Job Title: SecOps Engineer

Job Type: Permanent, Full-Time

Reporting to: Manager, Technology Operations

Summary:

The SecOps Engineer is passionate about technology and has experience with both traditional on-premises systems as well as cloud environments. The SecOps Engineer is responsible for safeguarding the operation of the company systems and network, and the organization's cyber security champion. They will be accountable for cyber security considerations and oversee system and network design, implementation, organization, and troubleshooting.

The incumbent is a self-starter who "owns" the product(s), knows inherently what is required to be successful in the role and has the leadership skills to engage others within the organization to help drive our business forward.

Key Responsibilities:

- Design, configure and maintain secure systems and protocols. Work closely with developers, system administrators and other stakeholders to identify security risks and develop strategies to mitigate them.
- Develop & maintain security policies and procedures, implement access controls, and ensure compliance with industry standards and regulations.
- Implement security tools to detect and respond to security incidents using tools such as IDS and SIEM.
- Utilize vulnerability scanners and penetration testing tools to identify and assist in remediation of software and hardware vulnerabilities.
- Conduct risk assessments to identify potential security threats and vulnerabilities.
- Educate employees and other stakeholders about the importance of security and how to protect sensitive information. Work with other teams to ensure that security is integrated into the organization's culture and processes.
- Staying up-to-date with emerging technologies and security trends.
- Provide after-hours support as required on emergency basis and for projects scheduled outside of business hours.

Requirements:

- Strong knowledge of network and system security, including firewalls, intrusion detection systems and encryption technologies.

- Familiarity with security standards and regulations such as NIST and OSFI.
- Experience with security tools and technologies, such as SIEM and vulnerability scanners.
- Understanding of cloud security, including cloud infrastructure and application security.
- Experience with developing a Zero-Trust framework model.
- Coordination and organization skills.
- Attention to detail and ability to follow processes and procedures.
- Strong Analytical skills and moderate strategic planning
- Experience with Azure Cloud Services, Azure Sentinel and Fortinet preferred.
- Both a team player and self-directed.

Qualifications:

- Minimum requirement: College Diploma in computer science, software engineering, technology or equivalent 4+ years in a networking or information security role.
- Strong facilitation, negotiation, and consultation skills, including the ability to communicate effectively both verbally and in writing at all levels of the organization.
- Cyber Security focused industry courses/certifications: Microsoft, CompTIA, Cisco or $(ISC)^2$ certifications considered an asset.
- ITIL Service Management exposure/knowledge/certification is also considered an asset.
- 5+ years of hands-on experience in a network or Cloud administration role, and 2+ years in a Security Operations role, including:
    - SIEM, log aggregation, IDS/IPS, EDR
    - LANs, Firewalls, L2/L3 Switches
    - Azure Cloud, GIT and DevOps
    - Windows Active Directory, EntraID, Microsoft Defender Suite
    - WAF, WAS