Example of Computer Network Defense Job Description

Our company is hiring for a computer network defense. Please review the list of responsibilities and qualifications. While this is our ideal list, we will consider candidates that do not necessarily have all of the qualifications, but have sufficient experience and talent.

Responsibilities for computer network defense

- Utilize BlackStratus LogStorm SIEM, WireShark, McAfee IDS/IPS, and other toolsets to identify, triage, and investigate anomalies
- Maintain and update (signature and system updates) SIEM and IDS/IPS systems
- Create technically detailed reports based on intrusions and events
- Recommend mitigation activities and provide after action reports to remediate vulnerabilities and reduce the chance of further exploitation
- Perform high-level gap analysis with regard to the customer's current solution and the existing JRSS CND tools
- Administers and supports systems and devices in support of Computer Network Defense
- Ensures proper performance of tasks necessary to ensure the correct operation of all Army Computer Network Defense components in Europe
- Administers multiple systems including Firewalls, Intrusion Detection Systems (IDS), and Intrusion Protection Systems
- Is responsible for administering complex Computer Network Defense systems
- Supports Computer Network Defense system component on unclassified NIPRnet, and classified SIPRnet networks

Qualifications for computer network defense

- Proficiency in word processing, spreadsheet, and presentation creation tools, Internet research tool
- Candidate must be extremely technical and have an understanding of core cyber tools to include SIEM, vulnerability assessment, infrastructure (firewall, IPS/IDS, proxy, network capture), host based security, penetration testing/external assessment tools
- Requires Both DoD 8570 IAT-II and CNDSP Specialty Incident Responder Certifications to start work
- Experience with providing expert guidance and direction to government and senior level technicians and managers
- Knowledge of DoDI 8530 compliance standards
- Ability to receive, acknowledge, disseminate, track, report, and update vulnerability management (VM) alerts, vulnerability assessments, red or blue team events, and security incidents