MA

(555) 234-5678

michael.anderson@email.com

San Francisco, CA

www.michaelanderson.com

SKILLS

- Financial Application Security
- Vulnerability Assessment
- Secure Coding
- Checkmarx
- Veracode
- PCI-DSS Compliance

EDUCATION

BACHELOR OF SCIENCE IN SOFTWARE ENGINEERING, UNIVERSITY OF FINANCE, 2015

LANGUAGE

- English
- Spanish
- German

ACHIEVEMENTS

- Successfully identified and remediated a critical vulnerability in a financial application, enhancing its security posture.
- Developed a training program that improved developers' security awareness by 40%.
- Awarded 'Best Security Project' for contributions to securing financial systems at FinSecure Technologies.

Michael Anderson

OFFENSIVE SECURITY ENGINEER

I am a dedicated Offensive Security Engineer with 6 years of experience in the fintech sector, focusing on securing financial applications and systems. My journey began in software development, where I gained insights into coding practices before pivoting to security. I specialize in identifying vulnerabilities within financial applications and implementing robust security controls to protect sensitive data.

EXPERIENCE

OFFENSIVE SECURITY ENGINEER

FinSecure Technologies

2016 - Present

- Conducted penetration tests on financial applications, identifying vulnerabilities that led to a 50% reduction in security incidents.
- Implemented secure coding practices by collaborating with developers during the software development lifecycle.
- Utilized Checkmarx and Veracode for static code analysis, ensuring secure code deployment.
- Developed comprehensive security policies that aligned with PCI-DSS compliance requirements.
- Facilitated security training for developers, increasing their awareness of potential security risks.
- Reported findings to stakeholders, influencing strategic security decisions within the organization.

SECURITY ANALYST

SecureFinance Corp.

2014 - 2016

- Performed security assessments on financial systems, identifying critical vulnerabilities and remediation strategies.
- Engaged in threat modeling activities to understand potential attack vectors within applications.
- Collaborated with IT teams to implement security patches and conduct vulnerability scans.
- Documented security incidents and responses, contributing to the organization's knowledge base.
- Participated in incident response efforts to mitigate security breaches effectively.
- Contributed to the development of a secure software development lifecycle framework.