Job ID: S-TST-001
Job Title: Senior Cybersecurity Analyst – Lead Assessor
Date: 06/21/2020
Location: Manassas, Virginia (Primary), Wash DC (Secondary)

At Cybereye, we are a small business with a laser sharp focus on bringing high quality cybersecurity assessment and assistance services to organizations that are embarking on a risk and compliance journey. We are building a team of driven, talented, and thought leading consultants that share our desire to become a trusted partner to our clients and fully vested in their business outcomes. Cyber security is as much a business challenge as it is a technical challenge, and we bring our clients solutions for both. Cybereye was founded by an expert in Governance, Policy and Compliance, built on a foundation of 18 years cyber strategy consulting for large corporations, military clients, and state and local governments. If you are looking for an entrepreneurial environment, crave a fast-paced setting, thought provoking work, and are looking for an opportunity to expand your cyber skills in new specialty areas, you may be the right candidate to help Cybereye bring our client's business to the next level.

Job Summary

Provide cybersecurity vulnerability assessment and risk assessment services to identify gaps in compliance across a broad set of security requirements frameworks such as National Institute of Standards and Technology (NIST) 800-53, Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), International Organization for Standardization (ISO) 27001, NIST Cyber Security Framework (CSF), and Center for Internet Security (CIS(Top 20. A qualified candidate will be responsible for the following primary duties and responsibilities, but are not limited to:

- Design and develop assessment plans to include security control baselines and applicable secure configuration vendor guidelines and available benchmarks
- Execute vulnerability assessments using industry standard tools such as Nessus, RedSeal, and Security Content Automation Protocol (SCAP) benchmarks, and available Cloud Service Provider (CSP) toolsets (e.g., Microsoft Assessment and Planning Toolkit (MAP))
- Develop risk assessments based on analysis of system architecture diagrams, vulnerability reports, and applied mitigations
- Lead a team of junior and mid-level cybersecurity assessors by providing templates, quality standards, coaching, mentoring, and oversight

Job Description

Key Role
Provide cybersecurity assessment services to help our clients understand their system vulnerabilities and remediate (or mitigate) the risk associated with the vulnerabilities to achieve an acceptable security posture. Perform technical assessments, and assess the risk associated with vulnerabilities, and make recommendations based on system and enterprise level risk. A qualified candidate will be responsible for the following primary duties and responsibilities, but are not limited to:

- Develop a standardized, mature assessment capability tailored specifically for the needs of our client
- Perform vulnerability assessments with documented assessment plans and security control baselines
- Analyze and document the risk associated with vulnerabilities and make risk recommendations with documented risk assessments
- Participate as part of the change review board, assessing system and network changes, for risk and impact to the enterprise-level security posture
- Actively participate in engineering and architecture review meetings, offering advice and recommendations based on past experience and understanding of Defense in Depth (DiD) security principles
- Provide day-to-day oversight and team leadership for all assessment activities

Submit Resume to kim.maurer@cybereyesolutions.com

Basic Qualifications:

- 10+ years of experience performing vulnerability assessments (minimum of 4 years of experience using Nessus, and SCAP benchmarks)
- 8+ years of experience leading a team of assessors, and building assessment and remediation plans
- 5+ years of experience providing test plans, reports and Plan of Actions & Milestones (POA&Ms) that directly supported the NIST Risk Management Framework (RMF) Assessment & Authorization (A&A) process
- 2+ years of experience assessing cloud-hosted systems for the purposes defining security control responsibility between providers and consumers, and validating secure configuration of cloud services
- 2+ years of experience generating, analyzing, and reporting assessment metrics using dashboards
- Experience independently authoring architecture diagrams, data flow diagrams, and other technical documentation
- Experience reviewing system architectures, decomposing systems into testable components, and selecting applicable configuration standards to achieve security requirements such as NIST 800-53, PCI DSS, HIPAA, ISO 27001, NIST CSF, and CIS Top 20.
- Experience with risk assessment and mitigation, Information Assurance principles, National Institute of Standards and Technology (NIST) special publications
- Possession of excellent oral and written communication skills
- BA or BS degree in IT related field (May be waived for equivalent experience)
- Professional security certification such as CISSP, Security+, CEH, ISSEP (alternative certifications will be considered)

Preferred Qualifications:

- Experience with RedSeal for networking mapping and vulnerability impact assessments
- Experience with Tableau, Splunk, or Power BI for security data analytics
- Experience with ServiceNow for GRC workflow management and tracking
- Experience generating test plans and reports for RMF A&A Packages or overseeing a team and resolving challenges
- Experience with both commercial and government organizations (e.g., Legislative Branch, DoD, or State and Local

Clearance:
Applicant selected may be subject to a security investigation and may need to meet eligibility requirements for access to classified information.

Submit Resume to kim.maurer@cybereyesolutions.com