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

# Example of Security Threat Job Description

Our company is growing rapidly and is hiring for a security threat. If you are looking for an exciting place to work, please take a look at the list of qualifications below.

## Responsibilities for security threat

* Deploy, mature and maintain our future logging tier, security event incident management (SEIM) system and alert, triage and response pipeline
* Lead in the evolution of our protection, detection and mitigation capabilities based on experience, evolving threat environment and findings from cyber security incidents
* Develop and maintain strong relationships with key partners to create our detection and threat disruption program
* Participate in threat hunting efforts
* Proactively investigate potential information security intrusions and breaches in our corporate, production, and service provider environments by analyzing root causes and trends of incidents
* Reproduce findings and tell the forensic story in non-technical terms, preserve the forensic and analysis details sufficient for investigations or other analysts to recreate attack scenarios
* Stay abreast of adversaries, attribution, and attacker motivations utilizing both open source and USG reporting
* Reserach attack patterns, threat reports, potential attackers and their Tactics, Techniques and Procedures (TTPs) and conduct risk/threat analyses
* Use automated tools to perform infrastructure vulnerability assessments, identify and resolve any false positive findings in assessment results
* Manage tracking and remediation of vulnerabilities by leveraging agreed-upon action plans and timelines with responsible technology partners and support teams

## Qualifications for security threat

* LogRhythm, Splunk, RSA (foundation)
* Juniper Networks experience
* Cisco CCNA, CCNA Security, CCNP
* Red Hat Certified Technician, Red Hat Certified Engineer
* ITILF (ITIL Foundation)
* Any experience of working with Frameworks