MIRABAUD

Mirabaud is an international banking group that provides a clientele of private and institutional investors, companies and finance professionals with highly customised investment, private banking and asset management services.

Headquartered in Geneva, Mirabaud has evolved steadily over the years and now employs over 700 staff who, through their experience and expertise, perpetuate the entrepreneurial spirit that has guided the bank since its foundation in 1819. The Group now conducts its **Wealth Management, Asset Management and Securities** businesses in the main financial centres around the globe and has offices in Switzerland, the UK, Luxembourg, France, Spain, Italy, Canada, the United Arab Emirates, Brazil and Uruguay.

Our WM - IT - GE team within our Wealth Management department in Geneva is looking to add:

ACCESS MANAGEMENT ENGINEER

As an Identity Management Engineer where you will be responsible for security, compliance and identity & access Management for on premise Active Directory and cloud services such as O365, Azure AD, as well identity management of our business applications.

You will be responsible for the analysis, design, implementation, and maintenance of all layers of IAM applications, including Authorization/Authentication and Account Creation/Management/Provisioning in data repositories. This position may focus on technical or administrative aspects of IAM, or could encompass a mixture of both.

Your responsibilities will also include all management, setup and administration of the IAM platform within the IS and to external partners or internal applications requiring IAM.

This role will encompass managing and refining a Role Based Security framework, where you will produce schema designs and operational plans to enforce this, alongside managing and implementing sign-on solutions utilising federated technologies such as SAML2 and/or OAuth2.

In this function, which reports to the IT department, you will work in close partnership with the Operational Security Teams, the Chief Information Security Officer to ensure that the directives and best practises are respected and correctly implemented.

This role includes the management of the definition key security risks, their control and reporting. The role will also be responsible for the training and support of the users in the area of information security awareness.

Main Responsibilities:

- Partners with Technology and Business Unit to serve as a security expert and trusted adviser in designing and providing systems that facilitate user provisioning/de-provisioning, authentication/authorization, and reporting based on business needs, industry best practices, and regulatory requirements.
- User Access Management: definition of the profiles, the roles and their evolution. Design and implement Identity and Access Management systems to ensure the appropriate security guidelines, policies and procedures are in place to adequately business and compliance requirements.

- Controls: definition of the key risks. Responsible for approval and auditing of user accounts and permissions with regular reporting to the management.
- Specify, design, and build Identity Access Management (IAM) solutions including password management, SSO, federation, and authentication.
- Data Loss Prevention Controls – reporting and evolution to adapt the solution according to the industry up to date best practices.
- Support the end users in relation with their access and rights to the Bank's applications, with regular recertification of the users' accesses and profiles.
- Develop and perform information security awareness trainings for the user population, informing them about the best security practices, providing them with an awareness of the risks and dangers of using technology in their daily activities, as well as helping them navigate the complex compliance framework fencing all the bank processes and interactions.

Candidate's Profile:

- At least four years of experience in a similar position – ideally in a bank, designing or maintaining permissions and roles for large enterprise applications such as an ERP or CRM.
- Strong knowledge of Microsoft Active Directory Architecture and Design, implementation, and Security.
- Demonstrable knowledge of current technologies in authentication, federation, and identity management space, such as OAuth 2.0, OpenID Connect, SAML, SCIM, U2F/UAF/FIDO2, etc…
- Familiarity with using biometrics for authentication and managing related privacy considerations
- Knowledge of identity best practices: RBAC, Zero Trust Identity Security, Least Privilege, Provisioning/Deprovisioning, Orphaned Account Detection and Removal, MFA.
- Strong experience in account-provisioning, self-service, and other identity management systems, as well as multi-factor authentication.
- Knowledge of identity management products including OKTA, CyberArk, Azure AIP, Azure PIM, and Role Based Access.
- Knowledge of PKI and Certificate Services, templates, and management.
- Knowledge of databases concepts and SQL language – an advantage.
- You are rigorous, autonomous, and dynamic with good interpersonal and communication skills.
- Capable to work in French and English environment.
- Particular attentive to the discretion and governance principles.

Mirabaud Group is an Equal Opportunity Employer.

If you are interested in this role, please send your application via email to the following address: recrutement@mirabaud.com

If you would like to **pursue a career within the Mirabaud Group**, please send us your CV to the same email address.

Notes:
Please be aware that Introductions from recruitment agencies will not be considered.
Only candidates with a suitable profile will receive a response.