Leading provider of information security & compliance solutions providing Governance Risks and Compliance Services, Enterprise Security Solutions, Managed Security Services, Training & Awareness Programs, is seeking highly motivated professionals to join our team to cover the following openings:

Security Architect (BE-ESA-1002)

As a member of the Security Governance department of a large mobile telecommunications company, the Security Solutions Architect assists the enterprise security architecture team in the specification of security requirements for business solutions and support processes, the development of reference architecture models, the authoring of security standards and the delivery of architecture roadmaps as part of security strategy definition.

Main Responsibilities

The candidate identifies, classifies and specifies architectural building blocks (ABB) for the purpose of guiding implementation and change activities in alignment with the strategic security goals.

Qualifications and Experience

- Minimum 5 years of experience in information and cyber security architecture.
- CISSP, CISM, GIAC, SABSA or similar Information Security certifications are a plus.
- The candidate has used multiple Enterprise Architecture methods:
  - Architecture Development Methods (method processes & content frameworks), such as:
    - TOGAF9 Architecture Development Method
    - SABSA
    - MASS Method (see associated IBM redbooks)
    - RUP / OpenUP
    - Kruchten 4+1
    - Model Driven Architecture
    - Test Driven Architecture
    - Attribute-Driven Design Method (Carnegie Mellon SEI)
    - Architecture Tradeoff Analysis Method (idem)
  - Architecture Description Languages:
    - Archimate 2
    - BPMN 2
    - UML 2
- Architectural requirements definition and management:
    - Process modelling incl. state & event modelling, use case modelling, domain modelling, service modelling
- Security tactics & design patterns: Tactics & patterns for confidentiality, integrity, availability, accountability, non-repudiation
- Architecture domain practices:
    - Component modeling (incl.integration, e.g., EAI, SOMA)
    - Data modeling
    - Operational modeling (deployment views)
    - Infrastructure sizing
- Security domains and standards:
    - Cryptography (incl. Key Life Cycle Management)
    - Public Key Infrastructure
    - Identity & Access Management
    - Vulnerability and Patch Management
    - Security in the Software Development Life Cycle
    - Resiliency, Disaster Recovery Planning, Business Continuity Planning
    - Application Security

    - Database Security
    - Web Services Security (OASIS standards)
- Networking technology:
    - Routing & switching standards
    - VPN (IPSec, MPLS) standards
    - Etc.
- IT and security infrastructure standards:
    - J2EE & Application Servers: WebSphere, WebLogic, JBOSS
    - XML (incl. XSLT, SPML, SOAP, XACML, SAML...)
    - ESB implementations
    - Directory technologies (LDAP) - Active Directory, Tivoli Directory Services
    - AAA: Kerberos, Tivoli Access Manager, WebSEAL, Juniper, Checkpoint...
    - Databases: Oracle, SQL, JDBC
    - Operating Systems: Windows, Solaris, Linux
    - OASIS WS-*
- Telco industry knowledge and experience:
    - The candidate must have multiple project experiences defining reference architectures or solutions within the telecommunications or cloud industry.

- Managed architectural work across the full life cycle from inception through to implementation.
- Applied and integrated a broad variety of security technologies, producing layered, defense-in-depth security architectures.
- Conciliated multiple stakeholder viewpoints, using architecture patterns and tradeoff scenarios.
- Applied Infosec industry standards / best practice frameworks (e.g., SANS 20) in large organizations.
- Maintained a holistic perspective on the security capabilities needed to support or deliver the enterprise's strategic goals and objectives. These capabilities cover a broad variety of security domains: IAM, EPP, application security, etc.
- Acquired skills in general project management, system development life cycle and architecture documentation.
- Applied regulatory and legal requirements related to information Security and Data protection.
- Proven team player with excellent communication, presentation and negotiations skills, and the ability to interface will all levels of the enterprise.
- Excellent analytical, conceptual, and problem-solving abilities.
- Ability to conduct research into emerging technologies and trends, standards, and products as required. Learns fast.
- Ability to effectively prioritize and execute tasks in a high-pressure environment.
- Proven leadership skills combined with a strong drive and orientation for results, ability to motivate self and others, and lead others towards a common goal.
- High integrity, work ethics and commitment.
- Strong decision making skills.
- Excellent influencing and facilitation skills, in particular in problem solving / troubleshooting activities.

Interested applicants should send their CV by quoting the reference code (BE-ESA-1002) to:

BESECURE
HR Department
133B Franklin Roosevelt
Fax: +357 222 62401
Email : hr@besecuregroup.com

All applicants will be acknowledged and treated in the strictest confidence.