Cyber Security (SOC) Analyst

Details: Candidate must be able to obtain a Secret Clearance or already have one on file.

Major Responsibilities:

- Direct the functions, processes, and operations of the SOC and ensures policies, procedures, and objectives align with industry best practices.
- Lead the operations of the SOC to ensure optimal identification/resolution of security incidents, and enhance client security
- Manage the collection, documentation and research of security events generated by the SOC monitoring platform
- Monitor key performance indicators, determine gaps in performance metrics, and recommend/execute change management techniques for efficiency/quality improvements
- Oversee the monitoring, identification and resolution of security events to detect threats through analysis, investigations and prioritization of events based on risk/exposure
- Manage outsourced and in-house SOC services for quality performance and fulfillment of Service Level Agreements (SLA)
- Develop and maintain an incident response management program that includes incident detection, analysis, containment, eradication, recovery and chain of evidence/ forensic artifacts required for additional investigations.
- Develop, maintain, and submit SOC compliance reports as required by the client
- Develop appropriate response strategies based on intelligence received
- Communicate threats to Senior Management which may impact the client
- Analyze applications functionality and new technologies to optimize effective/efficient incident review by staff and minimize client risk
- ·Conduct scheduled and ad hoc training exercises to ensure staff are current with the latest threats and incident response techniques
- Oversee and develop strategies to identify, detect, and prevent malicious activity
- Perform supervisory/managerial responsibilities
- Ensure adequate/skilled staffing; select employees
- Establish performance goals and priorities
- Prepare, conduct and review performance appraisals
- Develop, mentor and counsel staff
- Provide input and/or prepare budget requirements for Annual Financial Plan (AFP)
- Ensure section/branch goals and objectives align with division/department strategy
- Ensure efficiency of operations
- 10+ years of experience in the Cyber Security field.
- BS/BA degree or equivalent combination of related work experience desired.
- Prior MSS SOC Management experience highly desired.
- Prior Security Engineering Experience desired.
- Prior security analysis experience is required.
- Desirable certifications include, Security+, Splunk, CEH, GCIA, GCIH, CISSP or similar.

To apply, please send resumes to contact@intellectualpoint.com