



## Job Description

**Job Title:** Security Analyst  
**Reports To:** Manager, Managed Security Operations

### Summary:

Digital Defense has an immediate opening for a Security Analyst to work on the Managed Security Operations team. Candidates must have strong project management skills and prior experience performing network security consulting and/or working within an enterprise security organization. Candidates must also have at least one industry-recognized network security certification. The Security Analyst is responsible for acting as an on-demand security resource for Digital Defense clients, managing vulnerability assessments and remediation activities based on applicable standards. He/she must be a strong team-oriented person, working with other members of the Digital Defense Operations team to ensure that Digital Defense provides its clients with thorough, professional security and compliance 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 is rarely required, with no more than 5% expected. The candidate must live in or be willing to relocate to the San Antonio, TX, area.

### Specific Duties:

1. Perform research and analysis and provide recommendations for remediation of computer/network vulnerabilities discovered on client networks.
2. Project manage remediation activities for clients utilizing applicable standards, such as PCI-DSS, NIST and ISO 27001/27002.
3. Clearly outline and portray assessment findings via well-documented reports.
4. Conduct onsite and remote client briefings on results and prioritize remediation of vulnerabilities based on overall risk and severity.
5. Perform hands-on remediation of discovered vulnerabilities, following vendor recommendations where required.
6. Coordinate and conduct vulnerability assessments and testing in support of customer Payment Card Industry (PCI) requirements.
7. Act as an on-demand security resource for assigned customers.
8. Assist in the management of compliance activities for clients.
9. Other duties as assigned.

### Education & Experience:

1. Experience
  - **Must have** at least three years of industry experience.
2. Education
  - 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+, C|EH, etc. *Candidate will not be considered unless this requirement is met.*
- 4. Programming Skills
  - Proficiency in scripting languages, such as Perl, Python, or Ruby is a plus.
- 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.
- 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.
- 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
- Relaxed dress code and work environment
- Free soda and Red Bull/Monster for all employees

Interested parties should send resumes to [HRSECOPS@ddifrontline.com](mailto:HRSECOPS@ddifrontline.com). No phone calls, please.