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.

Mirabaud is proud to announce the launching of the largest project the bank has ever embarked on, pushing ahead its highly regarded entrepreneurial and passionate team to the next level of client servicing thanks to the adoption of enhanced digital front and back-office capabilities.

To support this ambitious digital transformation and migration to the cloud, our WM - IT - GE team within our Wealth Management department in Geneva is looking to add:

CYBER SECURITY ENGINEER

For this role, you will be part of the bank's Information Security team, working in close partnership with the Information Technology and the Business Transformation teams, to design, build and operate a highly secured, reliable and stable information system.

The Security Engineer tracks security best practices and then educate company leadership and fellow co-workers about the best way to implement the latest security protocols.

Responsibilities include security system configuration, monitoring and reporting. This position will have a lead role in performing vulnerability assessments, security testing, and working with operations and development teams on remediation and mitigation of findings.

Performs installation and configuration management of security systems and applications, including policy assessment and compliance tools, network security appliances and host-based security systems.

Develop security protections, such as encryption algorithms and data structure firewalls to protect company information. Performs technical activities for delivering effective host, network, data, and application security services.

Participates in infrastructure projects to develop, plan and implement specifications for network and distributed system security technologies in support of key information systems, supports cybersecurity architectural requirements.

Performs system security administration on designated technology platforms, including operating systems, applications and network security devices, in accordance with the defined policies, standards and procedures of the organization, as well as with industry best practices and vendor guidelines.

In addition to building and testing security infrastructure, the cybersecurity engineer will also be tasked with continually monitoring software and systems for intrusions or irregular behaviour.

Monitor's system logs, SIEM tools and network traffic for unusual or suspicious activity. In case of the identification of security-related issues, will conduct investigations and should be able to use digital forensic methods to track intruders and figure out the source of attacks.

MIRABAUD

Main Responsibilities:

- Support digital transformation and the migration to the cloud (SAAS) from an IT security perspective.
- Develop the threat intelligence capability and the security architecture for the bank.
- Manage data, applications and virtual infrastructures security in cloud environments.
- Engineering and configuration of network perimeters (next generation firewalls, WAF, CASB, IDS/ISO, logging aggregation & SIEM).
- Engineering and configuration of remote access technologies, including multi-factor authentication systems, remote access VPN, site-to-site VPN.
- Engineering and administration of Mobile Device Management (MDM) services.
- Analyse, troubleshoot, and investigate security-related, information systems' events.
- Manage the vulnerabilities management platform.
- Participate in the monitoring of the technological developments regarding Information Security.
- Provide CSIRT support as needed in response to information security related events.

Candidate's Profile:

- 5-7 years of experience in Information Security, previous experience in financial organisations is an asset.
- Certification such as a CISSP, SSCP, CEH or equivalent.
- Expertise in networking and platforms in a hybrid environment.
- Knowledge of zero trust concept and network micro segmentation.
- Understanding of privileged access management concept.
- Networking experience with the TCP/IP stack, as well as solid understanding of the OSI model and renowned ports and services (may not be a requirement, but is often preferred)
- Knowledge of current cybersecurity trends, as well as the continued research of emerging trends and hacking techniques
- Good understanding of log corrections, security incidences and events management.
- Good knowledge of the management and setup of security monitoring solutions together with tools/products enabling the collect, centralization and correlation of logs and events.
- You are rigorous, autonomous, and dynamic with good interpersonal and communication skills, as well as an aptitude for analytical problem solving.
- Good technical writing, documentation, and communication skills, both French and English required.

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.