`

Job Title	Security Engineer
Department	Cyber Resilience Team
Reports to	Cyber Resilience Manager
Grade	Technical Tier 1
Purpose & Overview	Deliver hands-on cyber security services ensuring the effective operation and continuous improvement of enterprise-wide Security Operations capabilities, including threat monitoring, vulnerability management, security engineering, identity and access management, security assurance, and cyber resilience activities across IT, cloud and OT (Desirable) environments.
Key Accountabilities	• Work with the Cyber Security Team to enhance the organisation's threat monitoring, detection, and incident response capabilities. • Own the implementation, maintenance, and continuous improvement of the cyber security estate, covering user, infrastructure, cloud, application, and OT assets. • Support alignment with the NCSC Cyber Assessment Framework (CAF) by implementing and maintaining technical controls mapped to CAF outcomes and contributing evidence for assessments. • Consult on, administer, and secure Microsoft Entra ID, including Conditional Access, Identity Protection, and Privileged Access Management (PAM), ensuring effective identity and access management controls are implemented and maintained. • Implement and maintain security controls for the Microsoft Fabric analytics platform. • Deploy, configure, and maintain vulnerability scanning tools and services to support the identification and remediation of security vulnerabilities. • Ensure appropriate documentation is maintained to support current and future security operations, onboarding activities, audits, and knowledge transfer within the team. • Act as the SME and trusted advisor for security technologies and products, representing Cyber Technology at governance boards and key stakeholder forums. • Collaborate with IT, OT, and key stakeholders to drive a cohesive and risk-based approach to cyber security across the organisation. • Provide expert security consultancy and assurance to WWU projects and programmes, delivering support on both a planned and ad hoc basis.

`

	• Mentor less experienced members of the team, supporting their personal and professional development and helping to build capability within the function.
Technical Know-How & Skills	• Deep, hands-on experience with the Microsoft Defender Suite (Defender for Endpoint, Defender for Identity, and Defender for Cloud), alongside Microsoft Purview for information protection and Microsoft Sentinel for SIEM and SOC capabilities. • •Strong knowledge and experience of establishing secure, well-governed Azure environments, implementing baseline policies, controls, and governance structures. • Strong technical knowledge of Azure services and architecture, including networking, identity, storage, and compute, and how security controls are applied across them. • Practical experience deploying and maintaining vulnerability scanning capabilities using tools such as Tenable, Intruder, and Microsoft Defender for Endpoint across cloud, network, endpoint, infrastructure, and OT environments. • Working knowledge of securing the Microsoft Fabric analytics platform, including workspace governance, OneLake data access controls, and integration with Microsoft Purview (Desirable). • Demonstrates a mindset that security exists to enable the business while appropriately managing risk. • Strong critical thinking and analytical skills, with the ability to break down complex problems, identify root causes, and determine risk-proportionate solutions. • Able to adapt quickly to the evolving cyber threat landscape, maintaining awareness of emerging risks, technologies, and industry developments. • Background in systems administration or engineering, providing a practical understanding of how systems are designed, implemented, operated, and fail under real-world conditions. • Experience working within project teams, influencing architecture and design decisions to ensure security is embedded throughout the delivery lifecycle. • Practical experience implementing and maintaining data security controls, including data loss

`

	prevention, classification, and protection policies within Microsoft Purview and related platforms. • Able to apply the NCSC Cyber Assessment Framework (CAF) and other recognised frameworks, such as ISO 27001, NIST CSF, and CIS Controls, to assess security posture, identify control gaps, and support continuous improvement.
Qualifications	<u>Essential</u> • Bachelor's degree in Cybersecurity, Information Technology, Computer Science or related field. • Proven experience in a security engineer role • Strong communication and interpersonal skills • CompTia Sec + • SC-200 (Security Operations Analyst) <u>Desirable</u> • GIAC (Desirable) • SC-400/1 (Information Protection Admin) • AZ-500 (Azure Security Engineer) • MS-102 (Microsoft 365 Administrator)