

Success Story

East Lothian Council

Building a Modern, Resilient Security Foundation for Public Services

East Lothian Council is a Scottish local authority responsible for delivering essential public services to thousands of residents, communities, and businesses across the region. With a growing digital estate and increasing pressure to maintain service availability, the council continues to strengthen its cyber security posture to protect sensitive information, uphold public trust, and ensure operational resilience.

As cyber threats targeting public sector organisations become more advanced, East Lothian Council recognised the need for a modern, proactive security operations capability that could provide deeper threat visibility and faster, more effective incident response. They chose CyberLab to implement industry-leading managed detection and response technology, providing 24/7 support that enhances their ability to identify, assess and respond to cyber threats in real time.

As part of their wider digital transformation journey, the council also sought a security partner that could provide long term operational resilience and support their ambition to modernise core services. CyberLab's consultative approach, combined with a deep understanding of public sector challenges and legacy environments, offered a clear path towards a more mature and sustainable security operations model. This ensured that East Lothian Council could strengthen protection of critical services while continuing to innovate and deliver for the communities they serve.



The Business Challenge

Improving Visibility, Speed and Operational Readiness in a Demanding Threat Landscape

Before partnering with CyberLab, East Lothian Council sought to enhance its ability to detect, investigate and respond to cyber threats round the clock across a diverse and complex IT environment.

Key requirements:

- Real-time visibility of malicious activity across the estate.
- Increased response speed to potential threats.
- Always-on security operations capability.
- Ability to meet short timescales to assess, procure and implement an advanced MDR solution.
- A partner with deep public sector understanding and the ability to support rapid deployment.
- A predictable total cost of ownership, with clear, consistent and transparent budgeting for long-term security operations.

East Lothian Council needed a solution to elevate its threat monitoring and incident response capability while supporting the unique operational demands of a local authority.



The Solutions

Establishing 24/7 Security Operations with Sophos Taegis MDR

Working closely with the council, CyberLab implemented Sophos Taegis Managed Detection and Response (MDR) as their new security operations foundation. Delivered as a fully managed service, Sophos Taegis MDR provides 24/7 threat detection, investigation and response, combining advanced telemetry with expert human analysis.

CyberLab supported the council throughout the entire process, including:

- A rapid procurement and proof of concept phase to meet urgent time requirements
- Full deployment and configuration of Sophos Taegis MDR across the environment
- Seamless onboarding designed to avoid operational disruption
- Ongoing strategic support and guidance tailored to public sector needs

To further strengthen their security posture, Sophos Taegis MDR provided several advantages not typically available from traditional SOC or SIEM based operating models. **The service delivers budget certainty and predictable total cost of ownership, eliminating SIEM build complexity, ingestion tuning effort, or unexpected consumption based charges. This ensured the council could access enterprise grade security operations without financial risk or operational overhead.**

Sophos Taegis MDR also accelerated the council's ability to detect and respond to threats. With access to Sophos security analysts 24/7/365, investigations are deeper, faster and more efficient, enabling threats to be contained swiftly and effectively.

By integrating Sophos Taegis MDR, East Lothian Council gained:

- Significantly enhanced visibility of threats across their digital estate
- Continuous monitoring supported by experienced CyberLab and Sophos analysts
- Faster and more confident responses to active security events
- Predictable, transparent long term operational costs
- Maximised ROI from existing cyber security tools through broad integration coverage
- A strengthened security operations model that reduces risk and supports resilience

The Outcome

Greater Confidence, Stronger Defences and a More Efficient Security Operation

The implementation of Sophos Taegis MDR has increased East Lothian Council's security capability, including round the clock. With real-time insights, expert guidance, and streamlined incident response, the council can focus on delivering essential services with greater confidence.

Key outcomes include:

- Improved threat visibility, providing deeper situational awareness across the environment
- Increased confidence in response capability, supported by expert MDR analysts
- Rapid and effective deployment, enabling protection to be operational in a short timeframe
- Reduced operational strain, with CyberLab acting as an extension of internal security staff
- Proactive vigilance and early threat identification, strengthening the council's overall security posture

The partnership has enabled East Lothian Council to modernise its approach to security operations, adopting a robust, future-ready MDR solution that supports a more resilient digital infrastructure.

“East Lothian Council has been working closely with CyberLab to strengthen our security operations capability. Their support in implementing Sophos Taegis as our managed detection and response (MDR) solution provided significantly improved visibility of threats across our environment and increased confidence in our ability to respond swiftly and effectively.”

The procurement process and proof-of-concept were progressed at an impressive pace, with CyberLab able to facilitate rapid turnaround and accommodate short-notice requirements without disruption. They provide added value through proactive vigilance. Beyond simply responding to a purchase order, consistently practical support, and a genuine understanding of local authority challenges.

CyberLab's team have been responsive, knowledgeable, and easy to work with throughout. Their expertise, combined with the capabilities of the Sophos Taegis MDR platform, has delivered tangible improvements overall security posture.”

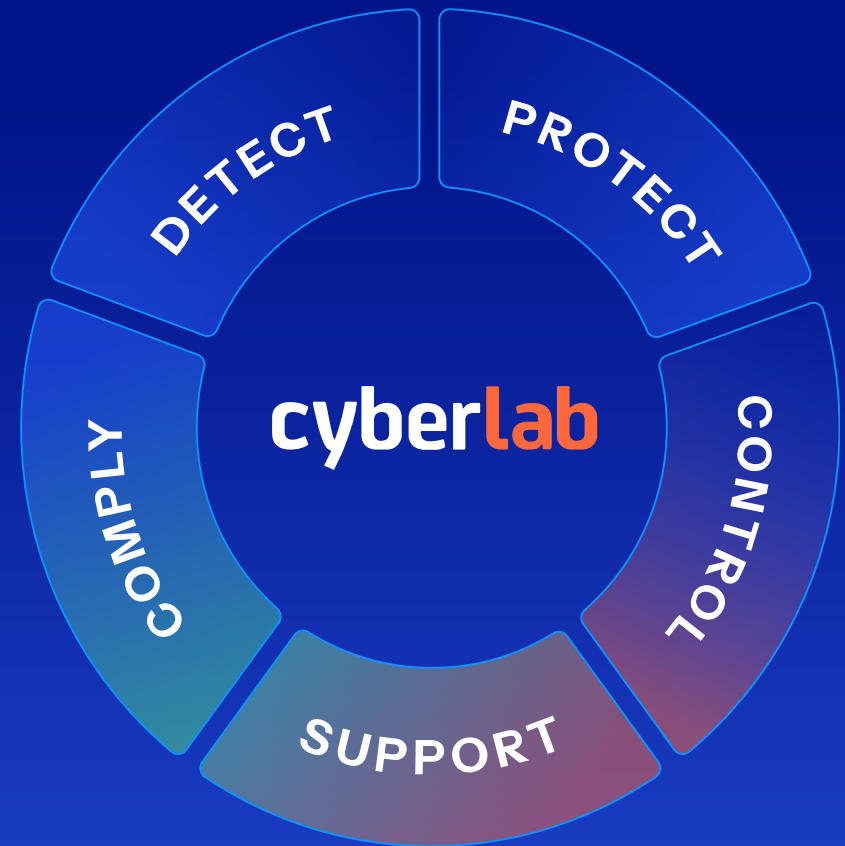
Graham Burke
Security and Infrastructure Manager
East Lothian Council

Protecting the Nation, Business & 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