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

# Example of Security Threat Job Description

Our innovative and growing company is searching for experienced candidates for the position of security threat. To join our growing team, please review the list of responsibilities and qualifications.

## Responsibilities for security threat

* Complete written reports in compliance with current reporting procedures and policies
* Active Engagement on the most critical Severity 1 & 0 Cyber Security Incidents
* Compliment 24x7 SIRT in analysis, assisting Incident Response (IR), mitigation recommendations, as required
* Act a subject matter expert during both active incidents and in the planning of future response and mitigation, including but not limited to Mock/Table top exercises, cross team educational sessions, business wide strategy building
* Plan and execute Mock and Table Top Incidents to improve IR readiness
* Define incident response policies and procedures, providing recommendations to improve response capabilities and create framework to support activities at the time of an incident
* Act as the project coordinator for all technology projects related to Information Security
* Work with upstream engineers and security researchers investigating threats to open source software
* Conduct investigations by analyzing and verifying information through various investigative techniques, internal resources, and conversations/interviews with persons of interest
* Utilizing next generation tools and technology to conduct deep behavioral analytics assessments/ investigations with a focus on mitigating information security related insider threats

## Qualifications for security threat

* 5+ years experience with Big Data analytics and other large scale data analytics
* 5+ years hands-on experience with SIEM technologies such as Splunk, QRadar, and/or Log Rhythm
* 5+ years of experience with netflow analysis and/or deep packet inspection technologies
* 5+ years of experience with log aggregation, correlation, and analysis
* 5+ years of experience managing network IDS/IPS solutions
* 5+ years of cyber forensics experience