

Sr. Network Security Engineer INFORMATION TECHNOLOGY – Walnut Creek, CA

The Network Engineering department located in Walnut Creek, California has an opening for a Sr. Network Security Engineer within its Network Engineering group. Position is highly technical and requires thorough understanding of IT network security infrastructure, a wide range of enterprise infrastructure technologies, system requirements, and business objectives. Engineer ensures that the technical infrastructure will provide optimal manageability and security. The position is a hands-on, customer facing position.

Key Responsibilities include, but are not limited to:

- Deliver network security architecture solutions for business application security and infrastructure technology.
- Technical security consulting.
- Influence and enable all IT and business projects with network security solutions.
- Maintain current knowledge of technical and industry relevance, ability to evaluate changes, and how they might apply to the company's environment.
- Discover and investigate suspect behavior, including IDS/IPS, Proxy, Firewall, and VPN analysis.
- Participate in ongoing network security audits and reviews regarding 3rd Party Business Partner connections and compliances (HIPAA, PCI, SOX, etc...).
- Troubleshoot performance and availability related problems
- Ensure risk free implementation of all security, business, compliancy and technology solutions.
- Key liaison and interface with Information Security and Network Operations.
- Interface with and work within cross functional IT teams to continually improve the company's security posture.
- Establish yearly goals, objectives and function metrics including status and management reporting.
- Influence network security technology, application architecture, and design.
- Perform product selection, proof of concepts, pilots, and implementation of production network security solutions which meet customer and business requirements.
- Implementation of IDS/IPS, Proxy, Firewall and VPN rules as identified by business needs and Information Security technical security requirements (TSR's)

Qualifications: The following are preferred or desired, unless specifically stated:

- 7+ years experience in Information Security and data communications industry.
- Must have strong knowledge and experience with Cisco based network equipment.
- Must have strong knowledge and experience with network based IDS/IPS network monitoring
- Must have strong knowledge and experience with networking security technologies including Proxy, Firewalls (Checkpoint and Cisco), router ACLs, VLANs, and other security and network appliances/devices with an emphasis on data communications.
- Must have a strong knowledge of WAN Technologies (Networking, OSPF, BGP, VPN/IPSec, and other assorted IP protocols), including comprehension and working knowledge of the OSI model.
- Proficient in TCP/IP and the associated ports to the most common applications
- Demonstrated working knowledge and/or proficiencies with networking, protocols, security technologies, risk assessment, intrusion detection/prevention, and analysis.
- Hands on engineering of firewall infrastructures, security policy creation, and implementation
- Able to interface with users and technical staff; team player, strong organizational skills, strong conceptual skills, ability to work in a team environment, and independently when required.
- Ability to recognize customer requirements when dealing with projects, assist customer in achieving their goals, and consistently achieve high customer satisfaction.
- Demonstration of the ability to manage customer expectations is necessary.
- Excellent organizational, project management, interpersonal, time management, presentation, written and oral communication skills.
- The ability to provide detailed documentation is a must. Use of Visio, MS Word, MS Excel, PowerPoint necessary.