**Job Objective:**

* To strengthen the Pixlr Group’s cybersecurity posture by implementing robust, scalable security solutions aligned with SaaS and cloud-native environments.
* To minimise organisational risk exposure and ensure business continuity through proactive threat management, incident response, and compliance alignment.

**Job Scope:**

* Security architecture and implementation
* Threat detection and incident response
* Vulnerability and risk management
* Compliance, audit, and security policies
* Security automation and tooling
* Cross-functional technical collaboration

**Job Description:**

1. Security Engineering & Architecture
   1. Implement and maintain advanced security solutions (e.g., SIEM, endpoint protection, firewalls, IDS/IPS).
   2. Configure, monitor, and fine-tune security infrastructure and tools.
   3. Support the design of secure cloud-native and hybrid IT architectures.
   4. Collaborate with development and operations teams to integrate security measures into systems and applications.
2. Threat Detection & Response
   1. Monitor alerts and security events, analysing threats.
   2. Lead incident investigations and response strategies.
   3. Track and apply threat intelligence to enhance defences.
   4. Conduct regular vulnerability assessments and penetration tests.
   5. Develop and implement remediation plans for identified risks.
3. Governance, Risk & Compliance (GRC)
   1. Perform technical risk assessments on systems and networks.
   2. Recommend and implement appropriate security controls.
   3. Implement and enforce security policies and compliance practices (e.g., ISO 27001, SOC 2).
   4. Support audit readiness and compliance reporting.
4. Security Automation & Tooling
   1. Develop and maintain automation tools/scripts (e.g., SOAR, automated patching).
   2. Enhance operational efficiency and response capability through scripting and workflow automation.
5. Collaboration & Documentation
   1. Maintain security documentation, including configurations, incident logs, and technical reports.
   2. Partner with cross-functional teams to embed security in operations.
   3. Contribute to internal security knowledge sharing and awareness initiatives.
6. Accept all other duties as assigned by the Line Manager or any of its authorised officers.

[This Remaining Space Has Been Left Blank Intentionally]