Success Story

Bedfordshire, Cambridgeshire & Hertfordshire Constabulary

Strengthening Detection and Response with Intelligence Led Purple Teaming

Bedfordshire, Cambridgeshire & Hertfordshire Constabulary (BCH) is a collaborative policing alliance serving communities across three counties. The Constabularies are responsible for protecting sensitive operational data, intelligence systems, and critical digital services that directly support frontline policing and public safety.

Operating in an increasingly hostile cyber threat landscape, BCH understands that Cyber Security is fundamental to maintaining operational resilience, protecting public trust, and ensuring continuity of policing services. With established security controls already in place, BCH sought to gain deeper assurance that its detection and response capabilities would perform effectively against the types of real world threats currently facing UK law enforcement.

cyberlab

Learn more at **cyberlab.co.uk**

The Business Challenge

Assessing Real World Threat Readiness

BCH required confidence that its existing security technologies, processes, and teams could detect and respond to realistic cyber attacks targeting UK policing organisations.

While traditional testing provided valuable assurance, it did not fully reflect how BCH would perform against modern adversary behaviour. The Constabularies needed to understand how effectively their Security Operations Centre (SOC) and ICT teams could identify, investigate, and respond to live attack activity aligned to current criminal threat actors.

Key challenges included:

- Validating detection and response capabilities against realistic attacker techniques.
- Understanding how effectively indicators of compromise were identified and escalated.
- Testing collaboration between SOC and ICT teams during security incidents.
- Identifying gaps in incident response playbooks and operational workflows.
- Strengthening shared understanding of security responsibilities across teams.

To address these challenges, BCH required an exercise that focused on real attacker behaviour rather than isolated vulnerabilities.

The Solution

Intelligence Led Purple Team Engagement

CyberLab was engaged to deliver an intelligence led Purple Team exercise designed to assess BCH's detection and response capabilities across people, process, and technology.

Attack scenarios were developed using current threat intelligence aligned to a criminal group active in the UK during 2025. The group's known Tactics, Techniques and Procedures (TTPs) were emulated to reflect realistic attack paths BCH could face, enabling a meaningful assessment of how existing security controls and teams performed under real world conditions.

The engagement was delivered in close collaboration with BCH's SOC and ICT teams, ensuring findings were contextual, actionable, and directly relevant to day to day operations.

What is Purple Teaming?

A Purple Team exercise brings together offensive and defensive security capabilities to improve an organisation's ability to detect and respond to cyber-attacks.

- Red Teaming activity focuses on simulating attacker behaviour to test whether an organisation can be compromised.
- Purple Teaming goes a step further by actively collaborating with defensive teams during the exercise.

Rather than simply identifying weaknesses, Purple Teaming helps organisations understand how attacks are detected, how alerts are handled, and how response processes function in practice. For BCH, this collaborative approach ensured that insights were shared in real time, enabling teams to learn, adapt, and improve throughout the engagement rather than only at the end.

The Outcomes

Clear Insight and Improved Operational Maturity

The engagement provided BCH with a clear, evidence based understanding of how effectively its security capabilities performed against realistic threats.

Key outcomes include:

- Improved visibility into detection effectiveness across existing security controls.
- Identification of gaps within monitoring, alerting, and response processes.
- Stronger collaboration between SOC and ICT teams during incident scenarios.
- Clear insight into where playbooks and escalation processes could be improved.
- Increased understanding of shared responsibility for Cyber Security across teams.

By focusing on real attacker behaviour and collaborative testing, BCH gained practical insights that could be directly applied to strengthen operational readiness.

Conclusion

Strengthening Cyber Resilience Across Policing Operations

Through its engagement with CyberLab, BCH gained meaningful assurance over its ability to detect and respond to real world cyber threats targeting UK law enforcement.

The intelligence led, collaborative nature of the exercise allowed BCH to move beyond traditional assurance and focus on genuine operational resilience. The findings enabled teams to refine detection capabilities, strengthen incident response processes, and reinforce a shared approach to Cyber Security across the Constabularies.

