ACTIVECYBER
SECURITY ▪ RISK MANAGEMENT

Information Security Analyst

ACTIVECYBER is seeking a full-time Information Security Analyst to support our growing cybersecurity team and commercial clients in the Washington DC metro area. The responsibilities of the position include security assessment and testing, vulnerability assessments, compliance assessments across multiple industries, governance, and information security policy/procedure development. The Information Security Analyst will be responsible for conducting security assessments, developing policies and procedures, and conducting compliance assessments for our customers.

Responsibilities

- Conduct security assessments of customer systems, services, and programs.
- Analyze customer processes and configurations to verify that previously identified flaws have been corrected, and document the results.
- Conduct compliance assessments against industry best-practices and frameworks
- Develop procedures and policies to help clients adhere to industry best-practices and frameworks
- Develop detailed remediation reports and recommendations for compliance and security improvements across industries based on changing threats.
- Develop and update a consistent approach to information security programs and ensure adherence with best practices.

Requirements

- Bachelor's degree in a technical discipline, or equivalent experience
- 2-4 years of information security experience
- Experience with at least one of the following security industry frameworks: NIST, ISO, HIPAA, SOX, GLBA, etc.
- Clearly articulates technical requirements and other information in written documentation
- Experience with developing information security policies and procedures at the enterprise level
- Experience developing security plans (such as Incident Response Plans and Disaster Recovery Plans) at the enterprise level accompanies by the development of test plans
- Vulnerability scanning experience is a plus
- Effectively communicates technical and nontechnical concepts to a variety of audiences.
- Communicates well with customer technical staff and management
- Methodically gathers, documents, and presents specific customer requirements
- Follows existing processes and procedures, and propose updates to such. Develop new processes and procedures as necessary
- Works with minimal supervision, set priorities, and give attention to detail and quality
- Demonstrates strong organizational and time-management skills: multitasking, working individually and with a team, having a positive attitude, being self-motivated and reliable, being trustworthy, having strong interpersonal and diplomatic skills
- Be proficient with Microsoft Office
- Excellent written communication skills
- Ability to work independently and lead small teams internally, whether onsite or remotely
- Willingness to travel domestically as needed, not to exceed 20%

ACTIVECYBER
SECURITY ▪ RISK MANAGEMENT

Additional Qualifications

- Security+, Certified Information System Auditor (CISA), and/or Systems Security Certified Practitioner (SSCP) highly desired
- Certified Information Systems Security Professional (CISSP) certification desired

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 SIMPLE IRA, 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.