Downloaded from <https://www.velvetjobs.com/job-descriptions/junior-security-analyst>

# Example of Junior Security Analyst Job Description

Our growing company is searching for experienced candidates for the position of junior security 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 junior security analyst

* Under close supervision designs and configures security systems, including proxy, remote access, mail gateway, intrusion prevention, wireless networking, data leak prevention, security information and event management and web application firewalls
* Update of training materials
* Escalate issues to developer
* Finance support for Brand Protection and corporate security
* Update of Spend Tracker with analyses
* Travel and Expense tracking and reporting
* Tracking and reporting end to end market brand protection budgets an spend
* Maintain global equipment inventories
* Training Admin
* Review data generated by Foreground’s Automated Threat Intelligence Platform (ATIP) and various client-side Network Security Monitoring (NSM) and Security Event and Information Management (SIEM) tools for signs of malicious or suspicious activity

## Qualifications for junior security analyst

* Ensure zero missed service level agreement conditions
* Analytical skills, critical ability and attention to detail
* High level understanding of business processes
* Leverage internal and external resources to research threats, vulnerabilities, and intelligence on various attackers and attack infrastructure On a rolling basis, use our custom hunting VDI solution to identify root cause, scope, and severity of each incident and compile findings into a finished analytical product
* Recommend tuning and instrumentation improvements to V-SOC clients
* Work with our Threat Intelligence and Digital Forensics and Incident Response (DFIR) Teams to identify threats, develop or recommend countermeasures to our clients, and perform advanced network and host analysis in the event of a compromise