MA

📞 (555) 234-5678

✉ michael.anderson@email.com

📍 San Francisco, CA

🌐 www.michaelanderson.com

SKILLS

- Industrial Control Systems
- ISA/IEC 62443
- Risk Assessment
- Vulnerability Management
- Security Training
- Incident Response

EDUCATION

BACHELOR OF SCIENCE IN INFORMATION SECURITY, UNIVERSITY OF INDUSTRY, 2014

LANGUAGE

- English
- Spanish
- German

ACHIEVEMENTS

- Reduced security incidents in manufacturing environments by 30% through effective audits.
- Recognized for excellence in cybersecurity initiatives by industry peers.
- Developed a comprehensive cybersecurity training program for operational staff.

Michael Anderson

CYBERSECURITY AUDITOR

Proactive Cybersecurity Auditor with 9 years of experience in the manufacturing industry, focusing on securing industrial control systems and operational technology. My expertise includes conducting audits and assessments to identify vulnerabilities in critical infrastructure and ensuring compliance with relevant regulations such as NIST and ISA/IEC 62443. I am skilled in collaborating with cross-functional teams to implement security measures that protect against cyber threats while maintaining operational efficiency.

EXPERIENCE

CYBERSECURITY AUDITOR

Industrial Security Solutions

2016 - Present

- Conducted audits of industrial control systems to ensure compliance with ISA/IEC 62443 standards.
- Identified vulnerabilities in operational technology and recommended remediation strategies.
- Collaborated with engineering teams to implement security measures for critical infrastructure.
- Facilitated cybersecurity training sessions for employees in manufacturing environments.
- Developed risk management frameworks tailored to industrial settings.
- Presented audit findings to senior management, driving security policy enhancements.

INFORMATION SECURITY ANALYST

Manufacturing Security Group

2014 - 2016

- Assisted in conducting risk assessments for operational technology environments.
- Monitored security incidents and responded to potential threats in real-time.
- Engaged in regular reviews of security policies and incident response plans.
- Collaborated with cross-functional teams to ensure security best practices were applied.
- Provided security awareness training to manufacturing staff on cybersecurity risks.
- Participated in the development of incident response protocols for industrial systems.