Information Security Officer

Starting Date: September 2021

Full Time

The Role

As Information Security Officer you will be part of the team developing program-specific performance products according to security and business objectives. You will use your expert analytical skills and your in-depth knowledge of security best practices to prevent security breaches while also designing and enforcing policies and procedures that protect our organization's infrastructure from all kinds of threats. You will also be responsible for identifying vulnerabilities and liasing with our team to resolve them, ensuring that our network and data remains secure.

Minimum Qualifications

- Experienced information security professional with 4+ years of experience.
- Professional Information Security Certification. Solid knowledge of various information security frameworks.
- Deep technical understanding to configure portals.
- Bachelor's degree in engineering, math, physics or computer science or equivalent (e.g. successfully completed commercial apprenticeship).
- Knowledgeable in DNS, routing, authentication, VPN, proxy services and DDoS defense, programming techniques, ethical hacking, threat modeling and analysis, firewalls and intrusion detection and prevention protocols.
- PCI, HIPAA, NIST, GLBA and SOX compliance assessments.
- Ability to provide technical planning and execution.
- Web services (REST, RPC, gRPC).

Preferred

- Master's degree in engineering, math, physics or computer science or equivalent.

- Skilled in conflict management. Assertive but professional.
- Effective verbal and written communication skills.
- Goal and solution oriented.
- Good Knowledge of Application Lifecycle Development.
- Knowledgeable in automation with CI\CD (Jenkins, Gitlab && etc.).
- Practical experience with TDD; Practical experience with cloud services.
- Experienced with git/github/gitlab.
- Experienced with budget analysis.
- Familiar with IoT and blockchain industries.
- Rest API development; Estimation development and analysis.

Responsibilities

- Information security planning, including identification of information security assets and associated risks.
- Initiating, coordinating and escalating investigations when security incidents occur.
- Maintaining and updating a risk management plan and monitoring the implementation measures adopted.
- Developing, implementing and maintaining information security policies, assuring that these are compliant with all applicable legal and regulatory legislation.
- Collaborating and planning with the team and CTO of high-performance backend and infrastructure.
- Monitoring network usage to ensure compliance with security policies.
- Performing penetration tests to find flaws.
- Analyzing and documenting any security breaches and assessing their damage.
- Keeping up to date with developments in IT security standards and threats.

- Advising and coaching team on all information security issues and supporting them in the implementation of technical and organizational measurements.

What we offer

- The opportunity to contribute to innovative projects in a new and exciting industry that has the potential to positively shape our world.
- High growth potential.
- Warm and open corporate culture at an international company with many different nationalities.
- An environment that values freedom, autonomy, team spirit and open communication.
- Flexible working hours.
- Decentralized (remote) working possibilities.
- Office space in the heart of Berlin and Potsdam. More offices will be opened soon.

We look forward to working with you.