Senior System Security/Information Assurance SME

- SAIC is currently seeking a motivated, career and customer oriented Senior System Security/Information Assurance SME to join our team in NCR area.

Shift Schedule: Monday-Friday, 8:00 to 5:00 PM core hours. Onsite work due to supporting systems hosted in an air-gapped environment. Flexible with potential 9/80 work schedule.

Position Overview:

- This position is for a Senior System Security/Information Assurance SME supporting our Department of Defense (DOD) contract, working in NCR area.
- The applicant will provide technical support and compliance for the network in a collaborative team environment.
- The candidate should have proven experience with Security and auditing Tools for Windows and Linux operating ACAS and HBSS systems.
- Candidate must have 1-5 years of experience with security products as well as working knowledge of Microsoft Products installing, configuring, and administering Microsoft Server 2012R2, Server 2016 / 2019 and Windows 10 operating systems.
- The applicant should have knowledge of Microsoft's operating systems, Active Directory, DNS, DHCP, and knowledge with other Microsoft Products.

Required:

- This position requires an active DOD Top Secret clearance.
- Possess DoD 8570.01-M/DoD 8140 Certification IAW established mandate prior to start of work - IAT Level II required (CCNA Security, CySA+, GICSP, GSEC, Security+ CE, SSCP); IAT Level III is desirable (CASP+ CE, CCNP Security, CISA, CISSP (or Associate), GCED, GCIH). Applicants not meeting this requirement will not be considered.
- Bachelor's Degree in Computer Science, Information Systems, or other related field or at least five (5) years of equivalent work experience in lieu of degree.
- At least 3-5 year experience working with Security and Auditing tools for Windows and Linux operating system such HBSS and
- ACAS to include: installing, configuring, maintenance, backups, and restore.
- Day-to-day operations and maintenance which include but not limited to; review of audit logs, creating backups of the data
- files, maintaining network documentation and reviewing scans.
- Server/Workstation Security and maintenance updates
- Maintain system configuration documentation
- Design/Maintain/Create system configuration and architecture documentation Design/Maintain/Create system process
- and procedure documentation
- Maintain virus definitions, patch versions and Department of Defense (DoD)
- Security Technical Implementation Guides (STIG) levels on all servers, workstations, and laptops
- Monitor and Maintain Host Based Security System (HBSS)

- Utilize the DoD Assured Compliance Assessment Solution (ACAS) to update, manage and track implementation of information security requirements for the IT assets and resources
- Provide technical support and implementation for security tools and upgrades
- Provide installation support for network systems applications
- Support DoD Information Assurance Risk Management Framework (DIARMF)
- Ensure all HBSS products are at the latest version
- Ensure the Security Center Linux server is at the latest DISA-approved version of Security Center, as well as having the latest patches installed
- Ensure the Nessus Scanner is at the latest DISA-approved version of Nessus
- Monitor Rogue System Detection within McAfee ePO and report all rogue systems appropriately
- Monitor Data Loss Prevention within McAfee ePO and report all DLP incidents appropriately
- Perform export of Microsoft updates from WSUS (Windows Server Update Services) server on JSP Network and import to WSUS server residing on the PRUN (Pentagon Reservation Utility Network).

Desired:

- Active DoD 8140 IAT Level III certification