

COVENTRY Building Society Group				ROLE PROFILE					
				Senior Cyber Security Technical Specialist					
Reports to:		Senior Manager – Cyber Security							
Grade:		Senior Professional / Technical			Job Family:		IT Cyber Security		
Leadership Responsibility:		Direct Reports:	0	Indirect Reports:	0	Regulatory Information:		Not Applicable	
Location:		Binley, Coventry. Manchester NW. Team-led hybrid working arrangements apply.			Working hours:		35 plus on call		
Effective Date:		V1 14/09/2026			WD Job Code:		JC_1338		
ABOUT THE ROLE									
The Senior Cyber Security Technical Specialist is responsible for the continuous monitoring, detection, analysis, investigation, and response to cyber security threats, vulnerabilities, and security incidents across the organisation. The role holder will leverage a broad understanding of security technologies, threat intelligence, and security operations processes to identify, assess, and mitigate cyber risks. The role requires strong analytical and technical capabilities to correlate data from multiple security platforms and business systems, enabling effective threat detection, risk assessment, and incident management. The role holder will lead the development, optimisation, and tuning of security monitoring and detection capabilities, ensuring cyber threats are identified and responded to in a timely and effective manner. The Senior Cyber Security Technical Specialist will support the continual enhancement of the organisation's security posture through the implementation of security controls, improvement of detection use cases, coordination of incident response activities, and the assurance that operational and change initiatives comply with organisational security standards, legal obligations, and regulatory requirements.									
ABOUT YOU									
You are a highly skilled cyber security specialist who thrives on solving complex technical challenges. You have a proven track record within a Security Operations Centre (SOC)—ideally in a regulated or financial services environment—and are ready to step up as a senior technical authority. As a skilled technical specialist, you bring deep expertise in security technologies, governance, and assurance. You don't just monitor threats; you proactively drive change and continuous improvement to mature our defence capabilities. To succeed in this role, you must be comfortable working dynamically, which includes participating in an on-call rota to provide escalation support and mentor colleagues during critical incidents.									
REQUIREMENTS:									
• Experience operating within a Security Operations Centre (SOC) in a complex enterprise environment. • Experience within the Financial Services sector, with an understanding of emerging threats, regulatory expectations, industry developments, and challenges facing the UK retail financial services market. • Strong knowledge of SIEM, EDR/XDR, threat intelligence, and security monitoring technologies. • Proven ability to investigate complex security incidents, conduct impact assessments, and coordinate effective incident response activities. • Experience of cloud security operations, including monitoring, detection, investigation, and incident response within cloud-hosted environments is desirable. • Understanding of cyber security frameworks, regulatory requirements, and industry best practices relevant to Financial Services such as NIST, ISO 27001, CobiT, ITIL. • Professional cyber security certification(s) such as CISSP, CEH, GCIH, GDAT, GCDA, GCFR, CREST, or equivalent industry-recognised qualifications are desirable.									

YOUR KEY RESPONSIBILITIES. (Additional detailed performance objectives will be set by your manager)	
General Profile	Security Monitoring & Detection • Monitor, investigate, and analyse security events, alerts, and anomalous activities across enterprise environments. • Develop, implement, maintain, and optimise threat detection use cases, correlation rules, and security monitoring capabilities within SIEM, EDR, NDR, and other security platforms. • Continuously tune security controls and detection content to improve threat visibility, reduce false positives, and enhance operational efficiency. • Leverage threat intelligence and emerging threat information to strengthen monitoring and detection capabilities. Incident Response & Investigation • Lead and coordinate the investigation, containment, eradication, and recovery activities associated with cyber security incidents. • Conduct detailed root cause and impact assessments for security incidents and suspected compromises. • Provide technical expertise during major security incidents and contribute to post-incident reviews and lessons learned activities. • Ensure incidents are managed in accordance with defined processes, service levels, and regulatory obligations. Security Engineering & Continuous Improvement • Design, implement, and enhance security controls that protect the organisation against cyber threats, vulnerabilities, and emerging risks. • Identify opportunities to automate detection, investigation, and response processes using security orchestration and automation capabilities. • Support the evaluation, implementation, and optimisation of security technologies and security monitoring platforms. • Drive continuous improvement of cyber defence capabilities through metrics, threat-led assessments, and operational feedback.
People & Relationships	• The role holder will work closely with business and technology stakeholders to ensure security requirements are appropriately considered within operational activities, projects, and change initiatives. Provide technical guidance and mentoring to colleagues within the Cyber Security Operations function. • Contribute to cyber security awareness and incident preparedness activities across the organisation. • Collaborate with internal teams to support the investigation and resolution of security incidents, vulnerabilities, and emerging cyber threats. • Develop and manage relationships with key third-party suppliers, managed security service providers, and technology vendors, ensuring the timely escalation and resolution of technical issues, effective delivery of services, and alignment with organisational security requirements
Governance, Risk & Controls	• Assess and communicate security risks identified through monitoring, investigations, and vulnerability management activities. • Ensure cyber security operations activities are conducted in accordance with organisational policies, security standards, legal obligations, and regulatory requirements. • Support audit, compliance, and assurance activities by providing evidence and operational expertise.
Impact, Scale & Influence	• The role holder will directly protect our estate from sophisticated threats by solving complex technical challenges and optimizing core security technologies. The role holder will drive continuous improvement will directly shape, automate, and mature our incident response capabilities. • The role holder will be comfortable operating in a fast-paced, highly regulated financial environment. The role holder will manage advanced alert queues, oversee complex technical changes, governance, and maintain a flexible approach to operational hours to secure our large-scale infrastructure.

	Lead technical expertise, the role holder will act as a mentor to Tier 1/2 analysts and a trusted advisor on assurance frameworks. The role holder will leverage excellent communication skills to lead collaboration across teams and champion an effective, supportive security operations function.
Decision Making / Problem Solving	The role holder is responsible for making day-to-day operational decisions relating to cyber security monitoring, threat detection, incident response, and the configuration and optimisation of security controls and technologies. They will assess risks, determine appropriate response actions, and provide expert recommendations on security improvements, emerging threats, and technology capabilities. The role holder will influence technical and operational decisions through specialist advice and guidance, while strategic, financial, policy, and risk acceptance decisions remain the responsibility of Cyber Security leadership and senior management.
Comparable Roles	N/A