Software Security Engineer
White City, London

The Role

The London based Software Engineering team are expanding and we are looking for an experienced Software Security Engineer to join us.

The purpose of the Software Security Engineer is to develop and implement software security framework and practices that informs and validates DNAe's R&D and product development strategies to ensure the highest level of security, especially related to compliance and regulations.

Duties and responsibilities As owner of DNAe's software security to:

- Work closely with the engineering team on Design Reviews for new features or major changes to the product in development
- Audit code for security flaws and ensure software security best practices are followed
- Perform Penetration Tests on new features and on the platform as a whole
- Develop, implement, and communicate vulnerability mitigation strategies to development teams
- Work effectively and efficiently either solo or collaboratively to deliver projects at the expected level of quality and within the agreed deadline
- Think like an attacker and solve complex security problems by proactively identifying vulnerabilities and design robust countermeasures to prevent, detect and mitigate potential threats.
- Perform security risk assessments (ISO 14971 and UL-2900-2-2) and threat modelling (using NIST/OWASP/Microsoft threat modelling tool) at the requirement and architecture level.
- Identify Common Vulnerabilities and Exposures (CVE) list from the packages being used as part of the product development and perform Common Vulnerability Scoring System (CVSS) to produce a numerical scope reflecting the severity of a CVE.
- To act as the subject matter expert (SME), for example in threat modeling and risk assessment, network and application security, emerging security technologies and trends.
- Implementing, testing, and operating advanced software security techniques in compliance with technical reference architecture.

Experience & Qualifications

- MSc or PhD in Information Systems, Computer Science, Mathematics, Physics, Statistics, Analytics or Actuarial Science, or an equivalently technical discipline. Alternatively, extensive software product development experience.
- At least four years of software security work experience including hands-on experience with application security, network security and system security.
- Strong knowledge of security protocols, cryptography, authentication, authorisation, security vulnerabilities and remediation techniques.
- An understanding of software engineering practices.
- Excellent analytical, problem solving and communication skills.

- Detailed technical knowledge of techniques, standards, and state-of-art capabilities for authentication and authorization, applied cryptography, security vulnerabilities, and remediation.
- Adequate knowledge of web-related technology (Web applications, Web services, and Service-oriented Architectures) and network/web-related protocols.
- Nice to have at least one of the vendor certifications: CISSP, CEH, OSCP, and CSSLP.

Desirable Experience:

- Ability to identify common (OWASP Top 10/CWE Top 25) web application vulnerabilities through secure code review (C, C++, Python)
- Application Penetration Test using industry standard tools (ex: Burp Suite)
- Knowledge of modern web application components, architecture, and design principles
- Ability to explain vulnerability risks and remediation options to developers
- Programming ability in at least one scripting language (ex: Python, Bash)

Workplace

This role is based at Scale Space, White City.
A hybrid working arrangement is available for this role, at least two days in the office in West London are required per week. (This may be after initial induction period).

Apply

To apply please email careers@dnae.com with your CV and salary expectations. Please include any other information you would like us to consider.
We are currently not sponsoring visa applications for this particular role therefore right to work in UK would also need to be confirmed in your application.