Managed Services - Security Operations Center Security Analyst (L1)

Title:	Managed Services – Security Analyst (L1)
Office Location:	Toronto
Role type:	Full-time
Reports to:	Cyber Security Operations Manager

About Scalar Decisions:

Scalar Decisions Inc. (“Scalar”) is an IT solutions integrator, specializing in architecting, implementing and managing mission-critical IT environments. A national organization headquartered in Toronto, Scalar’s 185 plus employees service customers from offices in Toronto, Vancouver, Calgary, London, Montreal, and Ottawa.

Scalar has grown aggressively since its inception, and is now the 15th largest ICT solution integrator in the country, up from #75 in 2007. We focus on recruiting top talent, and we work hard to keep them. To learn more about Scalar go to www.scalar.ca.

Job Summary:

Are you an individual who is motivated by CURIOSITY, driven for success and excellent customer service? Do you like working in a fun, fast-paced and rapidly growing work environment? Scalar Decisions is looking for a SOC Security Analyst to join its 24x7 Security Operations Centre team.

The Security Operation Centre (SOC) Security Analyst is the first level of monitoring in the SOC. The position monitors and responds to security events from managed customer security systems as part of a team on a rotating 24 x 7 x 365 basis.

Your background should include exposure to security technologies including firewalls, IPS/IDS, logging, monitoring and vulnerability management. You should have an understanding of network security practices. Excellent customer service while solving problems should be a top priority for you. Scalar is a fast-paced, entrepreneurial environment so to be successful you’ll need to be a pro-active individual, take direction well, communicate succinctly and collaborate effectively.

Core Responsibilities:

- The security analyst monitors security events from the various SOC entry channels (SIEM, Tickets, Email and Phone), based on the security event severity, escalate to managed service support teams, tier 2 security analysts, and/or customer as appropriate to perform further investigation and resolution.
- Recommend enhancements to SOC security process, procedures and policies.
- Participate in security incident management and vulnerability management processes
- Participate in evaluating, recommending, implementing, and troubleshooting security solutions and evaluating IT security of the new IT Infrastructure systems.

- Works as part of a team to ensure that corporate data and technology platform components are safeguarded from known threats
- Communicate effectively with customers, teammates, and management
- Provide input on tuning and optimization of security systems
- Follow ITIL practices regarding incident, problem and change management
- Document and maintain customer build documents, security procedures and processes.
- Staying up-to-date with emerging security threats including applicable regulatory security requirements.
- Other responsibilities and additional duties as assigned by the security management team
- Security Operation Centre positions require employees to obtain and maintain a Government of Canada Level 2 – Secret security clearance. This clearance requires Canadian Citizenship or Permanent Resident status with 10 years residency in Canada.

Qualifications:

Ideal candidates will have as much of the following

- Preferred Information Security professional designations such as CISSP, CISM, CISA
- 1-3 years previous Security Operations Centre Experience in conducting security investigations
- Detail oriented with strong organizational and analytical skills
- Strong written communication skills and presentation skills
- Self-starter, critical and strategic thinker, negotiator and consensus builder
- Good knowledge of IT including multiple operating systems and system administration skills (Windows, Solaris, Unix)
- Basic knowledge of client-server applications, multi-tier web applications, relational databases, firewalls, VPNs, and enterprise Anti-Virus products
- Strong understanding of security incident management, malware management and vulnerability management processes
- Security monitoring experience with one or more SIEM technologies – Q1 Radar, Splunk and intrusion detection technologies
- Experience with web content filtering technology - policy engineering and troubleshooting
- Strong understanding of networking principles including TCP/IP, WANs, LANs, and commonly used Internet protocols such as SMTP, HTTP, FTP, POP, LDAP
- A Bachelor's Degree / Diploma in a relevant area of study with a preference for Information Security, Computer Science or Computer Engineering
- Excellent english written and verbal skills.
- Shift work required
- After-hours availability required
- Carry rotating pager as required
- Candidates applying for the position must be legally able to work in Canada

If you are a passionate team player and you are interested in the above position or know someone who is send your resume to careers@scalar.ca