Job Description
ED Security Analyst/ Developer
Location: Bengaluru

Scope: Enterprise Data-Security
Trust is at the foundation of effective data analysis and consumption within Advanced Analytics and Data Sciences and is a key pillar in the Enterprise Data Program. In order for our business partners to effectively share, analyse and consume data to add value across the enterprise, they must trust that the appropriate people have access to the data and its integrity is maintained. The security of this data is fundamental to maintaining trust in the Enterprise Data Program, covering the three tenets of Confidentiality, Integrity, and Availability. The ED Security team is front-and-centre in delivering the features, processes, education, knowledge and consultation across all EDP teams and Lilly functional areas who are involved in building, ingesting, maintaining, analysing and consuming the capabilities of the Enterprise Data Program.

Skills:

- 7 -10+ years of experience.
- Demonstrated expertise and experience working in security-focused roles
- In-depth experience with Data security, especially AWS and Azure platforms
- Significant experience in cloud security architecture, methods and tools.
- Experience coding in Python, CloudFormation, and at least one scripting language
- Strong analytical and troubleshooting skills with the capability to handle and own critical issues through to resolution.
- Experience in Design and Implementation guidance to DevSecops process
- Experience leading large-scale projects from start to finish and mentoring other security practitioners
- Adept experience providing SME knowledge and guidance to stakeholders and engineering functions
- Focus on continuously improving Lilly Data security capabilities by assisting to lead the delivery of initiatives in support of the Global Lilly Security Strategy
- Comfortable operating in and reviewing modern cloud technologies from providers such as AWS, Azure
- Experience in understanding API development, integration and security
- Experience with security program management, cyber threat management, identity and access management and data protection(encryption) and privacy.
- Skills in security assessment, design, architecture, management, and reporting

Main Responsibilities

- Part of a scrum team leading and participating in projects to deliver data security and monitoring features for the Enterprise Data Program, and Enterprise Data Security.
- Leading the resolution of technical data security issues, working across Lilly IDS teams and in particular with ED Security and Information Security

- Working with core and functional teams (including business partners) to understand and gather requirements, in order to inform data security models, architecture designs and processes for security features.
- Collaborating with Lilly IDS teams to ensure EDP security models and designs are within Lilly's standard practices, technologies and architectures, incorporating privacy best practice, Protect Lilly principles and policies, and security-by-design principles.
- Collaborating with third party organisations and resources to help implement and delivery security projects
- Documenting security designs, architectures and processes according to Lilly validation and quality practices
- Working with Enterprise Information Security and the AADS team on conducting security assessments and any other needed activities as a result of audits, security findings and security improvement roadmaps.

Skills needed

- Understanding of Information Security practices, methods and tools
- Experience of working with cloud-based technologies, in particular AWS and AWS security processes, technologies and methods
- Relevant AWS Certifications (particularly security-related)
- Security Automation experience
- Experience and understanding of system development, API integration, data storage and movement
- Experience of technologies such as TLS, PKI, OpenID Connect, OAuth 2.0, JWT, SAML, XACML
- Experience of systems analysis to gather requirements and create/propose designs
- Knowledge of data security standard methodologies for structured and unstructured data repositories
- Experience of data protection technologies such as data-loss prevention, encryption, data masking/scrambling, access and rights management
- Desirable: Knowledge / experience of security monitoring tools and techniques
- Desirable: experience in working with data-focused applications and technologies such as databases, data lakes, warehouse