Downloaded from <https://www.velvetjobs.com/job-descriptions/senior-security-engineer>

# Example of Senior Security Engineer Job Description

Our innovative and growing company is looking for a senior security engineer. We appreciate you taking the time to review the list of qualifications and to apply for the position. If you don’t fill all of the qualifications, you may still be considered depending on your level of experience.

## Responsibilities for senior security engineer

* Understanding and utilization of basic SQL queries
* Ability to utilize languages such as PowerShell and/or Python would be a plus
* Utilization of SIEM tools (McAfee a plus)
* Incident Response in a team environment in other than a management role
* SPAM/Phishing detection and eradication
* Ability to asses and suggest mitigation for threats in a corporate environment
* Act as an escalation point for alerts generated by a SEIM and other related tools
* Perform systems and network analysis of intrusions to the network, servers, applications, operating systems, firewalls, proxies, and other infrastructure related devices
* Perform in-depth network security analysis and conducting preliminary incident response, event analysis and threat intelligence
* Perform vulnerability scanning of the environment and analyze the results to assess risk to the organization and prioritize remediation efforts

## Qualifications for senior security engineer

* Provide security control analysis using a Security Control Traceability Matrix as required by DNI ICD 503, CNSS, NIST special publications, FISMA, FIPS, OMB, of all managed national security systems during the accreditation process by performing documentation review (system CONOPS, network diagrams, SSP, SAP and policies), interviewing key organizational personnel, and presenting the findings for review and authorization
* Experience with creating and reading packet captures (Wireshark, tcpdump)
* Experience with Regular Expression (RegEx) pattern matching
* Must be able to obtain at least a secret level government clearance
* Extensive experience with both physical and network/host level security
* Must have an understanding of firewalls, switches, and IP routing hardware