Security and Operations Analyst

MacDon

PURPOSE and SCOPE:

As a member of the Information Technology team, the Security and Operations Analyst will be responsible for the implementation, maintenance, and integration of the corporate network and security architecture. This individual will also be responsible for implementation and administration of network hardware and software, enforcing the network security policy, and complying with requirements of internal and external security audits and recommendations.

The Security and Operations Analyst is not only responsible for the day-to-day availability of the security infrastructure, but will also leverage their experience, skills, and new technologies to provide new and better solutions in a challenging technical environment.

JOB RESPONSIBILITIES:

The following are the main job responsibilities and priorities that this position must focus on, must achieve, and must excel at:

- Administer day-to-day security operations, ensuring the identification and remediation of information security risks, threats, and vulnerabilities
- Administer security tools to protect systems, networks, and applications. This includes firewalls, intrusion detections and prevention systems, security gateways etc.
- Participate and document security incidents, with in-depth assessment of potential impact to MacDon and remediation steps to resolve and prevent future incidents
- Research, recommend, and manage the rollout, health, and support of projects related to IT Security solutions
- Contribute to the design, integration, and installation of hardware and software
- Assist in developing company-wide standards, policies, and best practices for IT security
- Create and maintain documentation for all equipment within the Security Operations
- Implement monitoring for security solutions and perform knowledge sharing with the team
- Provides tier two support to Service Desk in resolving issues and problems.
- Troubleshooting and quickly determining the resolution to infrastructure issues that arise
- Analyzing, troubleshooting, and correcting network problems remotely and on-site

QUALIFICATIONS:

Education and Experience

- A post-secondary degree or diploma in a relevant field (i.e., computer science, engineering, networking, etc.), or a combination of relevant experiences and education.
- A recognized certification in the application of enterprise cybersecurity best practices and/or auditing will be considered a strong asset (i.e., CSX-P, CISSP, CISA, etc.).
- Experience with any form of automation via tooling or scripting of the infrastructure, security, and configuration management layers
- Experience managing projects and a track record of delivering projects on time

Skills and Knowledge

- Exceptional communications and interpersonal skills accompanied with a strong work ethic and customer focus
- Ability to collaborate with teams and employees working across multiple locations
- Ability and willingness to work in a 24x7 on-call rotation schedule
- Strong analytical and problem-solving skills (including root cause analysis), critical thinking and attention to detail and quality.

Interested applicants can submit resume and cover letter to Tara Bees-Cook at employment@macdon.com