ACTIVECYBER
SECURITY ▪ RISK MANAGEMENT

Offensive Security Consultant/Penetration Tester

ACTIVECYBER is seeking a full-time Offensive Security Consultant/Penetration Tester to support our growing, fully remote cybersecurity team and commercial clients. The responsibilities of the position include vulnerability assessments, penetration testing, and information system security oversight activities that support complex systems from the perspective of sophisticated threat actors. The Offensive Security Consultant/Penetration Tester will be expected to actively engage with the testing team and to participate in the development of internal methodologies and processes.

Responsibilities

- Perform vulnerability scans, network penetration tests, red teaming, web application testing, threat analysis, wireless network assessments and social engineering assessments
- Develop comprehensive and accurate reports and presentations for both technical and executive audiences
- Effectively communicate findings and strategy to customer stakeholders, including technical staff and executive leadership
- Recognize and safely utilize attacker tools, tactics and procedures
- Develop scripts, tools or methodologies to enhance the penetration testing process
- Lead a penetration test and security assessment from kickoff through remediation

Requirements

- Bachelor's degree in a technical discipline, or equivalent experience
- At least 1-3 years of experience performing and leading assessments related to penetration testing of both networks and applications.
- Hands-on experience with commercial tools commonly used to perform security assessments (e.g., Metasploit, Nessus, Qualys, Burp, Accunetix, etc.)
- Ability to operate in C2 framework of choice (Covenant, Cobalt, etc.)
- Mobile Application testing knowledge is a plus but not a requirement
- Experience conducting analysis of electronic media, packet capture, log data and network devices in support of intrusion analysis or enterprise level information security operations
- Expertise consulting with stakeholders to define needs, develop requirements and analyze findings to advise and recommend solutions
- Excellent communication and presentation skills with the ability to present to a variety of external audiences, including senior executives
- Ability to work independently, whether onsite or remotely
- Willingness to travel domestically as needed, not to exceed 10%

Additional Qualifications

- GIAC Penetration Tester (GPEN) and/or Offensive Security Certified Professional (OSCP) or comparable certification required

ACTIVECYBER

SECURITY ▪ RISK MANAGEMENT

Organization Profile

ACTIVECYBER is a team of cybersecurity and risk management professionals located in the Washington, D.C. area. We advise C-Suite, Executive Committee and Technology leadership on maturing and maintaining your cybersecurity posture - whether responding to an incident, demonstrating third-party compliance or testing your employees' susceptibility to a phishing attack.

Our leadership team has been relied upon to spearhead and resolve the most discrete cybersecurity matters since 2002. Our clients are law firms, associations, healthcare organizations, financial institutions, think-tanks and more. We have earned the role of trusted advisor, but approach it in a collaborative spirit; from the Board Room dashboard to detailed risk analysis alongside your technical team.

With so many regulatory mandates and stakeholder requirements for accountability on the rise, organizations face continued demands to demonstrate an acceptable state of cybersecurity while constantly striving to keep pace with the ever-changing threat landscape and these third-party requirements.

Benefits

All full-time positions at ACTIVECYBER are eligible for benefits including healthcare, dental, vision, matching 401(k), PTO, and industry training. Competitive salary commensurate with experience and ability to demonstrate proficiency in the position requirements.

Candidate must be a US Citizen. ACTIVECYBER is an Equal Opportunity Employer.

Qualified candidates should submit resumes to careers@activecyber.us.