



Michael ANDERSON

DEVSECOPS ENGINEER

CONTACT

- 📞 (555) 234-5678
- ✉️ michael.anderson@email.com
- 🌐 www.michaelanderson.com
- 📍 San Francisco, CA

SKILLS

- Terraform
- AWS
- Azure
- Cloud Security
- IaC
- Security Auditing
- Vulnerability Management
- Incident Response

LANGUAGES

- English
- Spanish
- French

EDUCATION

**BACHELOR OF SCIENCE IN
CYBERSECURITY, NATIONAL
UNIVERSITY**

ACHIEVEMENTS

- Improved cloud security posture, resulting in a 50% decrease in security incidents over 12 months.
- Successfully led initiatives that achieved compliance with PCI DSS standards.
- Received recognition for outstanding contributions to cloud security improvements.

Accomplished DevSecOps Engineer with a focus on automating security protocols within cloud environments, leveraging over 6 years of experience. Skilled in using tools such as Terraform, AWS, and Azure to implement Infrastructure as Code (IaC) while ensuring stringent security measures are in place. Adept at conducting cloud security assessments and vulnerability management, providing actionable insights to development teams.

WORK EXPERIENCE

DEVSECOPS ENGINEER

NextGen Technologies

2020 - 2025

- Implemented Infrastructure as Code using Terraform, achieving a 30% reduction in manual configuration errors.
- Conducted security assessments of cloud infrastructure, identifying and mitigating risks proactively.
- Automated security compliance checks that ensured adherence to industry standards.
- Collaborated with development teams to integrate security into the software development lifecycle.
- Created detailed documentation for security processes, leading to improved team understanding and compliance.
- Provided training sessions on cloud security best practices, enhancing team capabilities.

CLOUD SECURITY ANALYST

SecureCloud Solutions

2015 - 2020

- Conducted vulnerability assessments and penetration tests, reporting findings to development teams.
- Assisted in the development of security policies for cloud environments, ensuring compliance with regulations.
- Engaged in incident response activities, helping teams recover from security incidents.
- Documented security incidents and provided recommendations for future improvements.
- Collaborated with IT teams to enhance overall security architecture.
- Developed security awareness training programs for staff, resulting in a more security-conscious culture.