Junior Information Security Analyst

Job Description:
Security Compliance Associates is seeking a Junior Information Security Analyst to join our team of qualified, diverse individuals. This position will be located at SCA corporate location in Clearwater, FL. A successful candidate will need to be able to perform the tasks below along with some other requirements.

Responsibilities include:

- Perform port and vulnerability scans of small and large networks, systems and applications
- Write clear, detailed assessment reports and recommendations for security enhancements and other security measures
- Assist clients with questions regarding vulnerabilities and propose mitigations
- Assess mobile and online applications for vulnerabilities
- Find/Identify web application vulnerabilities following OWASP Top 10
- Perform wireless vulnerability assessments, including access point detection and WEP cracking
- Password cracking, assessing strength of passwords hashes, generate custom doc/pdf files that tests for the existence of a vulnerability
- Perform research, analysis and testing of network and application vulnerabilities

Knowledge, Skills, Abilities:

- Technical certifications that support vulnerability and penetration testing
- Knowledge of application and infrastructure scanning tools such as Nessus
- Experience with common security controls including firewalls, proxies, IDS/IPS, Web Application Firewalls, Data Loss Prevention products, Internet filtering products
- Technical knowledge of fundamental Internet protocols, services, and technologies to include HTTP(S), TLS, DNS, SMTP, TCP/IP, ICMP, JSON, REST
- Understanding of server/client/operating systems and access control management solutions
- Knowledge of common vulnerabilities, exploits and mitigations
- Understanding of and experience either executing or defending against complex, targeted cyber threats to high-value systems and data
- In-depth understanding of commonly used layer 2-7 communication protocols, encoding and encryption schemes and algorithms
- Familiarity with NIST Risk Management Framework
- Solid understanding and knowledge of OSSTMM 3, NIST SP800-15, Penetration Testing Framework and OWASP Top 10 Project (Web and Mobile)
- Understanding of regulatory requirements relating to financial, medical, real estate and government entities (FFIEC, NCUA, HIPAA, ALTA, GLBA, NYDFS Cybersecurity Regulation)
- Excellent client expectation management and communication skills and the ability to translate technical concepts to business information for executive level staff report review
- Solid prioritization and time management and logical problem identification and diagnosis skills.
- Contribute to continuous process improvements
- Proactive research to identify and understand new threats, vulnerabilities, and exploits

ADDITIONAL SKILLS:

- Previous software development to support penetration testing; vuln dev, tool modules, covert tunneling, scanning scripts, passive collection, etc.

· Previous experience countering Advanced Persistent Threat (APT) type threats to large enterprises (USG or commercial), such that there is familiarity with techniques and tools employed
· Ability to keep abreast of developments and relevant technologies applicable to Information Security

Other:

· Casual dress work environment
· Flexible hours with work from home opportunities
· Bonus Compensation Available
· Health care and other benefits