Security Consultant | Offensive Security (WFH / REMOTE WORK)

Calling all security consultants, hackers, and nerds! Are you wanting to take the next step in your security career? Think you have what it takes to be the consultant who is performing the technical engagement? Do you want to be part of something new, something special, something that will make a difference in this world?

Then Blue Bastion has a role for you.

We are seeking out Security Consultants to help us grow our Offensive Security practice. In this role you will be responsible for working alongside our Senior Consultants conducting campaign based technical engagements to help our clients grow and mature, not just check a compliance 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 prioritize projects and remediation based upon risk and impact, not simple vulnerability counts and industry “standard” scoring.

As a security consultant you will assist our senior staff in delivery and execution and provide mentoring to our associates, and interns. You will learn to communicate complex findings, security strategy, and technical execution methodology to client stakeholders. As part of our OffSec team you will help brief 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:

- Assisting with the design and execution of 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.
- Contribute to the development of training and provide mentoring to our 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.
- Conduct threat assessments and technical testing following custom methodology and engagement plans via customer specified objectives.
- Strategize and coordinate with other Red Team staff to conduct complex engagements.
- Offer guidance and help refine our team tactics and techniques to ever improve our capabilities and methodologies.
- Assist with the testing, and deployment of custom attack tools designed to fill specific Red Team needs.

Experience / Skills:

- 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, NOT A REQUIREMENT.
- 2 - 5 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, Poshc2, Metasploit, 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 contribute to group projects
- Knowledge of application mobile security a bonus
- 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 network, host, and 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:

- 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