Application Security Engineer (Full Scope Poly)

Concept Plus is a mission-focused technology solutions provider that transforms IT concepts into impactful solutions for federal agencies. Headquartered in Fairfax, VA, we bring the agility, responsiveness, and customer intimacy of a small business combined with the quality and infrastructure of a larger firm.

Recognized as an award-winning Oracle partner, we have delivered innovative solutions across Defense, Intelligence, Civilian, Health IT, and Tribal sectors. Our highly certified experts build systems that drive efficiency, accelerate modernization, and ensure mission outcomes with certainty.

We offer competitive pay, comprehensive health, dental, and vision insurance, paid life insurance, paid time off, 11 paid holidays, performance bonuses, tuition reimbursement, unlimited training, and the opportunity to thrive in a collaborative, flexible, and innovative environment.

For more information, visit www.conceptplus.com.

About the role

Concept Plus is seeking a highly experienced and motivated Application Security Engineer for an exciting new contract. This role is fully onsite in Reston, VA (5 days per week required).

What you'll do

This role will be part of a team of Data, Cloud, and Security engineers delivering a cloud-native, centralized platform that provides end-to-end budget traceability. The Application Security Engineer will integrate security throughout the software development lifecycle, partnering with developers and cloud engineers to design, build, assess, and sustain secure mission applications.

Qualifications

- US Citizen
- Must possess a TS/SCI security clearance with Polygraph.
- Technical expertise and hands-on experience in application security, secure software development, software engineering, or DevSecOps, with the ability to apply these skills to Oracle Cloud and customer mission challenges.
- Experience integrating security throughout the software development lifecycle, including secure design and architecture reviews, threat modeling, secure code review, security testing, vulnerability remediation, and release authorization support.
- Experience developing or reviewing applications using Python, JavaScript frameworks, SQL, Shell scripting, PL/SQL, and other programming languages, with a strong understanding of common application vulnerabilities and secure coding practices.
- Experience with application security testing tools and processes, including static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), secrets scanning, and container or infrastructure vulnerability scanning.

- Experience building and securing cloud-native applications and services using Kubernetes, containers, Docker, REST APIs, and CI/CD pipelines.
- Experience implementing DevSecOps practices, including automated security controls and testing within build and deployment pipelines.
- Experience with cloud-native security services and controls; Oracle Cloud Infrastructure (OCI) experience is desired.
- Knowledge of security frameworks and standards such as NIST RMF, NIST Secure Software Development Framework, OWASP, DISA STIGs, and applicable federal security requirements.
- Experience securing Oracle RDBMS environments, including database access controls, encryption, auditing, and secure handling of sensitive data.
- Ability to assess, prioritize, document, and communicate application and cloud security risks, findings, and remediation recommendations to both technical and non-technical stakeholders.
- Passion for technology, curiosity, and willingness to continuously learn new security tools, techniques, and approaches for solving complex technical challenges.
- Experience working in an Agile framework.
- 8+ years of relevant experience in application security, software engineering, DevSecOps, cybersecurity, or a related technical discipline.
- Bachelor's Degree in engineering, computer science or related technical discipline. Master's degree preferred.

Preferred Qualifications

- Oracle Cloud Infrastructure (OCI) IaaS and/or PaaS certifications are preferred.
- Security certifications such as CISSP, CSSLP, Security+, GIAC, CEH, OSCP, or comparable credentials.
- Experience implementing identity and access management, privileged access controls, secrets management, encryption, logging, monitoring, and incident response capabilities in cloud environments.
- Experience with AI technologies for software development and securing AI-enabled applications or development workflows.
- Data engineering experience, including securing data validations, business rules, data transformations, and sensitive-data handling.

Concept Plus is an Equal Opportunity Employer. As such, we will give your application full consideration without regard to your race, color, religion, sex, age, national origin, disability, veteran status, sexual orientation, gender identity, or any other classification protected by federal, state, or local law.