

Job Description

Job Title: Application Security Developer

Reporting To:	Engineering Manager (Development)
Responsibility for Others:	None
Location:	Broadlands, Holmwood Campus, Horsham.
Hours of Work	Monday to Friday 9.00am to 5.30pm with 1 hour for lunch
Any Special Requirements	Occasional travel may be required in the UK

Overall Purpose of the Role:

This position is responsible for helping to validate and continually improve the overall security posture of the Creative Technologies suite of applications, alongside associated development processes and in some cases, infrastructure environments.

Key Activities & Responsibilities:

(This is not an exhaustive list of the duties to be performed. Job descriptions do not limit the tasks that an employee may reasonably be requested to perform. Changes in job descriptions may be necessary as the needs of the Organisation change over time.)

- Work within our scaled agile environment to collaborate with Architects, developers, QA engineers and product teams to help determine functional and non-functional requirements relating to security, for existing and new software and applications.
- Have a good understanding and experience of all aspects of a software development lifecycle, from appropriate technologies and workflows to coding standards.
- Work with SAFe teams to provide guidance around application security best-practices, principles and standards.
- Conduct code reviews, with a perspective on security
- Help in embedding security into development and operational lifecycles, with a focus on automation and shifting left.
- Help develop a security awareness culture in product design and development practices; assist in security training for developers and testers.
- Contribute to the development and implementation of cloud-based applications, utilising application security best-practices within that cloud infrastructure.
- Working closely with the Architecture and Information Security team to align standards, frameworks and security with overall business and technology strategy.
- Create solutions that balance business requirements with information and cyber security requirements.
- Contribute to the company-wide Secure Development Standards and related policies and apply these to the software development lifecycle.
- Help execute SAST and DAST using new and established tools and review findings.
- Assist with vulnerability discovery and testing, risk analysis and penetration tests, helping to produce remediation plans as an output.

Qualifications & Skills

- Proven experience in application development, with strong knowledge of .Net and .Net Core, ASP.NET, ASP.NET Core, Azure Technologies.
- Experience in coding in various languages - C#, TypeScript, JavaScript, as well as scripting languages such as PowerShell and Python).
- Knowledge of Single Page Application concepts and frameworks.
- A strong understanding of Application Security and related OWASP Frameworks, including but not limited to the current OWASP Top 10
- Strong experience with common Web Application Security testing tools and HTTP inspection tools, such as OWASP Zap, Burp Suite, Fiddler and Charles Proxy.
- Experience of Static Application Security Testing (SAST) tools would be desirable.
- An understanding of and experience with .NET cryptographic suites
- Familiarity and hands-on experience with Authentication and Authorization protocols (OpenId Connect and OAuth2.0).
- Understanding of software quality assurance principles
- A technical mindset with great attention to detail
- High quality organizational and leadership skills
- Excellent interpersonal, time management and communication skills- both written and oral.
- Customer focussed and can present ideas and concepts in user-friendly language.
- Flexible and willing to work outside core business hours as required.

Personal Characteristics

- Highly motivated, flexible and adaptable with a 'can do attitude'
- Passionate about Application Security and keeping up to date with trends
- Good analytical and problem-solving abilities
- Actively seeking to expand IT and security knowledge and to upgrade skill set
- Strong ability to work independently and as part of a team
- Strong interpersonal skills with a collaborative approach
- Effective organisational skills with attention to detail
- Positive outlook on work
- Delivery / solution focused

Note: This description is not intended to cover all the duties of the role. Reasonable additional duties may be assigned, or duties may be reassigned at any time and at the discretion of management.