



Job Description

Job Title: Security Analyst

Reports To: Team Supervisor, Remote Security Services

Summary:

Digital Defense has an immediate opening for a Security Analyst to work on the Remote Security Services team. Candidates must have prior experience performing penetration testing and vulnerability assessments and at least one 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, and physical site audits. He/she must be a team-oriented person, working with other members of the Security and Compliance Operations team to ensuring that Digital Defense provides its clients with thorough, professional security services that deliver value to business and technical end-users. The Security Analyst must also have outstanding written and verbal communications skills, with the ability to translate highly technical topics to non-technical customer staff. Travel up to 10% may be required.

Specific Duties:

1. Perform research, analysis and testing of computer/network vulnerabilities via vulnerability assessment, penetration test, war dialing and/or social engineering.
2. Clearly outline and portray test findings via well-documented reports. Delivers client briefings as needed.
3. Through prior experience, mentor and train junior-level analysts, enhancing their technical abilities.
4. Assist clients with questions regarding vulnerabilities and the remediation efforts involved in eliminating them.
5. Review IDS and or firewall signature/rule sets and make recommendations for improvement.

Education & Experience (Minimum requirements):

1. Experience
 - Must have at least three years of industry experience.
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.
4. Programming Skills
 - Proficient in at least one of the following languages: Perl, Python, Ruby, and/or C.
 - Proficient in UNIX shell scripting.
5. Networking
 - Must have a solid understanding of both data and voice networks and their associated peripherals. A candidate with strong Voice over IP (VoIP) security



experience is highly desirable. Should be well rounded in respect to knowledge pertaining to encrypted and clear text protocols and their usage.

6. Information Security

- Must have experience utilizing multiple vulnerability scanning tools and exploits including Nessus, NMAP, Metasploit and others. Familiarity with commercial firewall and IDS technology required.

7. 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.

Interested parties should send resumes to HRSECOPS@digitaldefense.net. No phone calls, please.