**Job Title: Operational Technology (OT) Cyber Security Engineer - New Grad**

**Job Description:**

We are seeking a highly motivated and detail-oriented OT Cybersecurity Engineer to join our team, focusing on securing critical infrastructure and operational technology (OT) environments. As a recent graduate, you will work alongside experienced cybersecurity professionals to safeguard industrial control systems (ICS), SCADA systems, and other OT assets from cyber threats. This is an excellent opportunity to build a career in a rapidly growing field, where you’ll play a vital role in protecting essential industries such as energy, manufacturing, and transportation.

**Key Responsibilities:**

1. Cyber Risk Assessments: Support the assessment of OT systems to identify vulnerabilities, risks, and compliance gaps. Assist in conducting penetration testing and vulnerability scanning of industrial environments.

2. Network Security Implementation: Collaborate with network engineers and OT teams to design and implement secure network architectures, including segmentation strategies, firewall policies, and access control mechanisms in line with industry standards (e.g., NIST, IEC 62443).

3. Incident Response & Mitigation: Participate in OT cybersecurity incident response efforts, working with teams to contain and remediate security breaches while documenting lessons learned.

4. Cybersecurity Policy & Procedure Development: Assist in developing and maintaining cybersecurity policies, guidelines, and standard operating procedures tailored to OT environments.

5. Security Audits & Compliance: Help prepare for and support security audits and assessments to ensure OT environments are compliant with relevant regulations and standards, such as NERC CIP, NIST, and ISO 27001.

6. Cybersecurity Training & Awareness: Contribute to cybersecurity awareness programs, helping OT staff and engineers understand security best practices for managing and maintaining critical systems securely.

**Qualifications and Experience:**

- Bachelor's degree in Computer Science, Cyber Security, or a related field. A Master's degree is a plus.

- Hands-on experience with vulnerability assessment tools, penetration testing, and security analysis tools specific to ICS environments.

- Proficiency in programming languages commonly used in ICS environments (e.g., C, C++, Java, Python).

- Foundational knowledge of networking protocols, firewalls, VPNs, IDS/IPS, and other network security concepts, with an interest in learning how they apply to OT environments.

- Strong analytical and problem-solving skills with an ability to think critically and innovatively in complex cyber security scenarios.

- Excellent communication and interpersonal skills, able to work collaboratively and effectively across teams.