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:	- Embedding security into the design and delivery of systems and projects to strengthen the organisation's security posture and support progression towards a Zero Trust model. - Identifying and remediating vulnerabilities across the IT estate, improving control maturity, and supporting effective incident response activity while ensuring security is built in from the outset and balanced with usability and operational efficiency.
You'll report to:	- Cyber Operations Manager
Your hours:	- 37.5 hours per week (FTE)
Your relationships:	- Engaging with external providers including cloud, SaaS vendors, consultants, and MSSPs to support secure design, remediation, hardening, and incident response activities. - Collaborating with internal teams including Infrastructure, Application Support, Service Delivery, IT Solution Delivery, SOC, GRC, and business stakeholders to embed security and support delivery.
What you'll bring to us:	- Experience as a Cyber Security Engineer, Infrastructure Security or similar technical security role - Managing Azure, Entra ID (Azure AD), and identity security controls including Conditional Access - Implementing Zero Trust principles, including MFA and device compliance integration - Working with Active Directory in hybrid environments - Securing network infrastructure (firewalls, switches, wireless environments) - Using Microsoft Intune and endpoint security controls (including ASR rules) - Using tools such as NinjaOne or equivalent RMM platforms - Supporting incident response and acting as technical escalation point (SOC Tier 3 level) - Mapping security posture against frameworks such as CIS, NIST, or ISO 27001 - Translating technical risks into clear, understandable business language - Experience in retail, co-operative or multi-site environments

What you'll bring to us continued:	- Experience with Windows Hello for Business, SSO, and modern authentication methods - Experience in security architecture or secure design review activities - Experience with automation and scripting (e.g. PowerShell) for remediation and deployment - Experience working with GRC teams or security assurance frameworks - Continuously learning and adapting to emerging cyber security threats and technologies - Demonstrating strong commitment to protecting systems, data, and organisational services

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:	- Acting as a security consultant for in-flight and projects, ensuring security is embedded from design through to delivery and not applied retrospectively - Reviewing architectural designs to ensure security controls are embedded - Evaluating third-party integrations and vendor solutions to ensure compliance with internal security and data protection standards - Identifying and remediating security issues in live projects prior to production release, providing clear corrective guidance to delivery teams - Supporting estate-wide security control gap analysis in collaboration with GRC, aligned to frameworks such as CIS, NIST, and ISO 27001 - Driving improvements in Microsoft Secure Score and Azure Security Benchmark through remediation activity - Designing and auditing Conditional Access Policies to strengthen identity security and support Zero Trust adoption - Implementing device compliance and authentication controls, including phishing-resistant MFA - Designing secure-by-default controls that balance security requirements with usability and productivity - Implementing frictionless security solutions such as SSO and Windows Hello Translating technical security requirements into clear business context to support understanding and adoption - Reducing user friction while maintaining a strong security posture across systems and services - Implementing and tuning Attack Surface Reduction rules via Microsoft Intune to reduce malware risk - Managing patching and configuration hardening across the estate using NinjaOne and Intune, including PowerShell-based remediation - Identifying and remediating vulnerabilities identified through audits and security assessments - Strengthening endpoint and infrastructure security across the organisation - Acting as Tier 3 escalation point for complex security incidents raised by SOC and internal analysts - Providing technical expertise to support containment, investigation, and resolution of security incidents - Supporting root cause analysis and driving preventative actions following security events - Contributing to continuous improvement of incident response capability - Deputising for the Cyber Operations Manager during periods of absence or escalation demand, ensuring continuity of cyber operations leadership and decision-making

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, architecture, and vendor information responsibly with confidentiality and transparency. – Using sound judgement when reviewing designs, assessing risks, and responding to incidents and threats. – Taking ownership for securing systems, configurations, and effective cyber risk analysis and remediation. – Collaborating across teams and partners to protect systems, data, and services.
I will be helpful by:	– Responding promptly and professionally to security issues, alerts, incidents, and project risks. – Providing clear guidance on vulnerabilities, remediation actions, and secure design best practice. – Sharing cyber security knowledge to support secure delivery and resilience. – Supporting teams to strengthen cyber defences, incident response, and risk mitigation.
I will be respectful by:	– Communicating security risks clearly for different technical understanding levels. – Treating colleagues professionally when addressing risks, incidents, and controls. – Supporting an inclusive and collaborative approach across cyber security, IT, and business teams. – Applying security standards and policies consistently and fairly.
I will inspire others by:	– Promoting strong cyber hygiene, secure design, and proactive risk reduction. – Demonstrating diligence when investigating threats, vulnerabilities, and security events. – Continuously learning about emerging threats, vulnerabilities, and security technologies. – Building relationships that support a culture of security and improvement..
I will value people by:	– Providing practical cyber security guidance to support safe working practices. – Encouraging secure behaviours and awareness across all teams. – Promoting collaboration to protect systems, data, and services. – Being approachable and supportive when security concerns arise.
I will empower others by:	– Enabling colleagues to follow security policies and secure-by-design principles. – Providing clear advice to help teams identify and manage cyber risks. – Supporting cyber awareness and shared security responsibility across the organisation. – Improving controls, processes, and resilience through continuous enhancement and remediation.