Job Description – Senior Security Operations Analyst

Department	Technology & Change, Information Security
Grade	13
Reporting to	Security Operations Manager
Direct reports (yes or no)	No
WTW Code	AFY637 P3 13

Job Purpose

- As a senior member of the Information Security Operations team (SecOps), you will maintain the confidentiality, availability, and integrity of MIB's information and information systems.
- This will primarily be achieved through identification and mitigation of risk through identification and prevention of threats and incident management.
    - Delivery of the 'run' state for the security technical systems, services and defenses at MIB.
    - Rapid response, detection, investigation, isolation and remediation of information security incidents.
    - Root-cause identification through expert forensic and security knowledge.
    - Research within the security community and MIB technologies and industry to enable detection and rapid response to threats.
    - To provide a focal point within MIB for technical information security expertise.
    - Deputise for the Security Operations Manager whenever required, due to workload or absence.
    - Lead major security incidents in MIB.

Key accountabilities

- Manage the Threat Intelligence platform, ensuring that the service is operational and constantly updated with MIB security profile monitor cyber threats and media reports against MIB's security profile to ensure that MIB technical controls are appropriate.
- Design, implement and monitor automatic security response with SOAR platform.
- Manage and operate 'Run' state of Information Security (technical) systems.
- Rapid response, detection, isolation and remediation of information security incidents.
- Leading / working with problem management teams on mitigation and incident prevention activities.
- Maintaining forensics capabilities in the identification, containment, eradication and root-cause of security threats. Be able to examine Malware using both static and dynamic methods to enhance detection capabilities.
- Lead and assign Threat Hunting activities – adding detection capabilities to security tools.
- To establish and maintain security technical standards, procedures, and guidelines.
- To provide Technology & Change teams with security focused technical support, training and consultancy to ensure compliance with security standards, policies and legislation.
- Be an expert in MIB services areas such as Cloud & end user computing to enable effective liaison with other technical groups and the coherent protection of MIB services.
- Develop and operate procedures that counteract potential threats/vulnerabilities.
- To provide a focal point within MIB for technical information security expertise.
- Assist in the rapid execution of information security initiatives by maintaining an appropriate level of prioritisation, focus and persistence in an environment of significant change and growth.
- Keep abreast of emerging trends, technologies and legislation in security and industry.
- Mentor other members of SecOps team, Information Security and wider business.
- Establish mechanisms, behaviors, and culture to encourage the protection of MIB information and information systems.
- Operating as a member of 'one team' within MIB working towards a common goal that supports a great business outcome.
- Subject Matter Expert on a range of security technologies used by MIB.
- On-Call (Out of hours support) ensuring 24/7 security cover of MIB services.

Role requirements

- Great technology experience and expertise across a wide range of security technical products and services.
- Thorough understanding of the Information security threat landscape, significant risks, technical developments and directions.
- Expertise in Microsoft Azure platforms and security stack and third party components.

Role requirements
• Strong interpersonal skills are essential, as the jobholder must be able to operate effectively at all levels within and outside of MIB. • Extensive experience in an IT Security/IT Operations, or equivalent position. • An excellent understanding of Tactics, Techniques, and Procedures (TTPs). • Proven experience in writing Information Security Standards, procedures, and guidelines. • Ability to conduct and direct research into threats and vulnerabilities and preventative capabilities. One or more of the following qualifications are highly desirable. • Industry Standard Certifications (CompTIA, SANS, ISC2) • Vendor technology trained (certifications) e.g., Web Application Firewall, Web proxy, Microsoft Azure security, Email security management etc