Flexiti Financial

Flexiti has reimagined point-of-sale (POS) consumer financing to drive sales for retailers in-store and online, becoming one of Canada's leading private label credit card issuers. Through our award-winning platform, we deliver a POS financing experience across any device that is customer-centric, simple and intuitive. Without the need to integrate into existing POS systems, retail partners can easily offer the same fast and paperless financing solution across all retail locations and sales channels to increase revenue and build loyalty through repeat purchases. For more information, visit www.flexiti.com.

Security Engineer

Flexiti Financial is looking for a Security Engineer to join its technology team. We are looking for this person to develop and maintain design plans for the overall logical and technical IT security architecture. The incumbent must provide technical leadership and consulting expertise across the organization, from the point of strategic decision making down to project planning and execution. . Supporting the VP, Cyber Security and DevOps engineering, the Security Engineer will be responsible for presenting findings and recommendations at all levels within the company to gain commitment for high-level security plans, as well as initiating and participating in projects to evaluate various technologies and methods for successfully implementing those plans. The incumbent will help bring Flexiti's vision to life; someone who is passionate about assessing and designing enterprise security systems for on premise and cloud platforms.

Responsibilities

- Conduct a broad range of analyses, define architectures and solutions, and provide technical recommendations with respect to specific IT service delivery functions defined within the Flexiti Security Service Strategy and Service Design categories:
    - Architecture Management
        - Define a blueprint for the future development of the technological landscape, taking into account the service strategy and newly available technologies. The incumbent will be a domain expert with business acumen that aligns to Flexiti's business strategies on digital transformation and cloud adoption.
    - Demand Management
        - Understand and anticipate internal client demand for services. Demand Management is coupled with Capacity Management to ensure that the level of IT provisioning is sufficient to meet the required demand.
    - Availability Management
        - Define, analyze, plan, measure and improve all factors related to the availability of IT services thereby ensuring that the IT applications, infrastructure, processes and tools are appropriate for maintaining agreed availability targets.
    - Architectural Governance

        - Develop Flexiti's security Architectural Governance in alignment with Corporate Governance by developing guidance on effective and equitable usage of resources to ensure sustainability of Flexiti's strategic objectives.
- Strategy & Planning
    - Maintain an in-depth knowledge of the company's strategic business plans.
    - Provide architectural consulting expertise, direction, and assistance to Business Systems Analysts, Business Solutions Architects, Infrastructure team, and Application Developers.
    - Evaluate and document the company's existing security architecture and technology portfolio.
    - Identify potential sources of application security risk, prioritizing them based on risk impact.
    - Develop and document multiple options for revised IT architectures and changes to the technology portfolio, with recommendations for security optimization and cost/benefit analyses for each option.
    - Provide guidance on Threat Assessment and Response initiatives in alignment with the strategic and operational objectives of the technology organization and the business.
    - Understand and articulate to key stakeholders how information aspects of the Security Architecture help achieve business strategy.
    - Develop, document, communicate and enforce a technology standards policy.
    - Conduct research on emerging technologies in support of infrastructure development efforts, and recommend technologies that will increase cost effectiveness and infrastructure flexibility.
    - Design, develop and oversee implementation of end-to-end integrated security systems.
    - Identify where change is required (development of a Gap mitigation plan) in order to keep the Security Architecture vital, sustainable and ready to support business capabilities.
    - Ensure alignment between different domains of IT architecture.
    - Define the Security Architecture framework in order to have non-redundant, integrated, cost-effective solutions with a common foundation for all systems.
    - Help define and articulate a strategic roadmap to enable Flexiti's current and future security needs, based on the IT strategic roadmap and Business strategy.
    - Support other domain architects - Address technical architectural issues throughout the construction of a solution to ensure that it remains true to the defined technical solution architecture.
- Operational Management
    - Collaborate with end users and senior management to define business requirements in support of complex systems development efforts and to gain buy-in for all technology plans.
    - Engage with the organization and IT team to identify and prioritize continuous improvement in Cyber response capabilities.
    - Provide guidance for the delivery of the Cyber Incident Response Program.
    - Work with external (Third parties) and internal clients (Internal Audit) to remediate identified gaps.

- Review new and existing IT projects, systems designs and procurement/outsourcing plans for compliance with IT standards and architectural plans.
- Provide guidance to junior members of the team.

Qualifications

- 10+ relevant experience, with 5+ years work experience as an Security Engineer/Architect.
- Good understanding of application security concepts such as SAST & DAST.
- Good understanding of the architectural principles of cloud-based platforms including IaaS, PaaS and SaaS. In AWS and Azure.
- Good understanding of cloud security and knowledge of enterprise security practices.
- Hands-on experience with business requirements gathering and analysis.
- Proven experience in systems design and development.
- Strong understanding of information processing principles and practices.
- Knowledge of security standards (ISO 27001, NIST 800-53, etc.) frameworks (NIST Cybersecurity, etc.) and regulations (particularly in financials) is preferred.
- Solid knowledge of network technologies, hardware platforms and operating systems.
- Solid understanding of security requirements through the entire technology stack.
- Solid Knowledge of current software, protocols and standards.
- Excellent knowledge of hardware and software evaluation principles and practice.
- Knowledge of multiple programming languages and development methodologies.
- Proven project planning and management experience.
- Strong knowledge of Cyber Simulations, Threat Modelling, and Penetration testing.
- Good knowledge of applicable data privacy practices and laws.
- Exceptional analytical, conceptual, and problem-solving abilities.

What We Offer

Below are just a few reasons why people love working here:

- An opportunity to be a part of an award winning and fast growing company
- An innovative culture that promotes autonomy and flexibility
- A dynamic team and working environment that provides ongoing support
- Competitive compensation package commensurate to experience