JOB TITLE: SOC ANALYST

PURPOSE: To perform Monitoring and Operator Services, Security Analysis and Incident Response activities

DUTIES:

- Monitors the dashboards of the various security solutions in order to detect any alerts of incidents
- Creates/updates tickets for all security Incidents that are observed or reported.
- Leads/participates in the investigation and validation of identified security incidents
- Proactively hunts for threats by analyzing security logs in order to identify incidents
- Assists in the response and resolution of security incidents
- Creates and maintain Incident Response documentation, including processes, and procedures to facilitate the resolution of cybersecurity incidents.
- Researches build and maintain an internal database on threat intelligence and vulnerabilities to aid in the analysis, resolution, remediation and reference of security incidents
- Escalates security incidents to the SOC manager so a decision can be taken to alert clients or other relevant stakeholders
- Communicates technical issues to non-technical personnel
- Generate and compile periodic and situational reports on security incidents for management, clients and other stakeholders

EDUCATIONAL QUALIFICATIONS:

- A Bachelor’s Degree in Computer Science, Computer Security, Electrical Engineering or related Degree OR Extensive working knowledge + certifications in Lieu of Degree.
- Must have IT Security Fundamentals, experience in the administration of Windows and Linux OS’s, and general databases knowledge, as well as general network knowledge.
- Desirable certifications like MCSA, CCNA, Linux+, Security+, CySA+, CEH, CHFI, CISSP, etc

Send your applications to HR@cyber-hawk.com