



## POSITION DESCRIPTION

Title: Network Security Engineer  
Location: Washington, DC  
Schedule: Full Time  
Travel: Based on customer requirements, must be willing to travel  
Clearance Level: **Active Moderate Risk Public Trust REQUIRED**

We currently have an opening on our team for an experienced Network Security Engineer to support our Government client at their offices in downtown Washington, DC.

### Experience in the Following:

- Performing complex project tasks involving integration of electronic processes or methodologies to resolve total system problems or technology problems. Apply analytical and systematic approaches in the resolution of problems of work flow, organization, and planning.
- Detailed understanding of TCP/IP.
- Working knowledge of NIST 800-53 security controls and understanding of NIST 800-37.
- Working knowledge of IP Routing (OSPF and BGP) and multi-VRF environment.
- Working knowledge of IDS/IPS implementation and operation.
- Working knowledge of Forward and Reverse Proxy implementation and operation.
- Firewall implementation and design.
- CCNA R/S or Security, CISSP, associate level, or higher, security certification.
- Experience with Tenable, Varonis, SkyBox, Linux

### Minimum Qualifications:

- Bachelor's degree or equivalent professional experience in the field of information security, computer engineering, information systems, telecommunications, or related technical or functional discipline.
- Minimum of eight (8) years of relevant work experience in information/cyber security engineering or operations, including hands-on experience with security tools and devices such as network firewalls, web proxy, intrusion prevention system, vulnerability scanner, and penetration testing tools.
- Two (2) or more years of experience in designing, architecting, and implementing security controls and securing enterprise-wide systems, applications, network, and infrastructure services.
- Strong analytical skills
- Strong familiarity with Federal compliance standards such as NIST 800-53, FIPS, FedRAMP.
- Specialization in one of the following fields with four (4) or more years of experience:
  - Building and administering security devices such as network firewall, web proxy, data loss prevention systems, and intrusion prevention systems.



- Building and administering Network devices (e.g., Cisco, Juniper)
- Conducting dynamic web application security testing, both manual testing and utilizing application security tools to discover exploitable vulnerabilities.
- Conducting database security assessment and monitoring.
- Experience with public cloud services providers such as Amazon AWS or Microsoft Azure.

### **Professional Certifications:**

Maintain at least one current professional certification. Acceptable certifications include: Any SANS GIAC Security certifications (Administration, Software, Forensics, or GSE Expert), ISC2, CISSP, or any security systems vendor administration-level certifications. Other certifications may be acceptable depending on relevance.

### **Benefits:**

Raventek Solutions' competitive benefits program includes comprehensive medical and dental care, matching 401K, paid time off, flexible spending accounts, disability coverage, and other benefits that help provide financial protection for you and your family.

Raventek Solutions provides equal employment opportunities to all employees and applicants without regard to race, color, religion, sex/gender, sexual orientation, national origin, age, disability, marital status, genetic information and/or predisposing genetic characteristics, victim of domestic violence status, veteran status, or other protected class status. This policy applies to all terms and conditions of employment, including, but not limited to, hiring, placement, promotion, termination, layoff, recall, transfer, leave of absence, compensation and training. The Company also prohibits retaliation against any employee who exercises his or her rights under applicable anti-discrimination laws. Notwithstanding the foregoing, the Company does give hiring preference to Seneca or Native individuals. Veterans with expertise in these areas are highly encouraged to apply.