Senior Security Consultant | Offensive Security (WFH / REMOTE WORK)

Calling all experienced security consultants, super sharp hackers, and talented nerds! Are you tired of spending your workdays repeating the same boring compliance checkbox pentesting? Have you been looking to take that next step in your career, and think you have what it takes to help lead engagements? Do you want to help create something special, something that will make a difference in this world?

Then Blue Bastion has a role for you.

We are seeking out Senior Security Consultants to help us grow our Offensive Security practice. In this role you will be responsible for designing and executing campaign based technical engagements to help our clients grow and mature, not just check a box. Our clients leverage us as a trusted partner, with intimate knowledge of their business. We make it a point to understand the mission, vision, and culture of the company. This helps us to prioritize projects and remediation based upon risk and impact, not simple vulnerability counts and industry “standard” scoring.

As a senior consultant you will help develop training and provide mentoring to our consultants, associates, and interns. You must be able to communicate complex findings, security strategy, and technical execution methodology to client stakeholders. This includes executive leadership, technical staff, legal counsel, and non-technical support staff.

We favor candidates who actively participate in the information security community. If you are an extrovert, we love to see you presenting your research at conferences, teaching classes, participating in CTFs, and helping to guide the next generation. More of an introvert? We get it. We welcome folks who want to work in the shadows (home office,) create new tools for the team, or focus on research, education, and delivery. Whatever your passion, we want to help you foster it!

CERTS:
We value and respect the OSCP, OSCE, OSWE, CISSP, GPEN, GXPN and other Offensive Security certifications but they are not required for the role.

Your role:

- Designing and executing complex campaigns against a wide variety of industries and targets. These technical offensive security engagements include but not limited to:
    - Red & Purple Teaming
    - Physical Assessments
    - Cloud, IoT, Network, and Application Pentesting (Dynamic and Static Analysis)
    - Adversarial Threat Emulation
    - Assumed Breech
    - Social Engineering
    - Ethical Hacking
    - Vulnerability Assessment
    - Malicious Software Analysis
    - Hardware Security Assessments
- Advising Incident Response and Blue Teams on adversarial actions, methods, and techniques.
- Develop training and provide mentoring to our consultants, associates, and interns.
- Interfacing with clients (technical & executive staff) helping them understand findings, risks, potential impact, remediation prioritization and activities, along with recommended next steps.
- Create threat models and engagement plans via customer specified objectives.
- Strategize and coordinate with other Red Team staff to conduct complex engagements.
- Research and refine our team tactics and techniques to ever improve our capabilities and methodologies.
- Assist with the development, testing, and deployment of custom attack tools designed to fill specific Red Team needs.

Experience / Skills:

- Demonstrate strong communication skills
- A passion for information security and previous consulting experience
- A degree in Computer Science, Electrical Engineering, Information Assurance, Network Security Computer Engineering or a related field, or equivalent experience is a bonus, this is NOT A REQUIREMENT.
- 3 - 7 years of experience in several of the following disciplines: Penetration Testing, Professional Consulting, Programming/Scripting (java, node, python, etc), Incident Response, Red Teaming, Ethical Hacking, Vulnerability Assessments, Social Engineering, Application Security Testing (Mobile, Web, etc.), Dynamic and Static Analysis, Malicious Software Analysis, Reverse Engineering, Hardware Assessment, IoT/Cloud/Network Pentesting

- Experience with the commonly used attack frameworks (Cobalt Strike, Metasploit, Poshc2, CANVAS, Empire, Core Impact, etc.)
- The ability to think and act as an adversary during remote and onsite engagements
- Ability to document and explain technical details in a concise, understandable manner
- Ability to manage and balance own time among multiple tasks, and lead other staff as required
- Advanced knowledge of application mobile security tools
- Familiarity and experience with security technologies such as security engineering, security architecture, cryptography, data security, risk management, identity and access management, communication and network security, security assessment and testing, software development security, security operations
- Thorough understanding of issues documents in the OWASP Top Ten and CWE Top 25
- Demonstrated ability to exploit and mitigate application-level vulnerabilities
- Strong understanding of cryptography as applied to web application security (encryption, hashing, PKI management), including analysis and implementation
- Some travel (<25%) and heavy lifting (50 lbs) may be required.

Compensation:

- Minimum Salary: $90,000 - Final salary will be determined commensurately with cost of living, experience level, and/or any other legally permissible considerations.
- Commission: All employees are eligible for commissions on referred business (include basic structure or percentages here)
- Health, Dental and Vision Insurance
- Life Insurance
- Short-term and Long-term Disability Insurance
- Retirement planning options (Simple IRA)
- PTO/paid holidays
- Annual bonuses
- Remote work opportunities
- Compensation for continued education and professional development (Certs)

Job Type: Full-time

Reports to: VP of Offensive Security