

SENIOR NETWORK SECURITY ENGINEER

CTEX delivers an agile, business need driven and wide global computing platform that is efficient, effective, scalable, flexible, and reliable through technology modernization, standardization and, ITIL guided service management practices.

Prominent IT organizations around the world have selected CTEX to improve their service levels, reduce capital expense and deal with the high costs of bandwidth, energy, real estate, staff and expertise. As a pioneer in utility computing, CTEX understands and harnesses the latest advances in technology such as virtualization, cloud computing and support process automation.

In a continuously evolving industry, we are looking for highly skilled professionals that are passionate about excellence, results-oriented, and have a long-term commitment to the company.

Job Description

SUMMARY

The Senior Network Security Engineer plays a pivotal role in the design and implementation of the security strategy. The Senior Network Security Engineer is responsible for maintaining the security SLA's of our customers. The Senior Network Security Engineer also oversees incident response and communication about potential vulnerabilities to business leaders.

The Senior Network Security Engineer works closely with the VP Operations and must have strong working knowledge of security architecture, solutions, policies and procedures. The services areas in the Data Center include data center operations network, server, storage, database, application server, information security engineering and maintenance, NOC and SOC operations, enterprise system monitoring and service management, application management, and facility management.

RESPONSIBILITIES

- Lead the engineering, implementation, and maintenance of security tools, solutions, processes, and policies to ensure an acceptable level of security and further improvement, including vulnerability management, wireless and wired network Intrusion detection, endpoint protection, host intrusion prevention, firewall, anti-spyware and anti-malware, baseline compliance and monitoring, perimeter protection, security incident and event management.
- Provide security guidance and drive infrastructure decisions in collaboration with other technical and management team, ensuring Security principles are being upheld and no violations of Security Policy is taking place.
- Support security systems deployment, management, and maintenance, including Firewalls, VPNs, and infrastructure monitoring, reporting, and associated sensor systems.
- Provide computer security incident prevention, reporting, and analysis support with a state-of-the-art subject matter expertise regarding information security vulnerabilities and solutions.
- Develop and maintain CSIRT policy, procedures, and protocols. Conduct computer security incident analysis, computer forensics operations, evidence gathering and preservation, incident containment, and incident recovery. Develop and maintain CSIRT reporting guidelines and procedures and perform the following:

SENIOR NETWORK SECURITY ENGINEER

- Compile information from various sources (log analysis, incident reporting, event analysis, etc.) into comprehensive monthly reporting detailing historical and trend information.
- Develop, update, and report performance metrics and status on security compliance.
- Automate reporting processes and data aggregation where appropriate.
- Track and correct any applicable information security deficiencies, conditions, weaknesses, findings, and gaps identified by audits, reviews, security control assessments, and tests, including those identified in FISMA audits, Statement on Standards for Attestation Engagements (SSAE 16) reviews, other applicable reviews and audits, and the continuous monitoring activities such as, but not limited to, vulnerability and compliance scanning of all the IT systems. Design, implement, maintain and improve, where possible, the IT portions of the COOP plan.
- Engage in ongoing research of emerging trends and new technologies which may benefit the project goal of strategically implementing technology to enhance or solve project problems.
- Conduct in-depth technical reviews of new and existing IT systems in order to identify the appropriate mitigation strategies required to bring these systems into compliance with established policy and industry guidelines.

GENERAL QUALIFICATIONS

- Bachelor degree in, Computer Science, Computer Information System, IT management
- 8+ years of experience system architecture design with experience providing security integration
- 6+ years of experience in information security solution engineering
- 3+ years of experience working with virtualization technologies
- Three or more of the following certification: GSEC, GCIA, GCIH, CCNA Security, CISA, CISM, CEH, CCSP, MCSA/MCSE and/or CISSP
- In-depth knowledge on government regulations, requirements, guidelines, and industry standards on Information Security.
- In-depth understanding of Cisco network technologies and standard network protocols.
- Hands on experience with the following security technologies: firewalls, Network Intrusion Detection Systems, Vulnerability Scanners, Virtual Private Networking, virus protection technologies, Log Management, network access control, proxy server and data loss prevention
- Must be highly experienced with security incident and event management solutions and processes. 5+ years of experience in forensic analysis
- Must be experienced with Network Security
- Must be highly experienced with the following operating systems: MS Windows, UNIX, and Linux.

DESIRED SKILLS

- Experience with deploying and administering cloud services and/or collaboration with cloud service providers is highly desired
- Prior security clearance is desired

SENIOR NETWORK SECURITY ENGINEER

INQUIRIES

Submit inquiries via email at careers@ctexpartners.com. For more information, visit our website at www.ctexpartners.com.