DevSecOps Engineer

About OptiFunder

OptiFunder is a leading provider of cloud technology to the residential mortgage finance industry and a pioneer of the Warehouse Lending Management System for mortgage originators. We provide technology solutions to non-bank mortgage originating institutions to help lenders originate more loans, reduce origination costs, and increase operational efficiency across the mortgage lifecycle. By joining OptiFunder, you'll become part of a forward-thinking company transforming how our customers embrace technology to enhance their business and the bottom line.

One of the fastest growing fintech companies, we offer the excitement of a rapidly growing technology disruptor with the stability of a seasoned management team, some of the brightest minds in mortgage banking, and the best talent around. Visit www.OptiFunder.com to learn more.

Job Description

OptiFunder is looking for a DevSecOps engineer who will work with the VP of IT, Information Security, and Compliance to design, implement, and maintain automation processes to build, test, secure, and deliver software applications in GCP using common DevOps and CI/CD processes. Additionally, the DevSecOps engineer will assist in designing and implementing internal IT systems and procedures (i.e., SaaS administration, endpoint management, device management, etc.).

Essential Functions

- Design, build, and maintain infrastructure-as-code used in the configuration and maintenance of the cloud infrastructure.
- Design, build, and maintain the CI/CD pipeline used to build, deploy, and test software applications in GCP.
- Actively develop and improve existing solutions for securing and monitoring all cloud environments, including SaaS products, GCP, Azure, and O365 workloads.
- Actively develop and improve existing solutions for securing and remotely managing all employee endpoint devices.
- Integrate security testing and controls into different phases of the software development lifecycle.
- Develop, scale, and control strategies, standards, guidelines, and governance of Continuous Integration systems
- Write and maintain documentation for internal systems and processes.
- Troubleshoot production issues in the CI/CD pipeline and Cloud environments.
- Collaborate with internal development teams on secure solution design and coding practices

- Work collaboratively with IT and Security to define and formalize detailed cloud security technical standards and guidelines
- Utilize agile methodology by making iterative progress toward achieving individual, team, and organizational objectives.

Skills and Experience

- 3+ years of relevant industry experience
- Experience with modern programming languages (e.g., Python, Java, Go) and distributed systems
- Deep expertise with one or more major cloud service providers like Amazon Web Services (AWS), Google Cloud (GCP), or Azure.
- Expertise in cloud service architecture and cloud security concepts
- Able to write clear, scalable, and clear design documentation
- Experience with Serverless compute services (e.g., Lambda, Cloud Run, Cloud Functions)
- Experience with Kubernetes and container security
- Infrastructure-as-Code experience (Terraform preferred)
- Linux and Windows operational experience.
- Experience with application security testing tools and methodologies.

Travel Requirements

This position can be remote and may occasionally require travel to corporate headquarters in St. Louis, client sites, or conferences.

Location: Open
Job Type: Full-time