Job Title: Senior Identity & Access Management (IAM) Engineer

OM Soft is seeking an experienced Senior Identity & Access Management (IAM) Engineer to join our Cybersecurity and Technology team. Identity is the foundation of modern security, and this role is critical to protecting systems, data, and digital services across the enterprise. The IAM team designs, implements, and manages secure, scalable identity solutions using cloud-native, zero-trust, and automation-driven security architectures, enabling secure access for employees, partners, and customers.

Roles and Responsibilities:

- Design, implement, and manage enterprise IAM solutions across Azure AD (Entra ID), AWS IAM, and other cloud platforms.
- Lead the implementation of Single Sign-On (SSO), Multi-Factor Authentication (MFA), Privileged Access Management (PAM), and Identity Governance & Administration (IGA).
- Integrate IAM solutions with on-premise, cloud, and SaaS applications using SAML, OAuth 2.0, OpenID Connect, and SCIM.
- Define and enforce identity lifecycle management processes including joiner, mover, and leaver workflows.
- Implement Zero Trust and Least Privilege Access security models.
- Develop and maintain role-based and attribute-based access control (RBAC / ABAC).
- Automate identity provisioning and deprovisioning using APIs, scripting, and CI/CD pipelines.
- Collaborate with security, cloud, and application teams to embed IAM controls into system architectures.
- Monitor and audit access controls to ensure compliance with security policies, regulatory standards, and industry frameworks.
- Support incident response and access reviews related to identity and access.
- Maintain IAM documentation, standards, and operating procedures.
- Mentor junior engineers and contribute to IAM best practices and governance frameworks.

Skills and Experience Required:

- Strong hands-on experience with IAM platforms, such as: Azure AD (Entra ID), Okta, Ping Identity, ForgeRock, AWS IAM
- Proven experience implementing SSO, MFA, PAM, and IGA solutions.
- Strong understanding of authentication and authorization protocols (SAML, OAuth2, OpenID Connect, LDAP).
- Experience with PAM tools such as CyberArk, BeyondTrust, or Azure PIM.
- Knowledge of identity governance, access certifications, and compliance reporting.
- Experience integrating IAM with cloud platforms, SaaS, and on-premise systems.
- Proficiency in scripting and automation (PowerShell, Python, Bash).
- Experience with DevSecOps, CI/CD pipelines, and Infrastructure as Code (Terraform, ARM, CloudFormation).
- Strong understanding of security frameworks (Zero Trust, NIST, ISO 27001).
- Experience working in Agile / Scrum / SAFe environments.
- Excellent problem-solving and communication skills.

Education Requirements:

- Bachelor's degree (S/NQF6 or above) in Computer Science, Cybersecurity, Information Systems, Engineering, or a related discipline.

Other Details:

- Salary: Competitive salary offered.
- Working Hours: 37.5 hours per week (Monday to Friday)
- Location: Elstree WD6 3SY, Hertfordshire, United Kingdom