## About us...

Lincolnshire Co-op is a long-standing, community-focused organisation proud to serve the people of Lincolnshire and surrounding counties. Our Support Centre, based in Lincoln, is the operational heart of our business. It's home to a range of specialist teams who work behind the scenes to support our front-line colleagues and ensure we deliver exceptional service across all our trading areas.

## **Essential Information –** what you need to know

| | |
|---|---|
| Job purpose: | - To uphold the confidentiality, integrity and availability of Lincolnshire Co-op assets by identifying, analysing and responding to cyber threats, while supporting the delivery of the cyber security strategy through proactive risk management, incident response and ongoing adherence to security controls.<br>- To promote a strong cyber security culture across the organisation through education, communication and awareness training. |
| You'll report to: | - Cyber Operations Manager |
| Your hours: | - 37.5 hours per week (FTE) |
| Your relationships: | - External 3rd parties included but not limited to: Cloud and SaaS providers, Consultants and Managed Security Service Providers.<br>- A wide range of internal and external contacts and collaborative partnerships with our Infrastructure, Application Support, Service Delivery and IT Solution Delivery Teams. |
| What you'll bring to us: | - Experience with Microsoft Azure / Entra ID / Intune for identity and access management, conditional access, and security configuration.<br>- Hands-on knowledge of Microsoft Defender for Endpoint or similar EPP/EDR solutions.<br>- Familiarity with SIEM platforms, preferably Google Security Operations (Chronicle) or equivalent (e.g., Sentinel, Splunk, etc.).<br>- Familiarity with ITIL or similar frameworks.<br>- Ability to work effectively in a team environment.<br>- Good communication and interpersonal skills.<br>- Proven experience as a Cyber Security Analyst or similar role.<br>- Solid understanding of threat detection, incident response, and vulnerability management principles.<br>- Ability to interpret and action insights from security tooling, alerts, and threat intelligence feeds.<br>- Strong knowledge of network security, including firewalls, proxies, and endpoint hardening. |

| | |
|---|---|
| What you’ll bring to us continued: | - Awareness of compliance frameworks (e.g., ISO 27001, Cyber Essentials, NCSC guidance).<br>- Excellent report writing capabilities with focus on communicating technical information to an audience with a non-technical background.<br>- Excellent problem-solving and analytical skills.<br>- Certifications/Qualifications such as: BSc in Cybersecurity, CompTIA Security +, (ISC)2  SSCP, CEH, GSEC, Microsoft SC-200 |

# Our Purpose

Bringing together energy, ideas and resources to make life better in our communities

## Together we are

Providing and supporting valued services

Helping to grow the local economy

Caring for our health and wellbeing

Looking after our local environment

## Your Purpose – I will contribute to **my team and the Society's ongoing success in this role by…**

Your duties and responsibilities:

- Monitoring, investigating, and responding to security events using the SIEM platform.
- Managing and maintain the EDR solution to ensure continuous protection, detection, and response to threats on endpoints.
- Administering and optimise Azure / Entra ID security configurations, including conditional access policies, identity protection, and MFA enforcement.
- Performing threat hunting and analysis across cloud and on-premise environments, leveraging data from EDR and SIEM tools.
- Supporting the delivery of the organisation's cyber security strategy, including risk assessments, incident response, and vulnerability management.
- Investigating and triage security alerts, providing recommendations for containment, remediation, and lessons learned.
- Collaborating with wider IS function and other business units to improve security posture and ensure alignment with internal policies and ensuring best practice by aligning cyber activities to recognised frameworks. (e.g., ISO 27001, Cyber Essentials).
- Maintaining and improve documentation, including standard operating procedures (SOPs), incident reports, and technical configurations.
- Staying current on evolving threats, vulnerabilities, and trends to proactively enhance the organisation's cyber defence capabilities.
- Supporting the incident management process by providing a timely and effective resolution of cyber security related incidents.
- Collaborating with the wider IT teams to identify root causes and implement corrective actions to prevent further reoccurrence
- Maintaining comprehensive documentation for cyber security processes and toolsets
- Working with suppliers to resolve technical issues or enhancements.
- Assisting in evaluating supplier performance to ensure adherence to service agreements.

# Our Approach

Our way of thinking about the purpose of what we do

## Together we THRIVE

- Trustworthy – we do what we say we'll do and trust others to deliver to the best of their ability
- Helpful - we support and challenge each other collaboratively, no matter the role or level.
- Respectful - we listen to other views and opinions with consideration and celebrate differences.
- Inspiring - we role model what good looks like and lead by example to be better.
- Valued - we recognise achievements and appreciate everyone's contributions.
- Empowered - we listen and encourage each other to take opportunities.

## **Your Approach –** how you will contribute to **your team and the Society's ongoing success in this role.**

| | |
|---|---|
| I will be trustworthy by: | - Handling sensitive security information responsibly while maintaining confidentiality and transparency.<br>- Using sound judgement when investigating incidents and responding to threats,<br>- Taking ownership for maintaining secure systems and reliable cyber analysis.<br>- Collaborating with colleagues to protect organisational systems, data, and users. |
| I will be helpful by: | - Responding promptly and professionally to security alerts, incidents, and support requests.<br>- Providing clear guidance on security risks, remediation actions, and best practices.<br>- Sharing cyber security knowledge to support colleagues in secure working practices.<br>- Supporting teams to improve cyber resilience and effective threat response |
| I will be respectful by: | - Communicating security risks clearly, considering different technical knowledge levels.<br>- Treating colleagues professionally when addressing cyber risks, incidents, and concerns.<br>- Supporting an inclusive environment across cyber security, IT, and business teams.<br>- Applying security policies consistently, fairly, and aligned with organisational standards. |
| I will inspire others by: | - Promoting strong cyber hygiene and secure working practices across teams.<br>- Demonstrating professionalism and diligence when monitoring and investigating cyber threats.<br>- Continuously learning about emerging threats, vulnerabilities, and cyber technologies.<br>- Building positive relationships to support the organisation's cyber security strategy. |
| I will value people by: | - Providing practical cyber security advice and support to colleagues when needed.<br>- Encouraging secure behaviours and awareness across all teams and departments.<br>- Promoting collaboration to help protect organisational systems and sensitive information.<br>- Being approachable and supportive regarding cyber security questions or concerns. |
| I will empower others by: | - Encouraging colleagues to follow cyber security policies and best practices.<br>- Providing clear guidance to help teams identify and manage cyber risks.<br>- Supporting colleagues in developing cyber awareness and security responsibilities.<br>- Proactively improving security processes, controls, and organisational cyber resilience. |