VISION IT
Professionalism, Integrity, Commitment.

Senior Information Assurance Security Network Engineer

Job Duties

- The Information Assurance and Security Network Engineer – Senior supports a highly-skilled team of technical network engineers responsible for providing capability management, technical engineering, integration, and troubleshooting services to NETCOM in accordance with (IAW) operational evaluation, and policy development practices from Ft. Huachuca, AZ
- Responsible for 165 CONUS and OCONUS sites providing predictive analysis for network performance and baseline metrics and troubleshoot identified issues either remotely or on-site
- The Information Assurance and Network Security Engineer will be responsible for analysis and troubleshooting of packet and network data from a security compliance perspective, accreditation packages as a component of the team's toolkit (to include STIGs, system documentation, IAVM compliance, etc.), monthly bandwidth report, team equipment inventory and accountability, and development of daily briefing slides
- Assist in the development, configuration, installation, and maintenance of networked systems including local area networks (LANs) and wide area networks (WANs)
- Perform routine network configuration management functions
- Plan, design, develop, and integrate network systems consistent with existing or planned network infrastructures
- Initiates actions to conduct cyber security engineering research and analysis and provides recommendations for the implementation of security mechanisms
- Initiates actions to apply advanced concepts of cyber engineering and cyber security to development and architecture projects
- Coordinates effort to develop/maintain cyber security documentation, concept papers, and test plans required by client policies and the Risk Management Framework
- Analyzes complex information independently and takes appropriate actions, and reviews and implements recommendations from others
- Maintains extensive knowledge and understanding of DoD and U.S. Army engineering efforts, across multiple engineering disciplines

Required Skills

- The Information Assurance and Security Network Engineer possesses knowledge of, and skill in applying:
    - Network standards, protocols, and procedures
    - Capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware the organization's network architecture and infrastructure local area and wide area networking principles and concepts including bandwidth management
    - Network systems design, development, testing, installation, operations, management, and maintenance concepts and methods the organization's network architecture, topology, and protocols
    - Assist in the development, configuration, installation, and maintenance of networked systems including local area networks (LANs) and wide area networks (WANs)
    - Perform routine network configuration management functions
    - Provide network services that support business requirements

- Plan, design, develop, and integrate network systems consistent with existing or planned network infrastructures
- Possesses a thorough understanding and ability to apply intermediate concepts of cyber engineering and cyber security
- Maintains thorough knowledge and understanding of DoD and U.S. Army cyber security policies and Risk Management Framework, NIST SP 800-53a
- Experience with eMASS or like tool to input system findings and artifacts
- Initiates actions to conduct cyber security engineering research and analysis and provides recommendations for the implementation of security mechanisms
- Initiates actions to apply advanced concepts of cyber engineering and cyber security to development and architecture projects
- Coordinates effort to develop/maintain cyber security documentation, concept papers, and test plans required by client policies and the Risk Management Framework
- Analyzes complex information independently and takes appropriate actions, and reviews and implements recommendations from others
- Maintains extensive knowledge and understanding of DoD and U.S. Army engineering efforts, across multiple engineering disciplines
- Prioritizes competing requirements and tasks, and manages long term and short-term obligations
- Initiates actions to evaluate functional operation and performance in light of data collection, baseline metrics and makes recommendations
- Assists in conducting technical assessments of security and surveillance equipment
- Effectively provide engineering guidance to the engineering team

- Working experience and knowledge in troubleshooting use one or more packet analysis applications: Wireshark, Fluke OptiView XG, NetScout nGenius Performance Manager, NetScout Unified Management Console, NetScout InfiniStream, Riverbed Packet Analyzer
- Working experience and knowledge in troubleshooting use one or more network and application performance management:, NetScout nGenius Performance Manager, NetScout Unified Management Console, Riverbed AppResponse Xpert, Riverbed Cascade Express
- Working experience and knowledge in one or more of the following technologies: RedHat Enterprise Linux 5.x and 6.x, MS Windows 7, 8, and 10, MS Windows Server 2008R2, 2012, and 2012R2, Cisco iOS, Juniper OS
- Working experience and knowledge in virtualization
- Working experience and knowledge in networking to include one or more of the following: IPv4/IPv6, VLAN, VRF/VPN, MPLS, routing protocols, QoS, NAC/NAP 802.1x, VoIP, Proxy Services, WAN optimizers, SSL accelerators, EoIP, wireless, VTC, remote access, performance and protocol analyzer, load balancer, IPSec
- Experience with one or more Army Enterprise Tools: MS Active Directory, MS Exchange, MS Center Operations Manager (SCOM), MS Center Configuration Manager (SCCM), MS Windows Server Update Services (WSUS), McAfee Host Base Security System (HBSS), Assured Compliance Assessment Solution (ACAS) and Tenable Security Center and Nessus, CA-Spectrum, NetScout, Arcsight

Education/Certifications:

- BS in Computer Science, Information Assurance, Information Systems, or other related scientific or technical discipline
- Maintain DoD 8570.01-M baseline certifications – IAT-II / IAT-III levels

- TOP SECRET/SSBI with current SCI-eligibility

Travel Requirements:

- Estimated travel requirement is 25%
- A passport and being medically capable of travelling OCONUS is required

Desired Skills

- DoD Experience – Army NOSC or DISA Experience Preferred
- Certified Information System Security Professional (CISSP) or CompTIA Advanced Security Practitioner (CASP) preferred