**Job Summary**

As the Product Security Architect (DevSecOps), you are a hybrid software/systems engineer who ensures that the Spreetail maintains the highest level of Security Readiness and meets current and emerging compliance standards. You will also be embedded within various developer teams to build security into the development/build/deploy pipeline, as well as embed security into the systems Spreetail deploys software.

This position needs experience designing and developing commercial enterprise software applications. You will work collaboratively with Product Management, Quality Assurance, System Architects, and Development team members in an agile environment to produce the highest quality software.

**Major Responsibilities/Activities**

* Review applications' architecture and documentation to validate their security posture.
* Review and/or proactively propose remediations for security vulnerabilities and work with product teams to ensure proper implementations.
* Work closely with Corporate Security and Cloud Operations to drive the software security certification process for the organization.
* Perform security risk analysis for our products and portfolio.
* Provide security guidelines for the organization to protect critical assets and data.
* Lead one or more security assurance programs, and be responsible for reviewing security assurance status of product releases.
* Be responsible for the evaluation of new technologies, tools, and/or development techniques that impact security
* Review, analyze, and evaluate both internally developed software and external vendor products and procedures to address security requirements.
* Maintain development security standards, policies, and procedures.
* Work with teams to perform on-going security code and testing review to improve their security posture.
* Help to define and develop consistent automated metrics covering all aspects of the security programs.

**Minimum Requirements**

* Prior development experience (3 years minimum).
* 5+ years proven work experience as an application security professional working with/within development team(s).
* In-depth understanding of background technical details of common application vulnerabilities, attack vectors and exploits, and techniques to remediate those vulnerabilities.
* Experience with performing product security reviews and analysis (Risk Analysis and Threat Modeling).
* Detailed technical knowledge of techniques, standards and state-of-the art capabilities for authentication and authorization, applied cryptography, data and communication protection, etc.
* Exposure to and knowledge of complete SDLC in Enterprise Cloud Software environments.
* Solid knowledge of Web-related technologies.