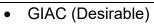


Job Title	Cyber Security Analyst
Reports To	Security Operations Manager
Grade	Grade 4
Purpose	The role holder will be expected to work with the Cyber Resilience team and assist with the delivery of enterprise-wide Security Operations function including EDR, SIEM, vulnerability scanning, gathering security control framework evidence and general day to day assistance with security tasks and incidents.
Key Accountabilities	 This is a technical role and will require knowledge and understanding of attack and exploitation techniques and adversarial TTP's. Work with the Cyber Security Team to provide resilience to our threat monitoring and response capabilities. Handle security Incident response with internal teams and other third parties to ensure that incident response lifecycle is undertaken to a high standard. Monitor and respond to security incidents, alerts and breaches Monitor and track remediation to all identified vulnerabilities Monitor the risk to WWU assets (people, infrastructure, data etc) using security tooling to carry out routine checks. Monitor and report on user behavioural analysis such as awareness training and social engineering campaigns. Gather evidence to support security control audits to support testing and assurance around the adequacy of controls. Ensure tooling is maintained and licenses are renewed within a timely manner. Input into regular testing of WWU's Security Incident Response Plan (for both Cyber IT and Cyber OT)
Technical Know- How & Skills	 Good knowledge and understanding of SOC processes and procedures. Basic experience using SIEM systems such as MS Sentinel. Good understanding of incident response and incident handling. Basic knowledge or experience using leading endpoint detection and threat management products as well as managing their operation. Good knowledge and awareness of global Information Security Standards including ISO27002, CIS, NCSC CAF, NIST CSF. Previous experience being part of or working with incident response teams. A knowledge of and experience handling OT/ICS environment security incidents is desirable but not essential.
Qualifications	CompTIA Sec + (Essential)



- CEH (Desirable)
 AZ-900 (Desirable)
 SC-900 (Desirable)
 SC-200 (Desirable)
 SIEM certification (Desirable)
 Blue Team Level 1 (Desirable)

