Application Security Specialist

JOIN PAYCHEX EUROPE

At Paychex Europe, you can truly make a mark in our international, collaborative, and innovative workplace. We foster a supportive and social team culture, where we solve our challenges together, and diversity is embraced so everyone can be authentic at work.
Our values aren't just words — they're how we work, every day:

- Integrity – we're honest, clear, and do what we say.
- Respect – we listen, value different perspectives, and treat people right.
- Partnership – teamwork wins; we share success and support each other.
- Curiosity – we challenge the status quo and try new ideas.
- Accountability – we own our work and focus on solutions, not blame.
- Service – we care about our customers and each other, and we show it.

About the Role

We are seeking a technically focused Application Security Specialist to join our security team of 5 - with a primary focus on Secure development lifecycle and Vulnerability Management.
In this role, you will work closely with our different software development teams, to identify, analyze, calibrate, prioritize, and drive remediation of security vulnerabilities primarily across our commercial products. You will play a key role in strengthening secure software development practices using security testing tools such as Checkmarx, industry frameworks including OWASP, and risk-based vulnerability management methodologies.

Key Responsibilities

- Perform technical review, triage, and calibration of vulnerability findings from SAST, SCA and container scans.
- Analyze Checkmarx findings to distinguish true positives from false positives and ensure accurate vulnerability classification.
- Assess vulnerabilities using CVSS, exploitability, business impact, and environmental context to determine appropriate risk ratings and remediation priorities.
- Partner with development teams to identify root causes of security vulnerabilities and provide remediation guidance aligned with secure coding best practices.
- Promote secure development practices based on e.g. OWASP Top 10, OWASP ASVS, CWE, and secure coding standards.
- Contribute to the development of AI-assisted workflows for vulnerability detection, analysis, prioritization, and remediation recommendations.
- Develop and maintain vulnerability metrics, remediation dashboards, risk reporting, and executive-level security reporting.
- Maintain evidence, audit trails, and documentation supporting security assessments, remediation activities, and compliance initiatives.

Required Qualifications

- Bachelor's or Master's degree in Cybersecurity, Information Security, Computer Science, Software Engineering, or a related field (or equivalent practical experience).
- Hands-on experience with application security, secure coding, vulnerability assessment, SAST technologies, and security risk analysis within a modern software development environment.
- Strong understanding of vulnerability management principles, vulnerability lifecycle management, and remediation processes.
- Hands-on experience with Checkmarx or other SAST platforms.
- Experience with vulnerability scoring and risk assessment frameworks such as CVSS.

- Understanding of vulnerability triage, calibration, false-positive analysis, and risk-based prioritization methodologies.
- Familiarity with security standards and frameworks such as CIS controls and secure software development practices.
- Strong analytical, documentation, and reporting skills.
- Ability to communicate technical security findings effectively to both technical and non-technical stakeholders.

Personal Attributes

We are looking for someone who is:

- Highly analytical with a strong technical interest in application security and vulnerability research.
- Detail-oriented and capable of investigating complex security findings.
- Strong documentation skills
- Team-player with a drive for knowledge sharing