Security Analyst/Engineer

Who we are
InfoStructures, Inc. is an information technology services firm located in Rockville, MD. Since 1988 we have been employing leading-edge technologies and techniques to improve the working lives of others. We are seeking an energetic, highly motivated, qualified Security Analyst/Engineer with the right attitude toward customer service. We place great value in the work our people do and in the difference their efforts make in people's lives.

What makes us different than other IT services companies? It's simple: the quality of our services and our attention to detail.

What experience you need:
Experience providing security services for different clients in different industry sectors. You should have:

- Managed security monitoring
- Performing security event and incident correlation using information gathered from a variety of sources within the enterprise
- Tracking and documenting cyber incidents from initial detection through final resolution
- Provide detection, identification, and reporting of possible cyber-attacks/intrusions, anomalous activities, and misuse activities.
- Perform and document audit procedures, conclusions and findings in accordance with best-practice, industry and InfoStructures standards
- Penetration testing and vulnerability assessments
- Compliance specific monitoring including HIPAA, FDIC, etc.

Additional job requirements:
- Superior problem-resolution skills
- Understanding and past experience working in an IT consulting environment supporting a wide range of clients, vertical markets (healthcare, finance, non-profit) with different levels of technology.
- Ability to work in a fast paced environment support multiple customers at once
- Excellent oral and written communication skills, including an ability to deal with people at various levels, from technician to executive
- Self-starter and highly motivated

- Strong track record in leading a technical team and in building client relationships.
- Ability to weigh options and provide the most efficient and cost-effective solution from a number of options.
- Experience providing consulting to clients, with the right balance of initiative and following instructions
- References that demonstrate these characteristics
- Ability to understand and categorize technical problems
- Remote and on-site problem-resolution skills
- Strong ability to build client and peer relationships

Working knowledge of installing, configuring, and troubleshooting products in the following areas:

- Splunk (Preferred) or other security analysis tools that also include SIEM knowledge
- Anti-Virus, various anti-spyware utilities (including McAfee ePO, Symantec, Avast/AVG)
- 2-Factor Authentication (2FA/MFA) implementations and support
- Windows (Servers and desktops) and 3rd party patching project, processes and methodologies
- Microsoft Windows 2008/2012/2016 Server with a high-level understanding of Active Directory design and implementation with regards to security requirements related to ensuring Windows servers are protected
- MS Office 2010/2013/2016/2019
- Outlook 2010/2013/2016/2019 including basic email troubleshooting

What education/training/certification desired/requested:
SPLUNK (HIGHLY PREFERRED)
CompTIA Security+
CEH
CISSP or other high-level security certifications
MCITP
Bachelor's degree

What you will do
You will provide on-site and remote network integration and support services to our government and commercial clients, mostly in Windows 2008/2012/2016/2019 and VMware v6 environments. You are expected to:

- On-Site evaluations + potential user interviews on potential security concerns based on way users are utilizing and working with IT
- Examine network architecture for any changes and ensure no backdoors are open for people to exploit network
- Discovery and recommendations on security controls in place, including but not limited to:

    - Email security, Encryption, data protection and DLP
    - AD policy, password management, and AD/File Audit reviews
    - NAS/SAN/storage security
    - Wireless security
    - Firewall/Internet edge security
- Recommendations and changes to existing IT security processes and procedures, including but not limited to:
    - Acceptable Use Policies
    - DR/COOP plans
- Bi-annual high-level overview of security measures put in place along with measures to prevent security vulnerabilities.
- Daily monitoring and alerting for SIEM “Splunk” solution which will be set up to ingest logs from all network devices (firewalls, switches, etc.), servers, desktops, WAF, and others to look for correlating security events.
- Weekly patch monitoring, reporting and assessment including Windows, and 3rd party patches.
- Weekly Anti-Virus configuration checks and quarantine results
- Monthly vulnerability scans of entire environment including a follow-up report and recommendations.
- Manage projects various migrations, new installations, etc.
- Provide team leadership on technical projects and technical guidance to other engineer
- Develop technical reports and documentation
- Complete other duties as assigned-Categorize the customer request
- When possible, solve entry level user technical issues
- Provide timely ongoing communications with client regarding status and resolution
- Complete other duties as assigned

Where you will do it
You will work primarily from our InfoStructures’ headquarters in Rockville, Maryland with site visits to client sites in the Washington, DC metro area (local travel is a must).

Hours are Monday through Friday, 9:00 a.m. to 6:00 p.m. with after-hours work (projects, break/fix) required, but limited as much as possible.

Benefits
InfoStructures provides a comprehensive benefits package that includes paid vacation, personal/sick days, employee health insurance coverage, and a 401(k)/profit sharing plan.

Please forward cover letter, resume and salary history/requirements to personnel@infostructures.com or fax to Personnel at (301) 417-7177. Equal Opportunity Employer.