Our growing company is searching for experienced candidates for the position of security operations engineer. To join our growing team, please review the list of responsibilities and qualifications.

Responsibilities for security operations engineer

- Build a strong network security model to include firewalls, IDS/IPS, signature analysis, web application firewall, API security, database monitoring
- Identifies and resolves operational problems through final resolution
- Monitor security systems and if a risk is identified, work with the responsible department to take necessary corrective action
- Document security incidents, drawing evidence from event logs, error messages, and user activity to identify future risks from which remedial action can be taken
- Analysing and Remediating CISCO advisories
- Identifying and implementing improvements to security within the infrastructure
- Planning network device firmware upgrades
- Provide subject matter expertise in at least 1 security focused area and deep skills in at least 1 other area for support of other team members
- Assist in proof of concept evaluations of new security devices and services
- Configure, implement, and provide operational management and support of all security devices and services

Qualifications for security operations engineer

- DB queries
- Familiarity with regulatory compliance (HIPAA, PCI, SOX)

- Effectively coordinate activities with their group
- Implement or improve team processes