Job description

This position is for a Cyber Security developer in the Medical Software team under HealUp. The person will develop & deliver for the HealUp level Cyber Security.
Build your career in next generation Healthcare Cyber Security software. Experience what it takes to own complete Secure Software Development Life Cycle phases and what it means to deliver a world-class software working in collaboration with IT team.
Essential responsibility:

- Develop and implement security related solution with the intent to streamline monitoring, alerting, and incident management efforts for platform.
- Lead the design, development, and deployment of solutions for securing in areas such as Edge computing, Application, Data or Security.
- Work with technical teams to understand requirements and automate processes to better enhance development of applications.
- Serve as security guide in platform and application development, database and micro-service design. Providing mentorship to project teams on the appropriate selection and implementation of security controls to follow enterprise compliance and security policies.
- Define and document standard methodologies from a security perspective.
- Participate/Drive in architecture security review. Reviewing technology designs and develop data security controls and solutions.
- Suggesting changes to the environment that would assist with eliminating vulnerabilities and mitigating the risk of exploitation resulting in potential incidents.
- Suggesting and implementing process improvements based upon lessons learned.
- Crafting and building custom policies required to facilitate alerting and workflow requirements.
- Performing other Enterprise Security & Support tasks as required and assigned.

Qualifications Required:

- Candidates for this position should have at least 2 to 3 years of Cyber Security experience and development, in addition to the following
- Bachelor's Degree in Computer Science, Electronics Engineering or related computer field
- Strong Understanding Of Secure Communication Methods
- Strong understanding of Cryptographic algorithms, certificates, PKI, Key Management
- Knowledge of WAF, Proxy-Server, Reverse-Proxy, Load-Balancing
- Knowledge of various vulnerabilities and penetration testing
- Strong analytical skills
- Able to track and lead a large number of simultaneous activities, as well as cross-team dependent activities
- Able to work collaboratively with minimal supervision
- Effectively escalates items as required, and can influence decisions and actions without direct authority
- Able to learn new technologies and processes quickly

- Able to quickly adapt to changes in timelines and sequences
- CISSP, CSSLP, CCFP, CISM certification preferred
- Knowledge of working in Agile