Cyber Vulnerability Scanner Analyst

FITS is currently seeking a Vulnerability Scanning Specialist to be part of our Vulnerability Team. The selected candidate will perform with various tools in support of the client's Continuous Monitoring effort. If selected, you will perform vulnerability and compliance scans of OS, database, and applications using industry standard tools. You must also have an understanding and experience with common cybersecurity toolsets and processes to include STIGS, ACAS, IAVA Management and Implementation.

Job Description

- Document DISA STIGs applicable to each network environment for all Assured Compliance Assessment Solution (ACAS) implementations.
- Assess current ACAS implementations for each of the networks and recommend changes.
- Document the steps required to design the ACAS solution for each of the networks to include IP address, Fully Qualified Domain Name, and physical location of each component.
- Create reporting dashboard designs and reports for each environment that are specific to the following audiences: Leadership & Executives; Cybersecurity Staff; and System Administrators.
- Ensure networks receive periodic updates from either the DISA/DoD Patch Repository or Tenable.
- Implement the Reporting Dashboard designs and use reporting tool to create reports.
- Ensure scheduled scans are covering 100% of intended assets and are being run successfully.
- Maintain the Nessus scanners and PVS's connectivity with the associated Security Center (SC).

Required Qualifications

- Active DoD Secret Security Clearance
- CompTIA Security + certification
- 1-3 years' hands-on ACAS and/or Nessus experience

Additional Qualifications

- Must be self-motivated and be able to work both in a team environment and independently.
- Demonstrates knowledge of networking concepts, devices (Firewalls, Routers, Switches, and Load Balancers), ports, protocols, and services.
- Has working experience with various Operating System Platforms (Windows, UNIX, and end-user) as applied to an enterprise environment.
- Must be able to research and recommend resolutions to technical issues.
- Has experience in configuration, customization, operation and troubleshooting Operating System, Database, and Application-Level vulnerability scanning tools.
- Has experience analyzing scan results to determine if scans were successfully completed.
- Demonstrates an understanding of network and web related protocols (such as, TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols).