Cybersecurity is a growing issue. The greater frequency of attacks and their higher sophistication require companies to utilize the services of true subject matter experts readily available to apply best practices for securing business assets. Many are the professional figures sought nowadays to help secure networks, but lately, Cybersecurity Analysts are in high demand.

The role of Cybersecurity Analyst (CSA) is similar to other jobs in the profession, positions like [Information Security Analyst](http://resources.infosecinstitute.com/job-titles/security-analyst/), [Computer Systems Analyst](https://www.onetonline.org/find/match/2/15-1121.00?s=Cybersecurity Analysts), [Malware Analyst](http://resources.infosecinstitute.com/job-titles/malware-analyst/) and [Information Assurance Analyst](http://resources.infosecinstitute.com/job-titles/information-assurance-analyst/), whose duties, in general, also comprise of studying the best ways to safeguard data in systems or files using analysis programs to identify threats, but a CSA “specializes in issues related to vulnerability discovery, exploitation techniques, and reverse-engineering attacks,” says Paul Mehta, a Senior Research Scientist in an interview for Wired magazine; the analyst can take on different roles to ensure appropriate security controls are in place for the protection of computer networks and information.

Manage multiple projects and/or analyst(s) within the areas of the following:

* Vulnerability management which included successfully scanning the LVSC computing environment for secure configurations and vulnerabilities, researching and eliminating false positives, tracking and remediating found issues, and tracking and performing the exception processes
* Network and Operating Systems Security Configuration assessment which performs security configuration reviews including hardening controls, firewall rules review, web/application security configurations
* Cyber governance, risk and verification which performs risk assessments, system security and industrial control system zone security plans including listing controls, gaps in implemented controls and tracking remediation of gaps, and provides input to the risk register
* Cyber policy/standard and standard operating procedure creation, review, distribution, and maintenance

Performs other related duties as assigned.   
  
JOB REQUIREMENTS

* Bachelor’s Degree in relevant field.
* Minimum of 4 years hands-on experience in Cyber Security.
* Ability to communicate clearly and effectively in English, both in spoken and written form.
* CISSP or similar certification would be advantageous.
* Must be able to obtain and maintain required licenses
* Demonstrated management experience in at least 1 area in the following list:
* Cyber Vulnerability Management
* Cyber Governance, Risk and Verification
* Cyber Policy/Standard/Standard Operating Procedures
* Working knowledge of threats and vulnerabilities and their significance to cyber risk, network operations, and end-point security
* Strong interpersonal skills with the ability to communicate effectively with guests and other Team Members of different backgrounds and levels of experience.