Penetration Tester / Ethical Hacker - CampusGuard

Position Summary

CampusGuard focuses primarily on the information security needs of institutions of higher education and organizations with a campus-type environment. All of our staff has experience working with the unique needs of a campus-based environment, including higher education institutions, healthcare providers, city councils and destination resorts. Currently we primarily focus on assisting these organizations with achieving compliance with the Payment Card Industry Data Security Standard (PCI DSS) and the Health Information Privacy and Accountability Act (HIPAA), but we are a full service security firm experienced in all industry standard compliance and information security issues.

The Penetration Tester/Ethical Hacker is responsible for assessing a customer's business and operating environment risk and infrastructure vulnerability posture. This position requires a wide range of knowledge of network infrastructures, operating systems hardware platforms, networking systems and the security vulnerabilities within each category. The qualified individual in this position will scan customer networks to discover and exploit security flaws and vulnerabilities with attack simulations on multiple platforms working against a specific customer-focused scope of work. This position requires a highly technical skill level to assess the risks and vulnerabilities of a customer's network while being able to articulate the issues to a non-IT professional audience. Excellent communication skills, both oral and written are required to provide the reporting information to the customer after the tests are completed. When not performing the specific Scanning and Penetration Testing / Ethical Hacking functions, the individual in this position will provide support to the Security Advisors with other security assessments and gap analysis functions.

Principal Responsibilities

Responsible for scanning and performing in depth penetration testing and reporting customer business and operating environments and network infrastructure related to compliance and other relevant industry standards. Activities include, but are not limited to the following:

- Understand the Scope of Work for each customer agreement and perform the duties and tasks required by those agreements in an organized, professional manner.
- Perform vulnerability assessments and penetration testing, utilizing commercial and open source tools.
- Conduct penetration testing in line with Open Web Application Security Project.
- Exploit security flaws and vulnerabilities with attack simulations on multiple projects working against specific customer systems and networks in accordance with an agreed scope of work.
- Effectively provide technical risk assessment of technologies in networks, applications, systems, wireless, and perform social engineering.
- Review and analyze security vulnerability data to identify applicability and false positives.
- Ability to solve complex technical problems and articulate to non-IT personnel.
- Document all processes and procedures in accordance with CampusGuard standards.
- Report on findings and assist customers in remediation activities as required.
- Research and develop testing tools, techniques, and process improvements.
- When time allows, perform security assessments and gap analysis of system infrastructures in alignment with the PCI DSS, HIPAA and other well-known information security requirements.

Assist with sales and marketing activities:

- Perform or assist with sales calls
- Attend conferences
- Perform industry presentations and/or webcasts
- Other sales/marketing duties as requested

Education and Experience Requirements

The Penetration Tester/Ethical Hacker must have sufficient information security knowledge and experience to conduct technically complex security assessments.

- Minimum acceptable education requirements: Bachelor's degree, and/or 5 years' experience in the information security industry (preferably at an institution of higher education)
- Minimum acceptable certification requirements: Possess industry-recognized security certification(s) including one or more of the following: GIAC Certified Ethical Hacker *(preferable*), Certified Information System Security Professional (CISSP), Certified Information Systems Auditor (CISA)
  Note: Candidate must agree to prepare for and pass the PCI Qualified Security Assessor (QSA) certification and any other certifications as directed by his or her manager.
- Minimum acceptable work experience requirements: If a candidate does not satisfy any of the above education criteria or certificates, he or she must have a minimum of five years of relevant information security experience or proof of other recognized security certifications.

Key Skills, Qualifications and Traits

- Demonstrates an ability to methodically analyze problems and identify solutions and communicate to a non-technical audience.
- Exhibits good writing and communications skills, to include the ability to render concise reports, summaries, and formal oral presentations.
- Adequately explains, presents, demonstrates [when applicable] and documents the operational impact of a particular vulnerability/exploit. Assists customers with remediation tasks for found vulnerabilities.
- Self-motivated and able to work both independently and with a team.
- Willing to travel up to 50% of the time.

Competencies

(C=Core Competencies; F=Functional)

- C- Understanding of Higher Education, Healthcare, and Government institutions and their structure.
- C- Understanding of information processing networks and related security issues.
- C- Understanding of Industry standard information security standards and their applicability.
- C- Understanding of system infrastructures, vulnerabilities, exploits and remediation tasks.
- F- Ability to flow from black box to gray box to white box testing methodologies dependent on customer needs
- F- Understanding of the well-known security standards e.g., PCI DSS, NIST 800-53, ISO 27001-27006
- F- Understanding of Health Information security standards e.g., HIPAA, HITECH.
- F- Understanding of differences between security breach, data compromise, and fraud
- F- Understanding of campus type environments, structures, operations, and security needs

Organizational Reporting

- Reports to: Manager, Security Advisor Services