Downloaded from <https://www.velvetjobs.com/job-descriptions/cyber-intelligence>

# Example of Cyber Intelligence Job Description

Our growing company is looking to fill the role of cyber intelligence. Thank you in advance for taking a look at the list of responsibilities and qualifications. We look forward to reviewing your resume.

## Responsibilities for cyber intelligence

* Conduct malware analysis from collected samples
* Conduct deep-dive intelligence analysis of threat actors and attacks
* Contribute to regular written and verbal briefings and presentations
* Produce and disseminate all-source integrated intelligence analysis to support DODIN and defensive cyberspace operations (DODIN/DCO-internal Defensive Measures) planning, integration, coordination, and execution
* Conduct analysis to identify indications of adversary activity and warn (Indications and Warning) leaders of potential threats, cyber developments, events or conditions that may adversely affect the DODIN
* Evaluate international events, all-source and open-source intelligence, and operational information to assist in the assessment of potential impacts to the DODIN and alert the JFHQ-DODIN Staff and Leadership to potential network exploitation or attacks
* Be in consultation with the senior threat engineers, assist in conducting both technical and contextual analysis of emerging and persistent cyber threats to known or potential vulnerabilities that exist in the enterprise environment
* Develop and disseminates intelligence reports used to provide strategic situational awareness to leadership regarding the cyber threat landscape
* Produce and disseminate periodic reports and briefs regarding financial sector relevant cyber threat landscape trends and events to inform operational and strategic decision makers as required
* Support the enterprise Cyber Threat Intelligence programs

## Qualifications for cyber intelligence

* Research, identify, and present best practices in the defense and mitigation of cyber-related attacks and other crimes
* Provide analysis of cyber based attacks as they pertain to critical infrastructures located within the area of responsibility (AOR) of the NVRIC
* Provide investigative case support to assist in cyber related investigations
* Minimum 10 years of total Information Technology experience, with 5 years Information Assurance experience
* Understanding of Risk Management Framework and supporting NIST Publications including FIPS 199 & 200, SP 800-53, 800-70, 800-37
* Bachelor’s degree or equivalent experience in computer engineering, computer science, or other closely related IT discipline