Network Security Engineer Job Description

Duties and Responsibilities:

- Project, configure, implement, and maintain all security platforms and any other related software, such as anti-virus, routers, Anti-SPAM, switches, intrusion detection or intrusion prevention, firewalls, cryptography systems, SIEM, and MDM
- Plan and appraise ongoing assessment of antivirus, application control, firewall, SIEM, VPN, SSL, intrusion detection or intrusion prevention and other network component policies
- Guarantee network security best practices are executed through auditing: router, change control, switch, firewall configurations, and monitoring
- Responsible for periodic vulnerability testing, and lead remediation projects
- Articulate systems and methodologies as well as reply to security-related events and support in remediation efforts
- Coordinate and oversee log analysis for company managed services offerings to ensure customer policy and security requirements are met
- Maintain network security devices to enable pro-active defense of networks within a managed service SOC environment, providing protective monitoring to multiple commercial customers
- Work under the direction of the Team Leader to maintain security devices and show practical experience in managing SIEM environments, firewalls, content filters, NIDS, proxy servers, HIPS, and packet capture devices
- Work with customers to form and fix appropriate policy and signature rules. This comprises tuning and development of the creation of custom intrusion detection and SIEM signatures and rules, including the efficient on-boarding and understanding of varying customer log sources into SIEM environments

- Work in collaboration with appropriate stakeholders to ensure customers have devices that are fully operational and secure
- Act under authorization from engineering to maintain the configuration and have a comprehensive understanding and technical know-how in server administration, including GPO deployment, patching, and network device configuration, and hardware management (including cable management)
- Work under strict change control processes to ensure only authorized changes are made to devices
- Collaborate with sales, product management, engineering, and other departments on security-related items and any other duties as assigned by the firm.

Network Security Engineer Requirements – Skills, Knowledge, and Abilities

- Extensive technical know-how of security network devices (switches, antivirus, firewalls, cryptography, SIEM) and any other security networking hardware or software tools
- Minimum, two years of experience identifying threats and developing appropriate protection measures
- Knowledge of Cisco ASA Firewall and strong routing & switching experience is an added advantage
- Reviewing system changes for security implications and recommending improvements
- Excellent hands-on experience and knowledge implementing, configuring, integrating and supporting the network security with Checkpoint, F5 Load balancers, BigIP LTM, GTM, IPAM, Cisco ISE, Palo Alto, Juniper, BlueCoast security solutions, or Fortinet. (Not all are needed but the more you have, the more advantages you accrue in securing a job)
- CISCO, CCNP, CCNA, CCIE, CCSA, FCNSP, CISSP, SSCP, CEH, GIAC, Security +, OSCP, CompTIA Server+, MCSE, LPIC, CompTIA Cloud+, VCP, or CCSE qualified

- Knowledge of networking concepts such as WAN connectivity, transport types and protocols, and experience with wireless technology and Wireless deployment for a user base over 500 users per site
- Cisco orientated IOS understanding, working with Routers and Switch Platforms and Experience working with stakeholders at an Operational Level
- Good team player, Self-confident, motivated, and independent
- Excellent communication skills
- Bachelor's degree or equivalent in information systems or Computer engineering/science
- Ability to remain calm while multi-tasking and working under pressure in a fast-paced environment
- Attention to details and good problem-solving skills.