Downloaded from <https://www.velvetjobs.com/job-descriptions/vulnerability-management-analyst>

# Example of Vulnerability Management Analyst Job Description

Our growing company is looking to fill the role of vulnerability management 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 vulnerability management analyst

* Produce actionable intelligence in the form of reports, notifications, and alerts
* Develop mitigation and countermeasure plans from collected threat intelligence
* Perform analysis of security issues and/or vulnerabilities
* Maintain knowledge of security trends and threats
* Provide subject matter expertise for relevant Cybersecurity technologies
* Develop metrics and capabilities to ensure effective vulnerability management
* Executing the vulnerability lifecycle management strategy across the organization
* Configuring, scheduling and executing vulnerability scans, and delivering scan reports
* Establishing relationships with system owners and business process partners for the purposes of ensuring that identified vulnerabilities are remediated in accordance to established timelines
* Working with cross functional teams and internal users to enforce technical security standards by providing assistance in applying established standards to projects

## Qualifications for vulnerability management analyst

* Executing penetration tests against network, web, and mobile assets
* 1 year of experience in corporate IT environment or equivalent
* Experience supporting operational IT security requirements or equivalent security training/education, preferred
* Experience with vulnerability assessment and administering vulnerability scanning tool, preferred
* Bachelor's Degree in Computer Science, Mathematics, Engineering or similar area of study preferred
* Understanding of cyber security and risk management best practices