MICHAEL ANDERSON

SENIOR IAM ENGINEER

CONTACT

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

SKILLS

- Identity Governance
- SailPoint
- RSA
- Risk Assessment
- Compliance
- Security Frameworks

LANGUAGES

- English
- Spanish
- French

EDUCATION

MASTER OF SCIENCE IN CYBERSECURITY, STATE UNIVERSITY, 2014

ACHIEVEMENTS

- Instrumental in achieving ISO 27001 certification for the organization.
- Recognized for improving user onboarding times by 60% through streamlined IAM processes.
- Speaker at national security conferences on IAM innovations and trends.

PROFILE

Dynamic IAM Engineer with a decade of experience specializing in enterprise security frameworks and identity governance. Skilled in deploying identity management solutions that enhance both security and efficiency within large organizations. Proficient in using tools such as SailPoint and RSA to develop comprehensive IAM strategies. Strong analytical skills with a focus on risk assessment and compliance.

EXPERIENCE

SENIOR IAM ENGINEER

Global Security Corp.

2016 - Present

- Led a team in the implementation of SailPoint IdentityIQ, enhancing identity governance across the organization.
- Developed and enforced IAM policies that reduced security incidents by 50% year-over-year.
- Conducted audits and compliance checks, ensuring adherence to industry regulations.
- Managed the integration of IAM solutions with cloud providers, improving access management efficiency.
- Collaborated with stakeholders to define access controls and user roles across multiple departments.
- Provided training and support to users on IAM best practices and tools.

IAM ANALYST

TechGuardians LLC

2014 - 2016

- Assisted in the deployment of RSA SecurID, which improved authentication processes for over 5,000 users.
- Performed regular access reviews and reported findings to senior management, leading to improved access control measures.
- Facilitated user training sessions to enhance understanding of IAM systems.
- Monitored IAM systems for anomalies and provided timely resolutions.
- Documented IAM processes and procedures for future reference and compliance.
- Engaged with IT teams to troubleshoot and resolve IAM-related issues effectively.