



Job Description

Job Title: Security Analyst
Reports To: Manager, Security and Compliance Operations

Summary:

Digital Defense has an immediate opening for a Security Analyst to work on the Security and Compliance Operations team. Candidates must have prior experience performing penetration testing and vulnerability assessments and own at least one industry-recognized security certification. The Security Analyst is responsible for performing security services for clients to include, but not limited to: penetration testing, remote and onsite social engineering, war dialing, wireless assessments, network security architecture reviews and physical site audits. He/she must be a team-oriented person, working with other members of the Operations team to ensure that Digital Defense provides its clients with thorough, professional security services that deliver value to business and technical end-users. The Security Analyst must have outstanding written and verbal communications skills, with the ability to translate highly technical topics to non-technical customer staff. Travel up to 15% may be required. The candidate must live in or be willing to relocate to the San Antonio, TX, area.

Specific Duties:

1. Perform research, analysis and testing of network, application, physical and procedural vulnerabilities via vulnerability assessment, penetration test, war dialing and/or social engineering.
2. Clearly outline and portray test findings via well-documented reports. Delivers professional onsite and remote briefings to clients based on results of testing.
3. Assist clients with questions regarding vulnerabilities and the remediation efforts involved in eliminating them.
4. Review IDS and or firewall signature/rule sets and make recommendations for improvement.
5. Improve customer deliverables through report template and procedural updates.
6. Other duties as assigned.

Education & Experience (Minimum requirements):

1. Experience
 - Must have at least three years of security industry experience with particular focus on conducting penetration testing and vulnerability assessments.
2. Degree
 - Bachelor's degree in Computer Science, Engineering, Information Systems, Physics, or similar field from an accredited university is preferable.
3. Professional Certification
 - **Minimum requirement** – Candidate must hold at least one recognized industry security certification, such as CISSP (preferred), CISA, Security+, etc. *Candidates will not be considered if this requirement is not met.*
4. Programming Skills
 - Proficient in at one or more programming/scripting languages, such as Perl, Python, Ruby, C, etc.



- Proficient in UNIX shell scripting.
- 5. Networking
 - Must have a solid understanding of TCP/IP.
 - Should be well rounded in respect to knowledge pertaining to encrypted and clear text protocols and their usage.
- 6. Operating Systems
 - Must have a solid understanding of a wide variety of operating systems, such as Microsoft Windows Server 2003/2008, Windows XP/Vista/7, and various flavors of UNIX.
 - Must understand Active Directory.
- 7. Information Security
 - Experience utilizing vulnerability scanning and assessment tools such as OpenVAS, NMAP, Metasploit and others is preferable.
 - Familiarity with commercial firewall and IDS technology is required.
 - Must understand and have the ability to apply penetration testing methodology
- 8. Communications Skills
 - Must be capable of working independently and as part of a dynamic team. Must have excellent writing skills and be able to convey ideas in a clear and concise manner.

Other Information:

- All applicants must pass a criminal and credit background investigation to be considered for employment.
- Government security clearance **is not** required
- All applicants must pass a practical exam where they will be asked to conduct an assessment of a target network and develop a formal report on their findings.
- Relaxed dress code and work environment
- Free soda and Red Bull/Monster for all employees

Interested parties should send resumes to HRSECOPS@ddifrontline.com. No phone calls, please.