned for 2026



CymruSOC – collaboration

Llywodraeth Cymru
Welsh Government

- Northern Ireland Executive
- NCSC
- JISC
- Scottish Government
- Police National Management Centre
- MOD
- Digital Health Care Wales (NHS in Wales)

Northern Ireland Executive

POLICE DIGITAL SERVICE

National Cyber Security Centre
a part of GCHQ

Scottish Government
Riaghaltas na h-Alba

Ministry of Defence

Jisc

GIG CYMRU NHS WALES
Iechyd a Gofal Digidol Cymru
Digital Health and Care Wales

NSRD

Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE

CymruSOC

Llywodraeth Cymru
Welsh Government

'DEFENDING AS ONE'

THE 'SECURITY PROJECT OF THE YEAR' WINNER AT THE 2024 COMPUTING SECURITY AWARDS CLEARLY SHOWED HOW CYMRUSOC, MANAGED BY SOCURA, IS ENHANCING THREAT DETECTION RIGHT ACROSS WALES

COMPUTING SECURITY AWARDS WINNERS

Security Project of the Year:
CymruSOC - Wales' National Security Operations Centre

Company: Socura

Project Overview:
How CymruSOC, launched in May 2024, is supporting a 'Defend as One' approach across Wales

Led by the Welsh Government, in collaboration with Merthyr Tydfil County Borough Council, CymruSOC - the first scheme of its kind in the UK - strengthens the resilience of public sector organisations across Wales. By fostering a 'defend as one' approach, it is also responsible for helping to safeguard the data of the Welsh population, as well as 60,000 employees in the public sector. CymruSOC is managed by Socura, a Cardiff-based Managed Detection Response provider. Socura operates as a partner of more than 21 local authorities and fire and rescue services in Wales, supplying the expertise and capabilities they need to monitor and respond to cyber threats around the clock.

Socura was awarded the CymruSOC contract following a competitive tender process, where the company demonstrated its pedigree in areas including cyber and technical expertise, support for detection technologies and customer service. It was also selected for its commitment to driving employment opportunities in cyber across Wales.

CYBER SECURITY CHALLENGES IN THE PUBLIC SECTOR

Every day, thousands of people rely on councils and other public sector organisations in Wales for essential services such as social care, education, and waste collection. Should a cyber-attack impact the availability of these services, the results can be devastating.

Unfortunately, many public sector organisations with tight security budgets often lack the level of security specialists they need, in order to adopt a proactive approach to security monitoring.

In the case of Merthyr Tydfil Borough Council, the organisation was aware its ability to minimise security risks was heavily linked to its ability to detect attacks early and shut them down before they caused disruption.

Keeping its Security Incident and Event Management (SIEM) platform always optimised, for example, was proving challenging and Ryan James, chief information security officer at Merthyr Tydfil Borough Council, was keen to achieve a more proactive approach. Key security concerns of the council included:

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

"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."

HOW SOCURA IS ENHANCING THREAT DETECTION ACROSS WALES

As the delivery partner of CymruSOC, Socura is rolling its Managed Detection and Response (MDR) service out to participating public sector organisations across Wales.

As the contracting authority of CymruSOC, Merthyr Tydfil Borough Council was the first organisation to benefit from the service. Operating as an extension of an organisation's security team, Socura MDR service supplies a 24/7 team of detection and response specialists. Detection technologies are included as part of the service, if required.

To centralise threat visibility, all available network, endpoint and cloud security controls deployed within an organisation are fully integrated with Socura's Security Orchestration, Automation and Response platform. New log sources are integrated regularly and Socura performs weekly threat-hunting activities to look for evidence of historical attacks.

"Previously, we may have only found out about an incident at eight in the morning when everyone starts work," adds James. "With Socura monitoring and responding to threats 24/7, we now get an early detection warning."

KEY BENEFITS OF THE SERVICE

How public sector organisations across Wales are benefiting from the CymruSOC service delivered by Socura:

Enhanced threat visibility: By aggregating security data from an organisation's choice of security controls, Socura centralises threat visibility and identifies coverage gaps. To increase the detection of adversary behaviours, Socura's team ingests new log sources and performs regular threat hunting activities.

Reduced mean time to respond: Socura's MDR service doesn't just detect threats such as malware and phishing attacks, it also helps organisations 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.

Genuine incident notification
Because all security incidents are thoroughly investigated and triaged by Socura's SOC team, organisations participating in CymruSOC are confident that when they receive a notification, it is usually a genuine incident that requires attention. Organisations now spend far less time investigating and responding to false positives.

'A defend as one' approach: By monitoring threat activity across all public sector organisations participating in CymruSOC, Socura can respond to security events at scale. Should threat activity be observed in one organisation, Socura's can take swift action to secure others against the same risk. To further support, CymruSOC's 'defend as one' approach, Socura shares regular threat intelligence bulletins to spread awareness of the latest threats and exposures.

Ryan James.

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, such as integrating new SIEM log sources.

Measurable outcomes
So that organisations can closely monitor their security posture, Socura shares monthly service reports and the data they need to measure improvements and identify potential risks. These are supplemented by regular reviews led by a dedicated customer success manager.

"The Socura team are experts in their field and we've already built great working relationships with their staff," adds 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."

- Article in February's edition of Computing Security
- Based on the recent "Project of the year" award won by CymruSOC

NSRD Yr Adran Diogelwch a Gwydnwch Cenedlaethol National Security and Resilience Division

Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE

CymruSOC – looking to the future

Llywodraeth Cymru
Welsh Government

Programme Business Case (PBC)

- 10 year PBC (2024-2034)
- Ambitious – number of costed options
  - Potential to offer additional services
- Aligns and complements the Cyber Assessment Framework (CAF) in Wales
- Establish the policy
  - Advising and getting approval from the First Minister
- Close working with Cardiff University's Cyber Innovation Hub to support the CymruSOC Business Case
- Funding sources

NSRD

Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE

CymruSOC – looking to the future

- Qtr 1 2026 - Programme Business Case to be approved
- Spring 2026 – begin procurement
- Spring 2027 – award contract

CymruSOC

Llywodraeth Cymru
Welsh Government

Diolch am gwrando

Thank you for listening

CyberResilience@gov.wales

SeiberGwydnwch@llyw.cymru

NSRD

Cymru SOC
Canolfan Gweithrediadau Diogelwch
Security Operations Centre

DATBLYGU SEIBERGADERNID
BUILDING CYBER RESILIENCE