



To be considered for positions with SE Solutions candidates must be clearable to a Top Secret level. A current Secret clearance or higher is preferred. US citizenship is required. All positions are full time, exempt, salaried and are eligible for our benefits package which includes medical, dental, vision, and 401k.

[Click here to submit your resume](#)

Cyber Security Senior Consultant

Provides advice and makes recommendations as an authoritative leader in the cyber security, networks, and networks operations arena and provides design, architecture, and engineering technical direction and leadership. Recommends solutions to the most difficult security problems in existing systems and systems development. Applies or assists with the application of formal methods in security architecture, security system design, engineering, and security technology integration and deployment. Leads and participates in security tests and evaluations, studies and experiments. Conducts technical and management briefings. Oversees and directs complex technical tasks. Determines enterprise information assurance and security standards. Develops and implements information assurance/security standards and procedures. Coordinates, develops, and evaluates security programs. Recommends information assurance/security solutions to support customers' requirements. Identifies, reports, and resolves security violations. Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Supports customers at the highest levels in the development and implementation of doctrine and policies. Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures. Performs analysis, design, and development of security features for system architectures. Analyzes and defines security requirements for computer systems which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solution. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle. Ensures that all information systems are functional and secure.

Qualifications: Must have experience in architecting a campus-level cyber-security architecture. Certified Enterprise Architect preferred. Must have experience with either FEA or DODAF and with NIST & DIACAP standards and processes.

Security Analyst

Performs much of the basic watch functions of the Security Operations Center (SOC). Uses resources such as ArcSight; Foundstone; data feeds of alerts and logs from firewalls, routers, and other network devices or hosts; data feeds and/or alerts from ISS, SourceFire, and other host and network-based IDS/IPS to watch for security violations and determine vulnerabilities. Provides real-time security monitoring and incident reporting of IT security issues on the customer's network and IT infrastructure. Logs all activities performed on his/her shift in the SOC shift reporting system. Perform real-time scans of hosts and network devices on the customer's network in response to the monitoring of threats or in response to CVEs listed by such sources as SANS, Microsoft, Center for Internet Security (CIS), etc., at the direction of the SOC Senior Security/Incident Response Engineer or Security PM. Escalates possible security incidents and vulnerabilities to the Security PM or Senior Security/Incident Response Engineer on duty. Makes recommendations for tuning of IDS/IPS and other security devices to the Security Program Manager and/or Senior Security/Incident Response Engineer for submission into the SOC Change Control Process (CCB). Helps maintain a log of customer's local site contacts and local dial access numbers. Handles Remedy security incident tickets in conjunction with and under the direction of senior SOC staff. Answers SOC incoming phone calls.

Qualifications: One year or more of previous experience in security event/alert monitoring employed in a SOC, CSIRT, or on a Security Response Team. Knowledge of Host/network CVEs, hacker methodologies and tactics, and the tools used; TCP/IP protocol suite, TCP/IP headers and packets, the OSI model, and commonly used TCP/UDP ports and associated services. Skill in the use of tools such as Trace Route, Visual Route, Ethereal, Nessus, and other commonly used security tools; monitoring and the analysis of firewall logs (PIX/ASA, Sidewinder), router syslogs (Cisco), and network/host-based IDS/IPS; basic network engineering and LAN/WAN technologies and topologies; ticketing systems such as Peregrine, Remedy, etc.; preferably IT security/IA training through such sources as SANS, etc. Should have basic security monitoring skills and at least a basic understanding of network/host vulnerabilities and exploits. Should also have knowledge of using such utilities as Ping, Trace Route, NSLookup, and ARIN WHOIS lookup. May have more advanced security monitoring skills and a more advanced understanding of network/host vulnerabilities and exploits, hacker methodology, host/network device hardening techniques, and security incident prevention/mitigation techniques.

Senior Network Engineer

Provides engineering and building solutions for deployments of new facilities and upgrades of existing facilities. Will engineer Local Area Network (LAN) and Wide Area Network (WAN) connectivity to DHS systems with Government organizations and designated DHS business partners as requested by DHS S&T. Conducts technology refreshment projects in accordance with DHS guidance and recommends new products and technology for supporting all layers of the IT infrastructure architecture. Network engineering projects may include tasks such as the following: Network design and planning, network configuration and implementation, network enhancements based on recommended best practices and technical assessments, documentation of network deployments and upgrades, integrating policy enforcement points (PEPS), system engineering projects may include tasks such as the following:

- Active directory services
- Anti-virus and Security Patching
- Backup and archive technologies
- Blackberry and wireless technologies
- Client platform designs including software images and hardware configurations
- E-mail and messaging services
- Federal Desktop Core Configuration
- File share services
- Management, configuration and utility servers
- Metadata collection points
- Microsoft Network services configuration and planning (DNS, DHCP, WINS)
- Network and server enhancements based on recommended best practices and technical assessments
- VMWare server consolidation and virtualization

Storage Engineering projects may include tasks such as the following:

