TIER 1 SOC ANALYST IN HERNDON, VA

Job Description

- Location: Herndon, VA
- Supporting:
    - Multiple Federal clients on multiple contracts (position is not tied to one specific contract)
- Clearance:
    - Citizens who can process for DHS EOD (can hold up to a DOD TS)

The SOC Analysts must be willing to work in a 24x7x365 Security Operations Center environment and demonstrate intuitive problem solving skills. The Analysts will be responsible with monitoring network traffic for security events and perform triage analysis to identify security incidents, respond to computer security incidents by collecting, analyzing, preserving digital evidence and ensure that incidents are recorded and tracked in accordance with SOC requirements.

This SOC supports 5+ government customers across 30+ programs. The SOC team is made up of around 35 Analysts (Tier 1 -3) and is growing! Because the SOC supports a matrix of programs, there are multiple tools used, so it's a great environment for a more entry level Analyst to join and learn in a sandbox environment.

We're seeking folks who have a general understanding of network security concepts and a passion for Cyber Security; those who follow Cyber Security blogs, articles etc. and make it a point to stay updated with recent happenings within the Security space are highly encouraged to apply! This is a terrific environment to get your foot in the door and grow within a Fortune 500 company! This opportunity will also process candidates for various clearances.

The SOC team works closely with the other teams to assess risk and provide recommendations for improving our clients security posture.

Day to Day Responsibilities:

- Performs network security monitoring and incident response for a large organization, coordinates with other government agencies to record and report incidents.

- Maintains records of security monitoring and incident response activities, utilizing case management and ticketing technologies.
- Monitors and analyzes Security Information and Event Management (SIEM) to identify security issues for remediation.
- Knowledge of creating Security Information Event Management (SIEM) tool rules.
- Recognizes potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information
- Communicates alerts to agencies regarding intrusions and compromises to their network infrastructure, applications and operating systems. Consolidates and conducts comprehensive analysis of threat data obtained from classified, proprietary, and open source resources to provide indication and warnings of impending attacks against unclassified and classified networks.
- Recommend changes to Standard Operating Procedures and other similar documentation
- Generates end-of-shift reports for documentation and knowledge transfer to subsequent analysts on duty.

Qualifications:

- 1-3 (+) years of related experience in information technology and/or information security preferred
- An understanding of Cyber Security Incident Response and Network Security Monitoring
- Fundamental understanding of computer networking (TCP/IP)
- Knowledge of Windows, Linux and Cisco operating systems and information security
- Knowledge of Intrusion Detection Systems (IDS) and SIEM technologies; Splunk, Symantec antivirus, Firewalls and Sourcefire and similar tools preferred.

Send Resume to info@intellectualpoint.com.