MA

CONTACT

☎ (555) 234-5678

✉ michael.anderson@email.com

🌐 www.michaelanderson.com

📍 San Francisco, CA

SKILLS

- Vulnerability Assessment
- Security Awareness
- Incident Response
- Burp Suite
- Nessus
- Documentation

LANGUAGES

- English
- Spanish
- French

EDUCATION

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

ACHIEVEMENTS

- Successfully reduced vulnerability exposure time by implementing a new tracking system.
- Recognized for outstanding contributions to security training programs.
- Achieved a Certified Ethical Hacker (CEH) certification in 2021.

Michael
ANDERSON

VULNERABILITY MANAGEMENT ENGINEER

As a detail-oriented Vulnerability Management Engineer with over 6 years of experience in the tech industry, I have developed a strong expertise in identifying and mitigating security vulnerabilities. My career began in a software development role, which provided me with a unique perspective on coding practices and vulnerabilities inherent in applications.

WORK EXPERIENCE

VULNERABILITY MANAGEMENT ENGINEER

NextGen Technologies

2020 - 2025

- Conducted vulnerability assessments on applications and networks, identifying critical security gaps.
- Utilized Burp Suite and Nessus to perform automated and manual testing.
- Collaborated with development teams to remediate vulnerabilities, reducing open issues by 35%.
- Developed and maintained comprehensive documentation of vulnerabilities and remediation efforts.
- Led security awareness training for teams, increasing reporting of vulnerabilities by 20%.
- Participated in incident response activities, providing insights on vulnerability impacts.

SECURITY ANALYST

Secure Innovations

2015 - 2020

- Performed regular vulnerability scans and assessments using various tools and techniques.
- Assisted in developing security policies and procedures to enhance compliance.
- Provided support during security audits, ensuring all findings were documented and addressed.
- Monitored security alerts and responded to incidents in a timely manner.
- Engaged with cross-functional teams to promote security best practices.
- Maintained up-to-date knowledge of emerging threats and vulnerabilities.