

Software Security Engineer

Description

About the role As a DevSecOps engineer at Applied Intuition, you will play a crucial role in integrating security practices into our software development and operational processes. You will be responsible for enhancing system security, optimizing software deployment, and improving development workflows. Alongside the rest of the Corporate Security & Infrastructure team, you will work closely with the engineering teams to ensure the operational success and security of our internal software development and external customer deployments. At Applied Intuition, we encourage engineers to take ownership over technical decisions, interact closely with users to collect feedback, and contribute to a thoughtful, dynamic team culture. At Applied Intuition, you will: Instill security standards and best practices in software development and deployment processes Develop and maintain CI/CD pipelines for efficient and secure software deployment Design and implement security processes and tools across major cloud providers (AWS, GCP, Azure) as well as on-prem Implement and monitor security measures to protect internal and external systems, networks, and data Support vulnerability scanning, pen testing and incident response for all cloud services We're looking for someone who has: 5+ years of experience in software development, security, and operations Strong understanding of modern secure software development best practices Proficiency in CI/CD technologies (e.g. git, buildkite) and secure software deployment In-depth knowledge of cloud services (AWS, GCP or Azure) and hands-on experience securing cloud services Experience with containerization (Docker), orchestration (kubernetes) and infrastructure as code (e.g. Terraform) Strong understanding of system security and data protection Excellent problem-solving and collaboration skills Bachelor's in computer science or related field Nice to have: Proficiency in security best practices for javascript, python and C++ development Experience implementing real time security monitoring solutions Understanding of cloud infrastructure including networking, access control, IaaS, and SIEM tools Master degree focused on computer and systems security Certified Information Systems Security Professional (CISSP), Certified Kubernetes Administrator (CKA), AWS Certified DevOps Engineer, or other relevant certifications The salary range for this position is \$65,000 USD to \$400,000 USD annually. This salary range is an estimate, and the actual salary may vary based on the Company's compensation practices. This position will involve access to export controlled information. Disclosure of certain export controlled information requires status as a U.S. Person (e.g., as a U.S. citizen or national, as a lawful permanent resident of U.S., or as a protected individual, including asylee or refugee) or the eligibility to obtain applicable authorizations from the U.S. government. Please mention the word **PROFUSE** and tag RMzQuODYuMTYzLjE1Mg== when applying to show you read the job post completely (#RMzQuODYuMTYzLjE1Mg==). This is a beta feature to avoid spam applicants. Companies can search these words to find applicants that read this and see they're human.

Contacts

Job listing via [RemoteOK.com](https://www.RemoteOK.com)

Hiring organization

Applied Intuition

Job Location

Mountain View, California, United States

Base Salary

\$ 75000 - \$ 120000

Date posted

May 13, 2024

[Apply Now](#)