Permanent Placement & Consulting Services in Information Technology

IT Security Architects/Engineers

Available Jobs

Cybersecurity Architect (Cloud) – Arlington, TX

Job Ref: 20181007

The Cybersecurity Architect is responsible for the development and delivery of a comprehensive Cybersecurity program to assure that information created, acquired or maintained and is used in accordance with its intended purpose and to protect information, applications and infrastructure from external and internal threats. Additionally, the program will comply with all statutory and regulatory requirements for information protection and Cybersecurity. The Cybersecurity Architect is responsible for developing and designing comprehensive security processes and controls into the IT infrastructure. The Cybersecurity Architect is responsible for designing and maintaining a secure development life cycle to assure that information created, acquired or maintained by GMF is used in accordance with its intended purpose. Additionally, the secure development life cycle will comply with all statutory and regulatory requirements for information access, Cybersecurity. Other key responsibilities include engaging in the initial requirements definition by analyzing threats and risks, facilitating security reviews to identity vulnerabilities, and testing security requirements. Analysis of threats and risks should consider malware analysis and protocol analysis. This position will work with application teams and IT groups by providing information on Cybersecurity practices, risk assessments and supporting incident response in the investigation of incidents. This position will work with internal and external groups to ensure the proper Cybersecurity policies and standards are effectively operating. This employee has contact with other departments and will assist in articulating and implementing the Cybersecurity strategy.

Responsibilities:

- Work with IT departments, IT Architects, data custodians and governance groups to develop and update Cybersecurity policies, standards and procedures for secure application architecture.
- Assist security management in creating, reviewing and updating the Cybersecurity strategy on a periodic basis.
- Recommend and implement changes in security policies and practices in accordance with changes in regulation or financial sector industry Cybersecurity practices.
- Initiate, facilitate and promote activities to create information security awareness within the organization.
- Coordinate the development and delivery of an education and training program on Cybersecurity and privacy for employees, contractors and other authorized users.
- Manage the efforts to conduct Cybersecurity control assessments for systems which store customer information whether hosted internally or cloud based.
- Assess and communicate security risks associated with development practices in place at the company.
- Provide input to engineers for additional configuration of application firewalls via IT project management and change management.

- Provide function/business requirements for security solutions/initiatives and identified areas to improve security posture.
- Advise and drive the security maturity of the development lifecycle.
- Determine security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates.
- Plan security systems by evaluating network and security technologies; developing requirements for local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), routers, firewalls, and related security and network devices; designs public key infrastructures (PKIs), including use of certification authorities (CAs) and digital signatures as well as hardware and software; adhering to industry standards.
- Monitor adherence to standards in architecture, application design, development, and testing frameworks.
- Actively partner with infrastructure, application and other stakeholders to ensure deployed solutions minimize security and privacy risks.

Qualifications:

- Must have knowledge and stay up-to-date on the latest Cybersecurity legislation, regulations, advisories, alerts and vulnerabilities.
- In depth, hands-on understanding in application architecture and technology including web applications, mobile technology, identity and access management.
- Familiarity with Cybersecurity hacking tools and techniques preferred.
- Strong knowledge of software development/deployment methodologies in web/mobile based environments.
- Knowledge of software security for web and mobile applications.
- Possesses knowledge in various information security areas, such as: Identity and Access Management, Threat and Vulnerability Management, Information Risk and Governance, IT architecture, Monitoring, Incident Response and Security Strategy.

Submit your resume for this job by contacting us today!

Contact Us

817-329-6830 Tel • 817-329-6833 Fax • PO Box 93538 • Southlake, TX • 76092
rr@prdfw.com • www.prdfw.com