Example of Network Cyber Security Job Description

Our company is growing rapidly and is looking to fill the role of network cyber security. We appreciate you taking the time to review the list of qualifications and to apply for the position. If you don't fill all of the qualifications, you may still be considered depending on your level of experience.

Responsibilities for network cyber security

- Local travel is required to support remote sites up to 70 miles from main site
- Manage cyber threat analysts researching current and emerging threats, campaign assessment, data collection and analysis
- Escalate new threats to leadership in a timely manner with appropriate information regarding risk, action times, and mitigation recommendations
- Lead EIS's external communication with industry partners and the NH-ISAC for information sharing and analysis
- Collaborate on workflow to feed lessons learned into Cyber Threat Detection and Response teams and IR Intel teams to enhance detection capability
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX and leverage for threat hunting activities within the enterprise environment
- Defining and documenting network security requirements, developing design packages and implementing the required firewall changes
- Participates and supports design reviews
- Analyzing network data-flows to create packet filtering firewall rules supporting application requirements
- Identifying security risks and the compensating controls to mitigate them

Qualifications for network cyber security

- Subject matter expertise in core network security fundamentals and

- Knowledge of the latest network security trends/ tools in the market with a strong aptitude to learn new technologies in a rapidly changing environment
- Experience delivering with private cloud based environments & applications
- Experience working both independently and in a virtual, collaborative environment is essential
- Familiar with techniques for recognizing malware behavior based on alerts and log file data
- Strong understanding of enterprise security management practices including incident response, security operations casework, forensic analysis, intelligence gathering, and malware analysis