**Ops Information Security Analyst**

**Job Introduction (the opportunity)**

The Security Operations Analyst is responsible for the continual monitoring of our Cyber security platforms and tools to identify Cyber Security threats, investigate and triage alerts and carry out appropriate containment actions, ensuring the protection of the WG&S IT systems and digital assets. This role demands a strong understanding of cybersecurity threats, the ability to analyse security data, and the skills to respond effectively to security incidents.

**Main Responsibilities (what you’ll be doing)**

* Security Monitoring and Incident Detection: Continuously monitor security alerts and events to identify potential threats. Investigate and analyse security alerts to determine their impact and scope, utilize security information and XDR platform for real-time threat detection.
* Security Incident Triage: Evaluate and prioritize security alerts based on severity and potential impact. Determine false positives and escalate genuine threats for further investigation.
* Incident Response and Resolution: Act promptly to contain and mitigate security incidents. Document incident details, actions taken, and lessons learned for post-incident analysis. Collaborate with cross-functional teams to coordinate incident response efforts.
* Threat Intelligence and Analysis: Stay informed about the latest cybersecurity threats and vulnerabilities. Analyse threat intelligence data to enhance proactive threat detection and prevention measures.
* Security Reporting and Documentation: Generate reports on security incidents, trends, and vulnerabilities. Maintain accurate incident records and contribute to the organization's incident response plan.
* Vulnerability assessment and penetration testing: Conduct regular security assessments to identify vulnerabilities and weaknesses in the infrastructure and applications.
* Provide 24x7 support for responding to Cyber security incidents, out of hours support (On call rota)

**Our Ideal Candidate (about you)**

Technical Skills:

* Proficiency in using security tools and software for monitoring and analysis.
* Knowledge of operating systems, network protocols, and cloud security.
* Familiarity with security assessment tools and techniques.

Cybersecurity Expertise:

* Strong understanding of cybersecurity principles, threats, and attack vectors.
* Familiarity with security technologies such as firewalls, intrusion detection systems, and SIEM tools.

Incident Response:

* Experience in handling security incidents, including containment and eradication.
* Familiarity with incident response frameworks and methodologies.

Communication Skills:

* Effective communication skills to report incidents to management and cross-functional teams.
* Collaborative approach to work with other team members.

Attention to Detail:

* Keen attention to detail to identify anomalies and threats within security data. Thorough documentation of incident findings and actions taken.

The role holder should hold one or more relevant industry qualifications. Examples are:

* Cyber related degree or relevant experience
* 2 years’ experience in a Cyber Security focused role
* Cyber Security professional certifications advantageous for example, CISSP, CREST, ISACA, GIAC.