Downloaded from <https://www.velvetjobs.com/job-descriptions/computer-network-defense-analyst>

# Example of Computer Network Defense Analyst Job Description

Our company is hiring for a computer network defense analyst. 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 analyst

* The CNDA is responsible for continuous network security monitoring, intrusion detection, and incident response actions to defend the C2BMC component of the Ballistic Missile Defense Communications Network (BMD COMNET) and C2BMC
* 2 years of work related experience with a Bachelors degree from an accredited college in a related discipline, or 6 years in lieu of a degree
* Must meet DoD 8570 IAT Level II certification requirements (Security + CE, CSA+, GICSP, GSEC, SSCP, CCNA - Security)
* Perform near-real-time network security alerting and problem resolution
* Prioritize remediation efforts using reliable threat intelligence
* Monitor and protect the security of the DCGS from internal and external threats
* Implement the Enterprise Audit Conceptual Framework as defined by Intelligence Community Standard (ICS) 500-27
* Perform all functions of the Computer Network Defense Framework
* Generate a complete list of auditable events for all user activity and then process, format, filter, and share the data
* Provide risk determination recommendations to the Authorizing Official (AO) regarding acceptance or rejection of an Authority to Operate (ATO) or Authority to Test (ATT)

## Qualifications for computer network defense analyst

* Must have TS/SCI clearance and must be willing to obtain and maintain CI Poly
* Must have a good understanding of networks at the packet level and be able to analyze packet captures at the expert level
* Must have experience using CND tools such as Enterprise Security Information and Event Management Systems (SIEM), Intrusion Detection and Prevention Systems (IDS, IPS), Web Content Monitoring Systems (Palo Alto), Firewall and Syslog logs
* Must have experience creating content in Splunk to hunt for malicious activity and ability to assist with implementation of countermeasures or mitigating controls
* Requires Both DOD8570 IAT-II and CNDSP Specialty Incident Responder Certifications to start work on the task order
* Monitor external data sources (e.g., computer network defense vendor sites, Computer Emergence Response Teams, SANS, Security Focus), update the CND threat condition, and determine which security issues may have an impact on the enterprise