THREAT AND VULNERABILITY ENGINEER IN WASHINGTON, DC

This individual will be responsible for identifying threats and driving out vulnerabilities for a large DoD client. The ideal candidate will have excellent analytical, engineering, communication, and technical skills including web scanning, performing vulnerability trending using ACAS, and validation of C&A activity. This role will include performing offensive security measures including threat hunting and red team activity.

Threat and Vulnerability Engineer

Ft. Belvoir, VA

Responsibilities:

- Threat hunting using Splunk.
- Utilizes Assured Compliance Assessment Solution (ACAS) to perform vulnerability trending for subscriber systems.
- Performs web scans on organizational public-facing websites using Burp to scan for vulnerabilities.
- Assesses and mitigates system security threats/risks throughout the program life cycle.
- Validates system security requirements definition and analysis.
- Establishes system security designs.
- Implements security designs in hardware, software, data, and procedures.
- Verifies security requirements.
- Performs system validation of certification and accreditation activity and supports secure systems operations and maintenance.
- Apprises the Subscriber of audit findings and suggests mitigation actions.
- Reports results to the Independent Verification & Validation team for further analysis and remediation coordination.
- Stays abreast of new technology and their potential for application in the organizational security stack.
- Briefing key stakeholders.

Requirements:

- Ability to obtain and maintain an Active DoD Secret Clearance (minimum)
- 8570 IAT Level II and CNDSP Auditor Certification
  (Sec+CE and CEH **or** Sec+CE andGSNA **or** CISA)
- 5+ years of relevant experience (information assurance and cyber security operations)
- BS in Computer Science, Engineering, or other related discipline from an accredited college or university is desired
- Familiarity with:

- Assured Compliance Assessment Solution (ACAS)
- STIGs and hardening guidance
- HBSS and malware systems
- External assessments (Red Team/Blue Team processes)
- Network security stacks
- INFOCON/CPCON
- EMASS
- EMRS
- Burp, Web Inspect, w3af, nikto
- Kali Linux

Send Resume to careers@intellectualpoint.com