CyberLab continues to support public sector organisations by delivering realistic, threat informed security testing that helps translate adversary behaviour into clear, actionable improvement, protecting the systems and data that underpin critical public services.

"CyberLab delivered an intelligence-led purple team exercise that gave us evidence-based assurance about how our detection and response capabilities perform against real-world threats. Their team brought genuine expertise and a clear understanding of UK policing. The collaborative format built real capability across our SOC and ICT teams, and the findings were immediately actionable. A professional partnership we trust to support our work going forward."

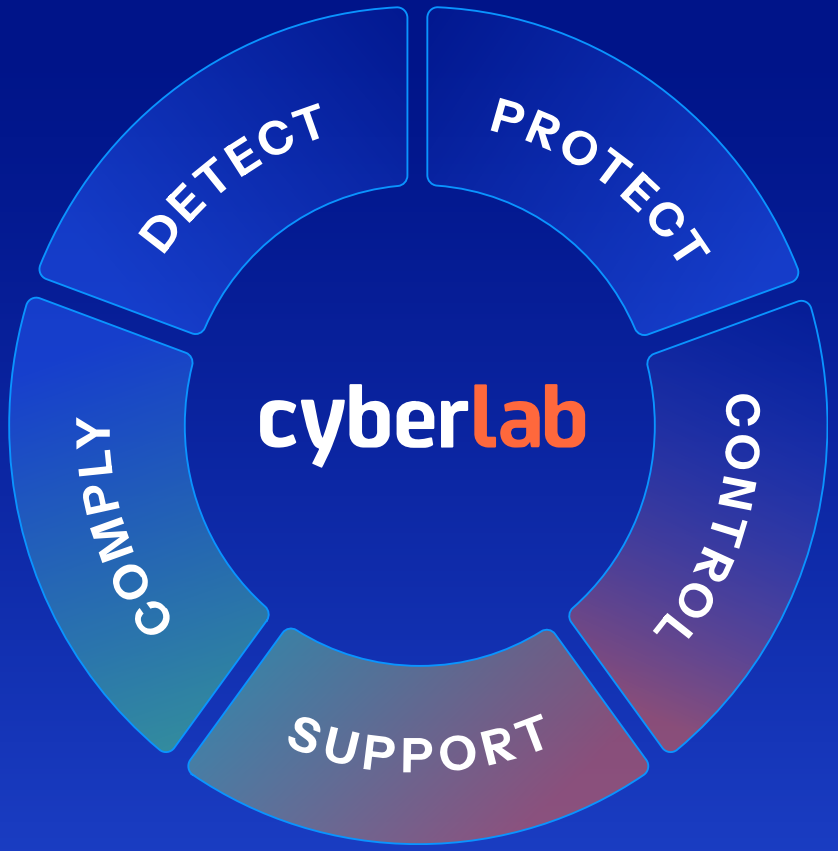
Neil Baddeley
Chief Information Security Officer
Bedfordshire, Cambridgeshire & Hertfordshire Police

Protecting the Nation, Business and People.

CyberLab is the UK-leading cyber security consultancy and managed services provider, trusted by over 1,200 enterprise businesses, government departments, and household names to secure their operations, systems and data. With more than 30 years of combined expertise, we take a deeply consultative, partnership-led approach guiding clients at every stage of their cyber journey.

Our strength lies in our people - highly accredited consultants, CREST and CHECK - approved penetration testers, and cyber specialists who don't just assess risk, but turn it into clear, strategic action. We combine technical rigour with practical, hands-on support through assessments, long-term advisory, and fully managed security services.

As an NCSC Cyber Advisor, Cyber Essentials certification body, and CREST-accredited partner, we've successfully delivered 1,500 Cyber Essentials and Cyber Essentials Plus certificates, helping businesses meet compliance and build long-term resilience. Protecting the Nation, Business and People.



Speak With an Expert

hello@cyberlab.co.uk

0333 050 8120

cyberlab

Learn more at **cyberlab.co.uk**