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:

OPERATIONAL SECURITY ENGINEER

In this function, you will work in close partnership with the Production team, the User Access team, the Chief Information Security Officer to maintain a highly secured, reliable and stable information system.

The Security Engineer provides support to planning, designing and implementing security controls which safeguard and monitor events for information systems, enterprise applications and data.

Performs technical activities for delivering effective host, network, data, and application security services. This position will have primary responsibility for security platforms in the production environment, as well as development, quality-assurance and staging environments.

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.

This position will have a primary role on the Computer Security Incident Response Team (CSIRT) and with Disaster Recovery/Continuity of Operations Planning (DR/COOP).

This role includes the participation with the Production team to integrate in production environment newly software and equipment, the patching measures and documentation of the production exploitation procedures.
You participate to the training and support of your colleagues, in case of changes in the configuration of security components or the deployment of new functionalities.

Main Responsibilities:

- Experience Data Loss Prevention Controls solutions and mechanisms.
- Experience the management of data, applications and virtual infrastructures security in cloud environments.
- Security architecture design (identification of controls and network design for security).
- Engineering and configuration of network controls (firewalls, router ACLs, anti-SPAM, IDS/IPS, logging aggregation, SIEM, sandbox products like FireEye).

- Engineering and configuration of host and server based controls (anti-malware, application whitelist/blacklist agents, and risk monitoring agents).
- Engineering and configuration of remote access technologies, including two-factor authentication systems, remote access VPN, site-to-site VPN.
- Engineering and administration of Mobile Device Management (MDM) services (controls for mobile devices).
- Engineering and administration of Web and E-mail proxy and filtering systems.
- Analyse, troubleshoot, and investigate security-related, information systems' anomalies based on security platform reporting, network traffic, log files, host-based and automated security alerts.
- Evaluate systems using vulnerability scanners and manual techniques to verify system security settings and configurations.
- Assist the development of security tool requirements, trials, and evaluations, as well as security operations procedures and processes.
- Provide CSIRT support as needed in response to information security related events.
- Participate in DR/COOP exercises and continuous improvement processes.

Candidate's Profile:

- A minimum of 4-7 years IT experience; at least three of those years focused on IT security– ideally in a bank.
- Must possess or obtain within 12 months from date of hire, an industry recognized information security certification, such as a CISSP (or Associate), SSCP, CEH, or equivalent.
- Expertise in networks infrastructures (LAN, WAN) and operating systems (Windows & Linux) together with protocols and internet services.
- Good knowledge in the management and setup of security monitoring solutions together with tools/products enabling the collect, centralization and correlation of logs and events.
- Interest in the technology development and concept in the security domain, as well as fundamental or greater understanding of encryption technologies.
- Education in security and IT technology required, understanding of the system hardening processes, tools, guidelines and benchmarks a plus.
- 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 are required.
- Particular attentive to the discretion and governance principles.
- Passion for information security.
- Capable to work in French and English environment.
- High capacity to handle stress.

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.