|  |
| --- |
| Job Description |
| Role and Responsibilities  GE Digital CyberSecurity is looking for an experienced embedded security engineer. The successful candidate will play an active role towards creating a secure reference platform for IIOT systems, applications and devices. He/She will be well adept in the intricacies and details of embedded, real-time system, mission critical hardware and software systems. Additionally, they will champion the secure product development methodologies including secure SDLC concepts. Security is a top concern/pillar in IIOT and a good candidate not only understands it but also uses their security know-how in furthering it. Essentially you will be a thought leader in building secure Industrial IoT devices and apps. Experience in Industrial Networks, Software and Devices will be an added advantage.   * 5+ years experience in embedded/real-time systems using linux/RTOS. * Good understanding of computer architecture, especially the hardware components, Software stack and protocols. * 5+ years experience in security technologies like TXT, TPM, TrustZone etc. This could overlap with experience in embedded systems. * Good understanding of applied cryptography fundamentals (Encryption, Authentication, Symmetric Cryptography, Asymmetric Cryptography etc) * Knowledge of Network stacks and technologies. * Hands-on experience with Linux/Unix and kernel development. * Hands-on experience writing code in several of shell/scripting-languages/c/c++/java/python etc * Good understanding of concurrent programming. * Experience using debuggers/gdb, static-analysis, dynamic-analysis, root-cause-analysis. * Be responsible for providing technical leadership and defining, developing, and evolving security within software in a fast paced and agile development environment using the latest secure software development technologies and infrastructure. * Work with Cyber Security Leaders and SMEs to understand product requirements & vision * Translate security requirements / vision into prioritized list of user stories and deliver to required timelines and quality standards * Perform Threat Modeling and Architecture Risk Analysis on software products. * Perform Security Code Reviews, Vulnerability Analysis and research on application code. * Coach and mentor developers to write and implement cryptography (PKI, Code Signing, Stored Secrets etc) * Work cross functionally to scope schedule and then analyze results from Red Team exercises on software products. * Guide developers to write secure code and implement secure engineering practices. * Provide response for security related incidents reported for software products. * Engage subject matter experts in successful transfer of complex domain knowledge * Apply principles of Secure SDLC and methodologies like Lean/Agile/XP, CI, Software and Product Security, Scalability, Documentation Practices, refactoring and Testing Techniques * Provide guidance and advise on writing secure code that meets standards and delivers desired functionality using the technology selected for the project. * Understand application security methodologies and frameworks. * Leverage tailored Secure SDL practice into specific engineering * Develop security requirements and utilize best practices to meet them * Research new application security technologies and implement them to improve application security. * Working with other scrum teams for security-focused design * Identifying and ensuring resolution of possible technical implications of each release * Maintaining a backlog of security-related tools that will improve the maintainability and security of our code and the pace of development * Promotes best practices based on OWASP, MSDL etc.   Qualifications and Education Requirements   * Bachelor's Degree in Computer Engineering or in a STEM major (Science, Technology, Engineering, or Math) and/or a minimum of 5 years of equivalent experience Minimum of 4 years of professional experience in developing Embedded systems and applications   At least 3 years of experience involvement with development team(s) that delivered hardware based services Preferred Skills   * A High energy and a result-oriented approach * Experience with Security Development Lifecycle processes such as Threat Modeling desired * Contribute to and lead discussions and communications within the team and outside, including customers and other business units * Strong knowledge of Object Oriented Analysis and Design, Software Design Patterns and Java/c++ coding principles * Hands-on Experience with developing web applications (Java, Spring Core, Spring MVC, Spring Security). * Hands-on experience with developing RESTful Java WebServices/MicroServices (Spring Boot) using Oracle MySQL and PostgreSQL. * Hands-on hardware security assessment experience * Experience in Pen Testing Harware/Firmware/LowLevel Software and devices. |