



## **IT Level 2 Network System Engineer**

**Onsite – Full time**

**Salary \$75k-90k, plus car and cell phone allowance**

### **Description:**

As the Level 2 Network Engineer you will perform network services from network design through implementation, maintenance, and upgrading of existing networks. You will be responsible for both managed service and project-based engineering activities and providing managed service support to customers at desktop and enterprise level. This role requires high-level technical skills, and expert knowledge of networking and associated technologies. The goal is to create value for clients that will help preserve the company's reputation and business.

### **Responsibilities:**

- Reviews existing system design and architecture and makes network, cloud, and security-related recommendations.
- Designs, deploys, and maintains company LANs, WANs including routers, switches, firewalls, VPN concentrators, wireless, or related equipment to optimize performance.
- Evaluate local area network (LAN) or wide area network (WAN) performance data to ensure sufficient availability or speed, to identify network problems, to minimize system security vulnerability, or for disaster recovery and eDiscovery purposes.
- Define parameters for testing of all systems: routers, switches, or related networking equipment.
- Performs vulnerability scans of networks, applications, and endpoints to assess the effectiveness of patch management and application development processes.
- Verify integrity of backups and backup systems and analyze network data to determine network usage, disk space availability, or server function.
- Ensure security and privacy of networks and computer systems, as well as maintaining PCI DSS security standards and encryption.
- Monitors, analyzes, and responds to alerts from network and security tools and services.
- Configure and maintain wireless system and access points.
- Creates and maintains documentation as it relates to network configuration, network mapping, processes, and service records.
- Consult with vendors to maintain security.
- Manage network access, enterprise antivirus and anti-malware; maintain and support end-user device access.
- Purchase, install and provide logistical support of hardware and software to end users to promote their effective use of technology (laptops, handhelds, printers, projectors, etc.)
- Collaborate on strategic initiatives and provide support of databases and ongoing evaluation of the technology plan to improve workflow.
- Plan, create, test, deploy, and maintain images, application packaging, scripting configuration, and final end-user personalization.
- Ensures network connectivity of all servers, workstations, and other network appliances.
- Develops, implements, and maintains policies, procedures, and associated training plans for network administration, usage, and disaster recovery.

- Conducts research on network products, services, protocols, and standards to remain abreast of developments in the networking industry.
- Notifies end users of planned network outages / maintenance, work with providers to understand impact and timeline of provider outages.
- Schedules conversions and cutovers.
- Coordinates with all responsible users and sites to resolve network or system incidents.
- Work with management and sales teams to provide relevant customer feedback to the product/service deployment process.
- Assists in responding to internal and external compliance audits, data requests, penetration tests, and vulnerability assessments.
- Ensuring efficient functioning of data storage and processing functions in accordance with company security policies and best practices in cloud security.
- Performs cybersecurity incident detection, analysis, and response.
- Performs security operations, administers security tools, and analyzes trends, methodologies, and best practices for securing services, platforms, and operating systems at cloud, network, server, and endpoint levels.
- Contributes to the design, development, and testing of hardware, software, and cloud-based systems to ensure they are protected against cyber threats.
- Assists in the development and implementation of information security policies, standards, guidelines, and procedures.
- Monitors and analyzes threat intelligence feeds and industry news and events to keep abreast of current and emerging security trends, vulnerabilities, and threats.
- Participates in change management and incident review as needed.
- Vigilantly protect Securewon and our client's data through our cyber security risk program that adapts to a rapidly changing threat landscape, changes in business strategies, risks and vulnerabilities.
- Acts as escalation point for Helpdesk.
- Provides guidance to junior members of the team.
- Participates in after hours, on-call rotation.

#### Requirements:

- Bachelor's degree in Computer Science or related field of Information Technology or equivalent experience and **8 years' experience** as a Network Engineer.
- CCNA required, CCNP preferred, CCNP Security preferred, CCIE preferred.
- Expert knowledge of Cisco routers, switches, gateways, TCP/IP protocol, LAN/WAN infrastructure and routing, EIGRP and BGP Protocols, VoIP, Video and Voice Compression Protocols (H.323, H.264, etc.), SIP, MPLS and other WAN communication protocols.
- Expert knowledge with Cisco IOS, routers, switches and gateways, wireless controllers, TCP/IP, OSI, EIGRP, BGP, OSPF, STP, VLAN trunking, Video and Voice technologies, LAN/WAN, MPLS, P2P, IPv4 and IPv6, Sub-netting, VLANs, ICMP, DNS, TCP and UDP, NetFlow, VPN.
- Support network protocols such as: BGP, OSPF, EIGRP, HSRP, VLAN, TCP/IP, MPLS, STP, IPv4, subnetting, routing
- Proficiency with Windows, MS Office, MS Visio, SolarWinds, WAN analyzer software and Wireshark.
- Expert knowledge of Firewall and security technologies using VPN, NAC and IDS/IPS, URL Filtering, SSL Offloading.
- Knowledge of telecom circuits such as DS1, T1s and PRIs.

- Technical understanding of storage concepts, protocols, and architectures such as FC SANs, iSCSI, NAS, CIFS, and NFS.
- Technical understanding of network concepts, networking principles, protocols, etc: TCP, UDP, IP addressing, VLANs, Firewalls, Routing, and Switching.
- Technical understanding of VMware vSphere architecture and components.
- Familiarity with Windows Networking and general TCP/IP networking.
- Familiarity with configuring, troubleshooting, and administration of Microsoft Windows, and various versions of Linux server.
- Experience with monitoring platforms, e.g., OpsRamp, ScienceLogic, LogicMonitor, PRTG, or comparable tools a plus. (Training on unfamiliar platforms will be provided)
- Experience configuring / administering a directory server such as Microsoft Active Directory
- Experience working in a managed services provider environment.
- Must possess thorough knowledge of TCP/IP, IOS, multiple routing protocols, and wireless protocols.
- Must have thorough understanding of VoIP and Legacy telephony systems.
- Must have thorough understanding of LWAPP, VPN & perimeter security, Layer 3, and content switching.
- Assist with developing network infrastructure expansion and replacement designs.
- Install, configure, and maintain network infrastructure equipment.
- Operational experience with security systems, intrusion detection systems, firewalls, anti-virus software, log management, authentication systems, content filtering, etc
- Strong interpersonal and organizational skills
- Strong technical skills with computer systems
- Superb attention to detail and a strong process-based approach to search execution.
- Highly detail-oriented, with strong organization and time-management skills; ability to manage multiple priorities in a high-pressure environment while delivering high results.
- Comfortable embracing existing technologies and be willing to learn new technologies when necessary.
- Flexibility to react quickly to changing business needs.
- Ability to work well within a team environment and take constructive criticism, coaching and feedback on a consistent basis.
- Ability to forge and maintain excellent working relationships with all members of the SecureWon Team and its clients.

#### **Other Requirements:**

- Occasionally required to sit; climb or balance; and stoop, kneel, crouch or crawl.
- Must be able to frequently lift and /or move up to 20 pounds and occasionally lift and/or move up to 60 pounds; with some installations requiring multiple personnel and coordination.
- Ability to climb up and down ladders.
- Must have reliable transportation, a valid driver's license, and ability to legally operate a motor vehicle.