Waratek

Principal Security Architect, Strategist and Product Owner

About the Company

Waratek is an award-winning pioneer of next generation application security solutions. Headquartered near St Stephen's Green in central Dublin, Waratek develops runtime protection technology for Fortune 500 companies to effortlessly:

- Patch known software flaws with Runtime Virtual Patches which are compiled in-memory with zero app downtime
- Protect applications from known and unknown attacks vectors such as the OWASP Top Ten and SANS Top 25 (SQL Injection, Remote Code Execution, Cross-site Scripting, Path Traversal, etc)
- Virtually upgrade out-of-support Java applications and platforms to the most current version without rewriting the app (TLS upgrades and more)

In 2015, Waratek won RSA's *Innovation Sandbox Award* and many more to date.

Role Overview

You will be responsible for driving the innovation behind most of the above security solutions by finding world-first, novel and efficient ways to solve intractable security challenges. Innovating, taking feedback from clients and partners, working with management to build out roadmaps and collaborating with our incredible Engineering team to realise new features and new products. Other aspects involve supporting the commercial side of the business with authoritative analysis and commentary of the latest exploits / vulnerabilities and becoming *the* Waratek Security Evangelist. This role is very much at the heart of the company's technological innovation.

Responsibilities

- Technical lead for product strategy and vision for security features which encompass Java and .NET. This involves collaborating with key stakeholders including Senior Management (CEO / CTO), Development & QA Managers, Marketing, Sales, PreSales and Client Services on product direction and priorities.
- Responsible for research, analysis, design, implementation, review and documentation of both production and proof of value security features.
- Create and maintain security feature roadmaps, lead workshops, promote communication and support planning / release efforts.
- Support colleagues with design and code reviews, realising security features in other languages, testing of security features and similar.
- Provide analysis of the quarterly Oracle Critical Patch Updates and zero-day exploits to provide insights for new virtual patches / security features as well as to Marketing to help form media alerts and advice for customers.
- Perform analysis of client pen test and vulnerability reports.
- Support Senior Management and Marketing with go-to-market strategies for new Waratek security related products and features.
- Assist Marketing in creating a blog, media content and technical customer alerts.
- Team with Sales, PreSales and Client Services to engage with clients on technical matters and to create and leverage continuous feedback loops on security features.
- Support Senior Management in establishing new partnerships and maintaining existing ones.
- Keep abreast of and provide commentary on:
    - Evolving cyber security-related issues and assessing how are Waratek products affected.

    - Competitive products and gaps in Waratek's capabilities compared to the competition.
- Be a Waratek security evangelist who can translate Waratek's security capabilities into language that is meaningful to varying audiences, including business and technical leaders.
- Deliver internal tech talks, educating staff and management.
- Support security recruitment endeavours including participating in interviews, create and maintain interview challenges and questions for the recruitment.

Core Qualifications

- Minimum of 3 years experience technically leading a Java / .NET related security function.
- Minimum of 5 years software engineering experience working with a team of developers and quality assurance.
- Extensive breadth and depth of Java and / or .NET security knowledge.
- A curious mind that needs to understand the inner workings of security including not just the how but the why.
- Exceptional communication skills, both written and verbal.
- Ability to build solid working relationships with your colleagues both inside Engineering, on the commercial side of the business and with clients and partners.

Preferred Experience / Requirements

- Experience of penetration testing including Metasploit, OWASP WebGoat, Security Shepherd and similar.
- Ability to solve problems creatively and efficiently.
- Ability to pitch, present and sell your ideas / solutions to various stakeholders.
- Can turn a healthy level of pressure into positive motivation.
- Flexibility regarding the working day as some clients and partners operate in different timezones and for attending security conferences such as OWASP, Black Hat, SANS and similar.