Job Description – Vulnerability and Patching Specialist

Department	Service Delivery
Grade	G 13
Reporting to	Service Manager
Direct reports (yes or no)	No
WTW Code	AIC000-P4-13

Job Purpose

- To be the primary point of contact for managing information security vulnerabilities on end user devices, servers and 3rd party desktop applications across the Business.
- To create, own and manage the framework for managing the application estate, ensuring only agreed versions of applications are in use, and a roadmap for version upgrades
- To be accountable for the management of the software catalogue to ensure only approved software applications are used across the Business.
- To create and manage a best practice vulnerability management process to protect against the exploitation of known/detected vulnerabilities

Key accountabilities

- Manage vulnerability scans in conjunction with the Security Operations team against agreed SLAs, on all endpoints and 3rd party desktop applications used in MIB's estate.
- Engage with the wider business functions to establish a catalogue of approved software and a process to manage the list effectively to include removal and blocking of non-permitted applications as well as an approval process for new software requests.
- Engage with the wider business to establish and effectively manage the version control of software being used across MIB's estate so that only the latest / single version is used unless otherwise approved
- Establish and manage an exceptions process with appropriate approvals for any deviations from approved software versions or patching levels
- Establish a framework to manage the application estate to ensure only agreed versions of applications are in use.
- Create and maintain a roadmap to ensure MIB's technology estate remains secure and on supported versions of applications and operating systems.
- Conduct research on the latest security threats and remediation activity to protect MIB against these threats

Key accountabilities

- Remediate critical, high and medium vulnerabilities in line with SLAs, utilizing agreed patching tools and direct user and supplier contact as appropriate
- Engage with 3rd parties (either directly or through Product owners) to maintain an agreed level of vulnerability management on their applications or servers.
- Document and verify all 3rd party patching arrangements.
- Proactive support Procurement, Legal and Contract Owners in identifying gaps in contracts relating to vulnerability management and patching needs for new contracts and renewals
- Work closely with TPRM and Third-Party Relationship Owners to deliver accurate reports and assessments to support 3rd party performance reviews
- To work closely with the Information Security team in managing and reporting on the security posture of our IT estate and performance against agreed SLAs
- Work closely with the Infosec team to ensure vulnerability management, the role and solution development occurs in line with their requirements
- Work with Third Party providers for outsourced services to ensure vulnerabilities are reported, patched and managed within agreed best practice timelines.
- Work alongside procurement and Third-Party Risk Management teams to identify gaps in contracts related to management and mitigation of vulnerabilities
- Deliver and support production of timely management information as agreed
- Promote awareness and education across the Business and support project and support teams to deliver within security requirements
- Work within the MIB Change Management Framework to deploy updates, patches and configuration changes
- Identify and document any gaps in patching on end user devices, servers and 3rd party desktop applications across the Business

Role requirements

- Fundamental knowledge of core cybersecurity concepts and experience of their practical application
- Experience of creating and managing patching frameworks across company estates including 3rd party application management
- Experience of supporting the inclusion and review of vulnerability management and controls in supplier contracts
- One or more of the following qualifications are highly desirable: Microsoft MCP/MSCA/ CISSP
- Experience of managing and supporting windows operating systems, M365 and MAC Operating systems
- Experience of Cloud based security tooling and vulnerability management systems (Intune, Defender, Sentinel, Nessus, Tenable, Qualys)
- Experience of using and managing patching tools such as Autopatch and Kandji
- Experience of using desktop management tooling such as SCCM and Intune and remote desktop tooling to apply patches and resolve issues
- Technical background in Microsoft Windows systems, Cloud security technologies, and network architectures
- Understanding of threat actors with the ability to articulate how they operate and demonstrate how they subvert common security controls
- Knowledge of application exploits and vulnerabilities. Knowledge of ports and services typical in the configuration of web servers, file servers, and workstations
- Excellent communication skills
- Ability to analyze and manage data
- Experience in producing performance, analysis and solution focused reports for senior management
- Effective team working, collaboration and experience of coaching and mentoring.