Jr. Vulnerability Scanning Engineer

Job Description

Role Summary
This Vulnerability Scanning Engineer will work to identify technical security vulnerabilities by conducting vulnerability scanning; reporting security vulnerabilities and the risks those vulnerabilities present to external customer's management, and other technical individuals. The selected candidate will maintain their knowledge of common operating systems, cybersecurity trends, as well as changing technologies. The candidate will provide customers with vulnerability scanning reports and security briefings to advise them of critical and high-risk vulnerabilities that may affect customer or corporate security objectives

Responsibilities

- The provision and delivery of Vulnerability Scanning Services in accordance with CyberTech methodologies.
- Leading or participating in vulnerability management projects
- Creation of draft reports and presentations;
- Assisting in the presentation of findings to the customer.
- Work with existing solution vendors (e.g., Nessus) as necessary; identify potential solutions.
- Perform assessments and correlate vulnerability data, in order to quickly identify risks.
- Produce reports on patches, exploits, and vulnerabilities.
- Recommend and track the application of fixes, security patches, and security updates.
- Document security procedures and policies.
- Other duties as assigned.
- Typical tasks involve:
- Carrying out research and data collection to understand vulnerabilities;
- Conducting analysis;
- Identifying issues, escalating issues and/or forming hypotheses and solutions;
- Presenting findings and recommendations to clients.

Desired Skills & Experience

Knowledge of Mac OS, Current Windows client operating systems, Windows Server and Cloud environment especially Microsoft Azure, and AWS systems is needed.

Other qualifications include:

- Bachelor Degree; or any combination of education and experience, which would provide an equivalent background.
- 2-3 years of experience in Information Security, Computer Science, Data Analytics, or related field.
- An understanding of Vulnerability Management technologies, methodologies and procedures.
- Knowledge of at least one of the following industry-standard vulnerability management tools. Nessus, Qualys, Nmap, or Rapid7 Nexpose.
- Knowledge of metrics, and trending for vulnerability management functions
- Verbal communications skills and concise written communication skills.
- Organization and multi-tasking skills.
- Security+, GSEC are preferred.