Job Title	Incident Response Analyst
Department	Cyber Resilience Team
Reports to	Cyber Threat Intelligence Expert
Grade	Grade 5
Purpose & Overview	– This position plays a crucial part in enhancing WWU's cyber resilience by providing actionable insights, informing decision-making, and proactively contributing to mitigating potential threats. – The Incident Response Analyst collaborates with various teams, both internal and external, to ensure a comprehensive understanding of the threat landscape and WWU's response to any incidents. – Often working within the security operations centre (SOC), the primary responsibility of an incident responder is to rapidly investigate and document cybersecurity incidents within an organization. – Once a possible incident has been identified, the incident responder is tasked to investigate events and mitigate potential impact. – As a member of the CSIRT, the incident responder works closely with the enterprise's security organization to categorize and classify attack methods and intended payloads in support of an effort to build protection for further similar incidents.
Key Responsibilities	– Monitor and analyse network traffic, system logs, and other data sources to identify potential security incidents. – Investigate alerts and suspicious activity to determine if an incident has occurred. – Contain affected systems and networks to prevent the incident from spreading. – Implement temporary measures to mitigate the impact of the incident. – Work with other teams, such as IT and security operations, to develop and implement a containment strategy. – Analyse incident data to determine the root cause of the incident and identify recommendations for improvement. – Document and report incidents to the incident response team and other relevant stakeholders. – Develop and implement security plans, policies, and training to prepare the organization to respond efficiently and effectively to cyber threats.
Technical Skills	– Experience in a similar role, ideally some of which has been spent in a CNI environment.
Qualifications	<u>Essential</u>: – Proven experience operating in a SOC or a related cyber security role. – In-depth knowledge of cyber threats, threat intelligence frameworks and cyber security best practice. – Strong analytical and problem-solving skills. – GIAC Certified Incident Handler <u>Desired</u>: – Bachelor's or master's degree in cyber security or related field. – Other relevant cyber security certifications

Additional Information	– Vetting