Example of Vulnerability Engineer Job Description

Our innovative and growing company is looking to fill the role of vulnerability engineer. Thank you in advance for taking a look at the list of responsibilities and qualifications. We look forward to reviewing your resume.

Responsibilities for vulnerability engineer

- Review automated threat indicators for veracity and relevancy
- Configure and review logs & alerts from automated threat intelligence tools
- Approaches for addressing vulnerabilities include system patching, deployment of specialized controls, code or infrastructure changes, and changes in development processes
- Solid understanding of Android mobile and embedded systems architecture from Boot through application layers
- Solid understanding of iOS mobile and embedded systems architecture from Boot through application layers
- Perform vulnerability assessments of operating systems, applications, databases and network infrastructure components to detect, enumerate and classify major vulnerabilities for performing trend analysis and reporting to Enterprise customers through the use of vulnerability assessment tools and methodologies
- Administer security operations management of operating systems, security applications and network infrastructure components to provide security configurations, controls for user account access, monitoring of services, centralized logging, network connectivity, job scheduling execution and routine maintenance through the use of administrative tools and methodologies
- Perform vulnerability classification based on industry publications, attack vector analysis, and external intelligence
- Conduct auditing of applications, operating systems and networks to provide

physical access to ensure availability, confidentiality and integrity to help the organization meet internal and external regulatory compliance
- Expand security knowledge on technologies and methodologies as it relates to operating systems, firewalls, proxies, access controls, encryption, networking, programming/scripting, auditing, vulnerability assessments, and operations management to assist the team with effective research, data gathering, analysis, metrics reporting and communications

Qualifications for vulnerability engineer

- Basic understanding of malicious code constructs (imports, exports, PE sections)
- Comprehensive knowledge of malicious code (worms, viruses, spyware)
- Advanced experience in automation and scripting of applications and systems systems Python, Perl, JavaScript, Splunk, Archer GRC
- Experience with Windows, UNIX, and Linux servers at the beginner to intermediate level
- Knowledge of basic networking protocols, including TCP/IP, HTTP/HTTPs, FTP, or DNS
- Ability to maintain current knowledge concerning vulnerabilities, Cyber threats, and information security tools