Windows Certificate Authority (CA) SME

Team SAIC is currently seeking an experienced Windows CA SME to provide platform services, security leadership, and direction in the support and sustainment of PKI systems within a large complex physical and virtual server architecture supporting enterprise applications, solutions, and services. This position requires demonstrated direct experience with CA/PKI management and administration within a Platform Systems Services (PSS) hosting environment.

Shift Schedule: Monday-Friday, 8:00 to 5:00 PM core hours with occasional after hours' onsite work to support both a NIPR and SIPR environment.

Position Overview:

- Performs system administration on 2012, 2016, 2019 Windows Server systems performing management, troubleshooting, and platform integration
- Online Certificate Status Protocol (OCSP) technologies, including PKI of Microsoft Active Directory; and Smartcard middleware technologies.
- CA knowledge, Tumbleweed, Axway and comparable technologies
- Active Directory, Active Client, Online Certificate Status Protocol (OCSP), and Certificate Authority (CA) and Smart Card (CAC) enablement.
- CAC and CAC enabled Active Directory domains.
- Microsoft Certification Authorities and hardware security modules.
- Working within a VMware (i.e. utilizing vCenter to access VMs)
- Assisting Windows systems / platforms with STIG'ing efforts
- Identification of technical trends in information technology, awareness on-going IT projects, and business unit requirements.
- Ensuring developed systems comply with the enterprise technical architecture.
- Mobilize certificate based security efforts and work across multiple teams of engineers within the program to implement security vision of maintaining and sustaining systems through security tools, processes, reporting, and verification.
- Provide reporting and briefing to customer leadership of efforts and make recommendations of direction, methods, and strategy across the program.
- Identify, communicate, and make recommendations to leadership on recommendation direction, methods, and suggested direction on achieving and maintaining an effective enterprise security posture.

Required:

- 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 in Science degree in Computer Engineering, computer information systems, telecommunications, or management information systems, or 10 recent years of documented experience relevant to this position.

- Experience administering and managing 2012, 2016, 2019 Windows Server based systems
- Experience administering and supporting AD, DC, DHCP, DNS and other Windows based / platform supporting structures
- Deep skills administering and maintaining Windows and Windows certificate based systems locally and distributed across remote sites for redundancy.
- Exposure to Linux, Oracle, and VMware systems and architectures; familiarity with imaging, such as 1909, etc.
- Exposure with ACAS, Tanium, Splunk, and other types of enterprise vulnerability reporting tools.
- Understanding of Online Certificate Status Protocol (OCSP) technologies, including PKE of Microsoft Active Directory; and Smartcard middleware technologies.
- Experience with Active Directory, ActivClient, 90meter, Hardware Security Module (HSM), Online Certificate Status Protocol (OCSP), and Certificate Authority and smart card enablement.
- Experience with DoD/CNSS PKI, Microsoft ADCS (in-depth and multi template and multi domain), Hardware Security Modules, 802.1x (wired and WiFi).
- Exposure to patching solutions and working with teams performing and maintaining enterprise patching solutions.
- Knowledge and exposure to network protocols and Windows based networking environment.
- Exposure and / or work related experience to include the following computer related areas: Networks, Servers, Storage Area Networks, and systems management; domain controllers, AD, directory systems; Public Key Infrastructure; computer server and workstation security, virtual environment exposure.
- Experience with and solid working knowledge of an enterprise ticketing system (REMEDY).
- Demonstrated ability for oral and written communication with the highest levels of management.

Desired:

- Windows Certifications
- Experience working in Platform as a Service environments
- Experience working with large enterprise systems with 40,000+ endpoints