- Work closely with Application and Infrastructure Architects in the creation of S&T Net Field site storage solutions
- Develop and maintain storage architectural strategy and roadmaps for a tiered storage model, consistent with enterprise objectives
- Develop and maintain the Reference Architecture/Blueprints for the storage environment, including: Storage, Arrays, SAN Switches, Tape Libraries, SAN design, Virtualization strategy, Backup & Replication solutions, and tools to manage performance, availability and capacity.
- Provide input and recommendations into broader infrastructure strategy including:
 - End to End Monitoring
 - Security Hardening & Access Control
 - Availability & Stability
 - Architecture, Disaster Recovery and Operational Governance.
 - Establishing policies, procedures & guidelines for storage/backup environment

Other Duties and Responsibilities of the position may include:

- Interface with Engineer teams to ensure Lines of Business objectives are met
- Analysis, design, provisioning, monitoring, validation, and Network/System/Storage recovery tasks
- Create and publish reports detailing utilization and status of Network/System/Storage environment
- Develop and maintain departmental processes and best practices for Network/System/Storage Infrastructure and environment
- Travel to Field sites to support contract activities

Qualifications: Qualifications: Candidates have a BA/BS degree with 10yrs work exp, must be strong with layer 2 switching, specifically with the Cisco Catalyst platform. Firm understanding of layer 3 technologies (i.e. IP Routing, OSPF, BGP, HSRP, GRE). Proficient with Cisco IOS. Familiarity with the multilayer design model (Core, Distribution, Access). Knowledgeable on industry best practices. Experience with Cisco PIX firewall is desirable, but not required

ADEX Architect Support

The DHS Email and Directory Services project requires technical support from Systems Architects. This position will be responsible for providing consultative support to the project management team on all technical issues relating to the Email and Directory Services activities within the department. The position will be responsible for analyzing system requirements and contributing to the design of technical solutions that meet the requirements. The position will be responsible for creating technical documentation in support of the project and in accordance with the DHS Systems Development Life Cycle (SDLC). The position will be responsible for writing white papers and briefings on an as-needed basis. The position will be responsible for making decisions regarding system capacity, security, configuration, and operation, and will be required to document these decisions for technical and non-technical audiences. The position will be responsible for representing the project team in meetings, and for communicating project activities to management, and to other infrastructure teams within the department. The position will be required to analyze activities of other infrastructure teams to determine their impact on the Email and Directory Services project, and for coordinating with other infrastructure teams to ensure integration and interoperability of the Email and Directory Services systems with other infrastructure components.

Qualifications: Strong skills with Microsoft technologies including: Windows 2003, Windows 2000, Windows XP, Exchange 2003, Exchange 2000, Exchange 5.5, DNS, WINS, and DHCP, Microsoft Identity Integration Server (MIIS), , Active Directory, Server Clustering, Group Policy Objects. Strong writing skills and ability to produce technical documents and drawings such as design documents, requirements documents, system build documents, system architecture documents. A basic understanding of network infrastructure components is also required to include: routers, switches, and firewalls. Other qualifications include: strong knowledge of TCP/IP, strong technical understanding of Enterprise environments, ability to analyze impact of technology insertions into Enterprise infrastructure, and the ability to communicate successfully with technical and non-technical staff.

Network Engineer

As a member of the Department of Homeland Security's (DHS) Office of the Chief Information Officer, you will be responsible for the design and implementation of the DHS HQ network. Duties include campus infrastructure design for current and new DHS HQ locations. Provide solutions as new requirements emerge. Present new technologies and recommendations to improve current infrastructure. This position offers the opportunity to directly influence the design of the DHS Headquarters network. Personnel will be interfacing directly with deputies of the CIO.

Qualifications: Candidates must be strong with layer 2 switching, specifically with the Cisco Catalyst platform. Firm understanding of layer 3 technologies (i.e. IP Routing, OSPF, BGP, HSRP, GRE). Proficient with Cisco IOS. Familiarity with the multilayer design model (Core, Distribution, Access). Knowledgeable on industry best practices. Experience with Cisco PIX firewall is desirable, but not required.

Senior Consultant

Develops detailed requirements for integrated financial systems. Provides technical assistance and consulting in the areas of business finance budgeting, and project management. Assists in the identification, evaluation, and recommendation of system solutions. Prepares supporting analysis. Implements project management best practices. Provides project status and schedules. Coordinates activities of Integrated Project Teams and work teams, as assigned. Provides support for System Engineering Life Cycle Processes per Department of Homeland Security and FEMA directives. Provides support planning, implementing, and assessing performance of existing financial systems. Assists with any business process reengineering; and performs duties as assigned by the Federal PMO Lead.

Qualifications: BA/BS degree or equivalent experience with 8 years experience in a related field. Project Management Professional Certification. General knowledge of Federal financial policies, procedures, and regulations, financial management practices and reporting. Working knowledge of project management practices. Intermediate level skills in MS Office, MS Project, MS SharePoint, and MS Visio.

SE Solutions is an Equal Opportunity and an Affirmative Action Employer. We participate in the [E-Verify Program](#) developed by the Social Security Administration (SSA) and the Department of Homeland Security (DHS). [Click here for more information.](#)