***Job Title: Senior Application Security Architect / Engineer***

## Location: Dublin

French speaking strongly preferred

**Company Overview:**

Murex is a leader in the provision of trading and risk management technology and was established in Paris in 1986. Murex software is used by the world's leading investment banks, asset managers, hedge funds, commodity houses and corporations to price, analyze and manage their exposures for foreign exchange, interest rate, equity, commodity, inflation and credit derivatives. MX.3, Murex integrated trading and risk management platform, comprehensively covers Front Office, Back Office and Risk Management.

Murex has had to continuously adapt its internal organization and product in order to maintain its leadership in the fast-paced, global and highly competitive financial software industry. The result is a dynamic, fast growing organization where team players with initiative can take responsibility quickly. Murex has one of the highest R&D investment rate in the industry

**Role:**

The Application Security Architect is responsible for assuring that IT application software and infrastructure are designed, implemented, and operated in accordance with applicable security standards and practices.  Primary responsibilities include application security, risk assessment, validation of security pen test results, problem resolution, system documentation, and system security management and support.

Key responsibilities for this role will be to engage in the initial requirements definition (including analysis of threats and risks and alignment with Architecture standards); conduct and facilitate security reviews including SSDLC testing requirements throughout the development lifecycle; facilitate "table-top"/red-team/scenario analysis exercises in conjunction with other Subject Matter Expert's; and plan the resolution of any identified vulnerabilities/issues. Monitor changes in the risk profile and exposure for the application, perform regular assessments based on changes in the threat landscape and on industry incidents, and review all proposed changes to ensure that effective controls remain in effect.  
  
This role will also work with the Global Information Security organization to identify potential requirements/enhancements to IS and IT standards, tools, and processes based on the results of the work with the SASA's applications.  
  
This role will also assist other application teams and IS functions including in the following areas: Provide ad-hoc security advice; Support technical risk assessments; Assist Security Incident Response Teams in the investigation of incidents; Assist the system development and infrastructure units in identifying IS risks and the appropriate controls for development, day-to-day operation, and emerging technologies.  
  
Additional skills critical to this role: In depth, hands-on understanding and application architectures and technology (including web applications, mobile technology, web 2.0 technology, identity and access management); Thorough understanding of industry and corporate technology standards for Information Security; detailed familiarity with security hacking tools and techniques; Strong understanding of business processes in support of trading within financial industries; Strong judgment and decision-making skills; Excellent skills in preparing and present strategies, recommendations, and value propositions to senior leadership teams.

**RESPONSIBILITIES:**

* Good understanding of the architecture and the various application tier and database tier components: underlying objects, schemas/products, database objects, file system structure, tables, views, packages, procedures, sequences, indexes, and constraints.
* Conduct information security threat analysis on new and changed application development initiatives towards design, review, and incident response planning.
* Provide in-depth assistance with the integration of information security within the application development life cycle.
* Review security requirements at relevant phases for both technical and operational perspective. Review remediation activities for completeness.
* Identifying security requirements and recommending appropriate solutions to IT and business problems.
* Review application source code for vulnerabilities, using both manual and automated code scanning techniques (static code analysis) aka Whitebox Testing.
* Perform vulnerability scanning and penetration testing at all application tiers using appropriate tools (dynamic code analysis) (network scanners, web scanners, database scanners, etc.) aka Blackbox Testing.
* Knowledge of operating systems (Windows, Unix, Solaris) and common products used to deliver web services, including IIS, Apache, Tomcat, Oracle Application Server, WebSphere, etc.
* Identify and convincingly explain the risks associated with common application vulnerabilities, demonstrate exploitation, and recommend mitigation options.
* Discern, document, and setup standard practices for application security audits.
* Partner with operations, legal, and administration teams to support the information security needs of their projects and ensure that risks are accurately identified and appropriately managed to the enterprise’s accepted level of risk.
* Participate in developing standards for information technology security practices.
* Identify and evaluate tools and techniques to be used for capture, modeling and analysis of information security architecture.
* Analyze, review, customize and recommend security architectures for internal projects and initiatives.
* Identifies, implements, and monitors best practices for information security architecture.
* Determine and clearly communicate – quantitatively where possible – the information security risks to the application development teams.
* **Assure compliance to security policies, standards, and procedures, including international regulations (SEC, MAS, FSA, etc.).**
* Monitor and recommend changes in standards that affect application security.
* Initiate and promote activities to foster information security awareness and education among application development.
* Work with Information security peers and managers to assure standards compliance on various platforms (e.g., OSs, databases, networks, etc.) upon which application development group relies for the operation of its applications.
* Identify threats and risks to the confidentiality, integrity and availability of all data residing on information systems platforms.

**QUALIFICATIONS:**

**A minimum of 5-7 years’ experience working with core database technologies (Oracle & Sybase), Unix/Linux & Solaris & secure code development (Java, Python, C/C++, XML, PHP, etc.)**

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily.  The requirements listed below are representative of the knowledge, skill, and/or ability required.

* In-depth understanding of common operating systems (UNIX/Solaris/Windows), networking protocols, databases, and applications development.
* CSSLP and CISSP from ISC2 as strongly desired qualifications (Certified Software Security Lifecycle Professional & Certified Information Systems Security Professional)
* Must have thorough knowledge in IS security components, principles, standards, procedures and practices.
* Must have a thorough knowledge with application security.  Must have a broad knowledge in information technology trends.
* Strong knowledge in application security and network and server security.
* Advanced knowledge of the application development, data storage and encryption technologies required for transferal of data in and out of the organization.
* Advanced knowledge and understanding of a range of computer and networking software related technologies.
* Ability to navigate within the applications with respect to the security environment, configure and maintain the application security roles.
* Ability to analyze and assess application security requirements and determine optimum, cost-effective solutions.
* Ability to communicate technical information to non-technical personnel.
* Strong interpersonal and communication skills and the ability to work effectively with a wide range of constituencies in a diverse community.
* Ability to analyze complex problems and recommend/negotiate solutions.
* Ability to communicate security objectives orally and in writing to a variety of audiences.
* Ability to work independently in a self-directed manner and collaboratively as a member of security team.
* Ability to create and implement detailed action plans for security solutions.
* Ability to understand legal and regulatory requirements and business drivers and priorities, and integrate these requirements into overall security design.
* Familiarity with project management lifecycle and providing security consulting to project teams.
* Ability to write security requirements and design documents.

## NOTE: GIAC Secure Software Programmer-Java from SANS.org (GSSP-JAVA )