Position: Mid-Tier Incident Response Team Analyst
Location: Washington, DC

Summary of Position

Kent, Campa and Kate Inc. (KCK) is a federal contracting company that provides professional services to government agencies. We are currently looking for a Veteran, Family Member or qualified candidate to fill a Mid-Tier Response Team Analyst position supporting Health and Human Services (HHS).

Position Description

We are currently looking for a Mid-Tier Incident Response Team Analyst, whose secondary duties are to serve as an Assistant Team Lead and on a Security Operations team on a contract with a federal government client with an important mission.

Duties and Responsibilities

- Support/assist the client with real-time monitoring and triage of incident received at the operations center.
- Work collectively with other team members on incident analysis and response, and coordinate with external teams on resolution of incidents.
- Support efforts on threat hunting, network, host, and malware analysis, sensor tuning and custom signature creation.
- Lead the application of cyber intelligence to improve security operations.
- Oversee and perform investigation of network and hosts/endpoints for malicious activity, to include analysis of packet captures.
- Oversee and assist in efforts to detect, confirm, contain, remediate, and recover from attacks.
- Prepare executive summaries and conduct briefings on significant investigations.
- Measure and manage individual and team performance.
- Ensure adequate metrics and documentation of team operations for leadership and other constituents.

Required Qualifications

Education

- BS/BA degree from accredited university
- Five or more years of work experience
- Three or more years of cyber security work experience
- Prior leadership experience with direct reports in a cyber environment
- Experience and effective participation in hunt, computer network defense, real-time analysis and incident response activities, to include ability to reconstruct events from network, endpoint, and log data
- Experience and understanding of host-based/endpoint protection systems
- Cyber intelligence, disk forensics and memory forensics experience

Please submit resumes at KCK's website at www.kckforvets.com or email to earlgray@kckforvets.com
For additional information email earlgray@kckforvets.com or call (703) 282-0767.

- Server administration experience
- Enterprise forensic tool(s) experience
- Federal contract experience

Training Requirements

- One or more certifications in information security (such as GCIA, GCIH, CEH, CISSP, SSCP, Sec+, etc)

Specialized Knowledge/Skills Requirements

- High technical ability/aptitude, demonstrated through prior technical experience and accomplishment
- Network investigation experience, to include netflow and packet/protocol capture and analysis
- Endpoint/host forensics experience
- SIEM experience
- Strong critical thinking, problem solving, and organization skills
- Strong teamwork and collaboration skills
- Good written and verbal communication skills
- Ability to pass a security clearance background investigation
- Sound cyber security knowledge foundation, to include understanding of
    - Adversary TTPs
    - Network technology and common protocols
    - Network security
    - Host security
    - Malware
    - Security tools and sensors

Please submit resumes at KCK's website at www.kckforvets.com or email to earlgray@kckforvets.com
For additional information email earlgray@kckforvets.com or call (703) 282-0767.