BENDER CONSULTING SERVICES, INC.

Career Opportunities for People with Disabilities

Recruiting and Hiring people with disabilities for competitive career opportunities.

SECURITY ENGINEER (DEV SEC OPS) IN PITTSBURGH, PA

THE DEV SEC OPS ENGINEER IS RESPONSIBLE FOR UNDERSTANDING AND PROVIDING GUIDANCE TO INTERNAL TEAMS ON THE BEST PRACTICES IN SOFTWARE SECURITY AND ARCHITECTURE.

ABOUT OUR COMPANY:

With over 20 years of experience in supporting corporate and federal recruitment, workplace mentoring, and technology accessibility initiatives, Bender Consulting Services, Inc. is the leading national expert in disability employment solutions for private and public sector employers. To learn more about how to start your career with Bender Consulting Services, Inc., please visit our website at www.benderconsult.com.

HOW TO APPLY:

To apply for consideration for the following career opportunity for people with disabilities, please visit www.benderconsult.com/careers/submit-resume and complete the electronic form.

POSITION DESCRIPTION:

- Coordinate with other IT teams on timely resolution of IT security-related issues
- Identify and define security requirements for operating systems and applications
- Investigate anomalies and assist with developing remediation to network and application infrastructure security related issues and concerns
- Recommend, implement, and test control sets and security measures to mitigate inherent risk identified through cyber-security risk assessments.
- Assist with the creation, development, and maintenance of IT security related policies, procedures, and standards documentation
- Maintain knowledge on current and emerging security trends, risks, vulnerabilities malware, infiltration techniques, forensics, and threats
- Design technical control standards and strategies for a variety of information systems based on industry best practices and guidelines
- Perform other duties as assigned

QUALIFICATIONS:

- Bachelor's Degree in Computer Science, Systems Engineering, CIS or related technical subject, or qualifying in field experience
- Knowledge of HITRUST CSF, NIST 800-83 cyber security framework, PCI, HIPAA, HITECH, COBIT, ISO 27001/2, and/or ITIL 3
- Experience with technologies such as Intrusion Prevention Systems (IPS), firewalls, endpoint protection, web/email filtering, Data Loss Prevention (DLP), digital rights management, encryption, Security Event and Incident Management (SEIM), and virtualization platforms
- Proven ability to maintain a high level of concentration over an extended period of time
- Strong verbal communication and problem-solving skills
- Ability to estimate efforts, commit to timelines and complete technical tasks on time
- Must be self-driven, able to work independently while still coordinating with multiple departments
- Ability to multi-task with a calm demeanor and work under pressure in a fast-paced environment
- Knowledge of NIST Risk Assessment methodology
- Knowledgeable in security best practices including industry standards