MA

Michael ANDERSON

APPLICATION SECURITY ENGINEER

Experienced Application Security Engineer with 6 years of experience in protecting enterprise applications from cyber threats. I began my career as a software tester, where I developed a keen understanding of application vulnerabilities. Over time, I transitioned into security roles, focusing on vulnerability assessments and security architecture.

CONTACT

☎ (555) 234-5678

✉ michael.anderson@email.com

🌐 www.michaelanderson.com

📍 San Francisco, CA

SKILLS

- Vulnerability assessments
- Threat modeling
- Secure coding
- Incident response
- Security policies
- Security awareness training

LANGUAGES

- English
- Spanish
- French

EDUCATION

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY, UNIVERSITY OF SCIENCE, 2015

ACHIEVEMENTS

- Achieved a significant reduction in critical vulnerabilities, leading to improved application security ratings.
- Recognized for outstanding performance in security assessments at Enterprise Solutions Group.
- Developed an internal security awareness program that increased employee engagement by 45%.

WORK EXPERIENCE

APPLICATION SECURITY ENGINEER

Enterprise Solutions Group

2020 - 2025

- Conducted security assessments for enterprise-level applications, identifying high-risk vulnerabilities.
- Collaborated with developers to implement secure coding practices, reducing vulnerabilities by 30%.
- Utilized threat modeling techniques to assess application risk profiles.
- Developed and maintained application security testing tools for continuous integration.
- Provided security expertise during architectural reviews and design sessions.
- Trained development teams on the OWASP Top Ten vulnerabilities and mitigations.

SECURITY ANALYST

SecureNet Corp.

2015 - 2020

- Performed vulnerability scans on critical applications, identifying and remediating security flaws.
- Assisted in developing security policies and procedures to enhance organizational security posture.
- Worked with incident response teams to address security breaches effectively.
- Maintained documentation of security assessments and remediation efforts.
- Conducted security awareness training for staff, promoting a culture of security.
- Evaluated third-party vendor security practices to ensure compliance with standards.