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

# Example of Computer Network Defense Analyst Job Description

Our company is growing rapidly and 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

* Maintain all documentation relevant to the emergency security measures and train the subordinates to create an awareness about the same
* May interface with external entities
* Performing computer network defense (CND) incident triage, to include determining urgency, and potential impact
* Identifying the specific vulnerability and making recommendations that enable expeditious remediation, and making recommendations that enable expeditious remediation, perform initial, forensically sound collection of images and inspect to determine mitigation/remediation on enterprise systems
* Performing real-time computer network defense (CND) incident handling (e
* Receiving and analyzing network alerts from various sources within the enterprise and determining possible causes of such alerts, and track and document computer network defense (CND) incidents from initial detection through final resolution
* Employing defense-in-depth principles and practices, collect intrusion artifacts (e.g., source code, malware, and Trojans) and use discovered data to enable mitigation of potential computer network defense (CND) incidents within the enterprise
* Assisting with analysis of actions taken by malicious actors to determine initial infection vectors, establish a timeline of activity and any data loss associated with incidents
* Customer Support Desk operations- Support IA Ops reviews, assessments, exercises, and operations surges
* Anti-virus software support

## Qualifications for computer network defense analyst

* Must have ten (10) years of experience in network defense and/or Incident Response and a Bachelor's degree in Computer Science or other technical field or eight (8) years or more experience with a Masters Degree
* Examine network topologies to understand data flows through networks and provides mechanisms to tip countermeasures
* Develop, document and synchronize the recommendations and the tasking of signature and rule sets across ail sensors , IDS, FW, used by the customer
* Bachelor’s Degree required plus twelve (12) years of related work experience
* Master’s Degree in Computer Science or IT Engineering or related field of study may be substituted for six years of experience
* Knowing how to string together data, what questions to ask, what activities will point to a target that we care about