SOC Manager

JOB DESCRIPTION

Reporting directly to the CEO, you will lead a team of individuals dedicated to providing the following services:

- Network security architecture planning;
- Operational Security Support;
- Security incident management;
- Post-compromise investigations;
- Security Information and Event Management
- IT infrastructure documentation;
- Change management / implementation

In this position, the selected candidate will have customer-facing responsibilities and will need to be experienced in the fulfillment and delivery of IT solutions.

You will use your leadership and vision combining with exceptional technical ability to grow and mature an existing team.

KEY RESPONSIBILITIES

- Manage SOC team of 15 analysts
- Foster relationships with industry partners and customers to ensure monitoring compliance and smooth incident response
- Manage team efforts to monitor for security events and provide first and final escalation analysis
- Lead team in next-generation firewall (NGFW), Intrusion Prevention System (IPS) and SIEM management, maintaining and improving organization defensive controls
- Lead staff in proactive change management for defensive controls and maintaining an effective defense for clients over time
- Lead staff to proactively identify, prevent and respond to security incidents
- Lead and manage security incidents from identification through remediation
- Coordinate with the ASOC and IR teams during compromise assessments or as part of IR escalation
- Collaborate with technical security assessment (intrusion testing) and cyber threat intelligence teams to validate security events and perform advanced analysis
- Develop salient information security metrics and present to senior leadership
- Additionally, the SOC Manager will have a major role in developing the vision for GoSecure Managed Security Services
- Professional communication, including executive level, and documentation of processes and procedures.
- Perform tasks related to security incident response, such as monitoring and discovery

DESIRED SKILLS AND EXPERIENCE

The ideal candidate will have the following qualifications:

- Bachelors or college degree of computer science, computer engineering or other relevant degree;
- Relevant industry certifications such as GCIH, GCED, CISSP, CISA, CISM.
- Relevant technology vendor certifications (Cisco, CheckPoint, RSA, etc.)
- Experience building and maintaining a high performance team of analysts
- Expertise with industry standard frameworks (ISO, NIST, PCI)
- Familiarity with ITIL and Agile framework / methodologies
- Experience maintaining metrics and SLAs
- Strong knowledge of incident management, problem management and change management best practices
- A high level understanding of multi-tiered applications, load balancing and firewalls
- 8+ years of Information Security / Cybersecurity experience
- 2+ years working in a security operations center
- 2+ years in a leadership role
- Understanding of private, public, and hybrid cloud operations
- Experience networking and telecommunications integration, design and architecture
- Experience in the fulfillment and delivery of proposed solutions;

Due to the nature of services we provide and our clients, we conduct strict criminal, financial and reputational background checks. Applicants must be eligible to work in Canada and have (or be able to obtain) Government of Canada Level II (SECRET) clearance.

The following personal abilities are favored at GoSecure:

- Excellent problem solving skills;
- Exceptional organizational skills;
- Ability to think of problems and operational activities beyond technical scope, envisioning general business and political ramifications;
- Ability to work independently and handle multiple tasks concurrently;
- Adaptable to diverse environments;
- Superior verbal and written communication skills in English and French are mandatory;
- Assertive and self-driven individual who can ensure tasks are followed through until completion
- Attention to detail and motivated to deliver exceptional quality
- Energetic and positive with a "can do" attitude.

GoSecure has a policy in place to support Canadian Forces reservists.

GoSecure has a strong continuing education policy for its employees, ensuring our personnel achieves graduate level degrees within a few years of hire.

ABOUT OUR COMPANY

Founded in 2002, GoSecure is focused on managing risks inherent to information management systems through its highly specialized Ethical Hacking and IT Security Infrastructure Co-Management services.

Throughout its 14 years in business, our firm of forty-five dedicated engineers and analysts has distinguished itself by the depth of its technical knowledge, model ethics, and the overall professionalism demonstrated by its members. GoSecure combines the best technology through its partnerships and its unique know-how in regards to security trends, threats and solutions in order to meet the needs of its most demanding customers.