Stratejm is currently seeking a Cyber Intelligence Center (CIC) Team Lead with advanced skillsets in cyber security, to manage and supervise cyber security services for a variety of customers. Candidates should have excellent written and oral communication skills, be able to work independently and as part of a team, with demonstrated leadership capabilities. Skills and experience in Operations Management, Security Event Analysis, Incident Response, Threat Hunting, Malware Analysis, and Cyber Threat Intelligence (skills in more than one cyber discipline are preferred) are required for this position. The ideal candidate will have hands-on experience supporting a 24x7x365 SOC/NOC environment. The candidate will recommend improvements in current processes and implementation of system changes. Monitors procedures and provides top management with reports on a regular basis. Responsible for doing quality control checks on all client-facing deliverables for the Cyber Intelligence Team.

**Responsibilities**

* Provide high quality analysis of security incidents detected within the customers environment.
* Supervision of the CIC team, recruiting, hiring, training and assessment of staff and technologies.
* Manage day-to-day activities of the CIC Team in regard to: Security Monitoring, Investigations and Response, and Threat and Vulnerability Intelligence
* Support the development and analysis of the effectiveness of security tools and processes
* Work with Clients internal technology teams and CIC analysts for conducting Root Cause Analysis (RCA) and provide remediation recommendations.
* Management of the escalation process and review of incident reports
* Development and measurement of CIC Performance and Service Level Metrics
* Being an advocate for security services to our clients
* Maintaining working knowledge of cyber threat actor tactics and techniques
* Reviewing client issue and taking steps to remediate security threats and incidents

**Qualifications**

* Previous hands-on experience with a Security Information and Event Monitoring (SIEM) platforms and log management systems that perform log collection, analysis, correlation, and alerting.
* A working knowledge of the various operating systems (e.g. Windows, OS X, Linux, etc.) commonly deployed in enterprise networks, a conceptual understanding of Windows Active Directory is also required, and a working knowledge of network communications and routing protocols (e.g. TCP, UDP, ICMP, BGP, MPLS, etc.) and common internet applications and standards (e.g. SMTP, DNS, DHCP, SQL, HTTP, HTTPS, etc.).
* Experience with the identification and implementation of counter-measures or mitigating controls for deployment and implementation in the enterprise network environment.
* Ability to work on-call during critical incidents or to support coverage requirements (including weekends and holidays when required).
* Ability to work independently and yet be effective within a team setting
* Must be capable of managing multiple efforts with time related constraints in a fast-paced contracting environment
* Demonstrated ability to effectively communicate and collaborate with diverse internal and external stakeholder groups and individuals
* Friendly presence, helpful attitude, good interpersonal skills, and ability to work well with others.
* Bachelor’s degree in technology, information systems, or related field preferred.
* Security+, Network+, CySA+, SSCP, CISSP, CEH, or CASP a plus.
* Technical writing experience.
* Proven team leadership, effective employee relations and interpersonal skills
* Strong organizational skills and result-oriented
* Understand, adhere to, and enforce Corporate Policies & Procedures.