POSITION DESCRIPTION

Title:	Tenable Security Engineer
Location:	Washington, DC
Schedule:	Full Time
Travel:	None
Clearance Level:	**Active Public Trust (Desired but not Required)**

We are seeking a Tenable Security Engineer to join our team of engineers supporting our government client in Washington, DC. You will be providing on-site expert technical support on cyber/systems security projects.

Duties and Responsibilities:

- Implement Tenable SecurityCenter and Nessus scanner.
- Develop Nessus compliance audit files and associated conversion from DISA STIG or CIS.
- Maintain, update, patch, and enhance Tenable SecurityCenter system to ensure optimal operational state.
- Perform data clean up and configuration of scan jobs, asset groups, dashboards, data repositories, and reports.
- Run ad-hoc scans, queries, and reports.
- Identify and fix problems with scans (such as incorrect credentials, firewall blocks and failed scans).
- Validate and maintain asset lists for scans.
- Develop custom reports.
- Develop new or updated compliance audit files.
- Compile scan data for IT priority remediation and executive status presentations.
- Manage scans from Tenable.io.
- Define, plan, design, and evaluate information security systems and architecture
- Installing and updating security systems with latest vendor updates
- Coordinate the provision of any required regular reporting on security metrics.
- Develop and implement information systems security policy

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 the area of 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 familiarity with Federal compliance standards such as NIST 800-53, FIPS, FedRAMP.
- Specialization in at least 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 Windows Server and Active Directory.
- Building and administering Linux/UNIX based 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.
- Operating System Firewall configuration on Windows and Linux Systems.
- Secure system to system communication including but not limited to RDP, WinRM, SSH.
- System level security protocols such as IPSec, PKI, SSL.
- Excellent written and verbal communication skills.
- Proficiency with Microsoft Office products: Word, Excel, and PowerPoint, Visio.
- Timely and precise organizational skills.
- Critical and creative thinking and analytical skills.
- Ability to multi-task in a high volume, fast-pace work environment.
- Ability to perform effectively in a flexible, team-oriented environment.
- Ability to build and maintain strong working relationships with colleagues.

Benefits:

Seneca Nation Group offers competitive compensation and a strong benefits package including comprehensive medical and dental care, matching 401K, paid time off, flexible spending accounts, commuter benefits, disability coverage, and other benefits that help provide financial protection for you and your family.

Seneca Nation Group 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.