1934 Old Gallows Road, Suite 350
Tysons, VA 22182
703.226.8018
zentekconsulting.com

Position Title: HIPS Signature Writer

Start Date: July 1, 2017 (Tentative - based on anticipated award)

Clearance Requirements: Active DOD Top Secret with SCI or SCI Eligibility

Location: Fort Meade, MD

Travel: Minimal

Job Description:

- Develop custom Intrusion Prevention System (IPS) signatures/content that encompass existing and/or newly created signatures/content based on threat findings
- Develop and prioritize requirements of countermeasures derived from findings, (e.g. existing Host Intrusion Prevention (HIPS) policies, signatures and content from the DoD Enterprise)
- Transform existing general and customized IPS content in accordance with the changing threat landscape (severity, prioritization) to meet existing and future security requirements based on policy guidance from government cybersecurity entities
- Integrate newly created IPS signatures/content and transform custom developed IPS content into core IPS content packages
- Develop custom IPS content into a high quality data stream for consumption/distribution to both Windows and non-Windows supported IPS platforms
- Participate in piloting/testing efforts
- Prepare reports and presentations as required

Skills:

- Must be capable of providing customer-centric IPS content, policy creation, distribution mechanisms and implementation guidance
- Ability to develop and write custom IPS signature content specific to the DoD in collaboration with malware analysts for coverage of emerging threats
- Must be able to interpret security vulnerability protection requirements and translate them into IPS signatures
- Mastery of vulnerability, threat mitigation and existing threat tactics
- Ability to troubleshoot IPS signatures
- Familiarity with, and adherence to, quality assurance and development standards
- Experience supporting QA testing of custom signatures and subsequent content streams for HIPS/NIPS

- Experience supporting piloting and testing efforts to achieve high quality IPS signature content with a focus on reducing false positive alerts and ensuring cross-platform compatibility
- Intel/McAfee Host Based Intrusion System (HIPS)/Network Intrusion Prevention system (NIPS) development expertise a plus
- Experience preparing reports and presentations to include:
    - Architecture Diagrams (depicting both logical and physical views)
    - HIPS Custom Content Development (HCCD) Implementation and Signature Guides
    - Systems Engineering Reports
    - Monthly Content Packages
    - Concept of Operations (CONOPS)
- Proficient with Microsoft Office suite of products
- Excellent presentation, written, and verbal communication skills