pillarsystems CORPORATION
"Supporting Our Clients Through Pillars Of Excellence"

Senior Vulnerability Analyst

Clearance	Active Top Secret
Position Responsibilities	Looking for a Senior Engineer for a cybersecurity team which performs vulnerability analysis for a customer with a complex network featuring over 100,000 endpoints. The objectives of the team are to develop a risk picture for the enterprise and to provide tailored remediation strategies to stakeholders in order to improve the overall cybersecurity posture of the organization. In this role, you will assist a small team in vulnerability management for stakeholders at all levels across the enterprise. This will include analysis of high-profile and high-impact vulnerabilities, zero-day threats, the creation and execution of mitigation strategies, and the liaising with various IT stakeholders to coordinate implementation of such strategies. An ideal candidate will have a proactive Computer Network Defense (CND) mindset and both a strategic understanding of the protection of complex Internet-facing networks, as well as the technical experience to implement of comprehensive vulnerability remediation strategies. Strong customer service and project management skills are also desired to provide technical guidance to other IT teams.
Responsibilities	• Leading enterprise efforts on risk assessment, detailed technical recommendations and coordination of remediation and mitigation strategies. • Preparing reports and conducting briefings for senior leadership related to routine and high-profile vulnerability analysis. • Developing and perform high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, policy compliance and vulnerability analysis of the overall enterprise security posture. • Communicating recommendations to the responsible parties, and engaging in both tracking and verification of their remediation efforts. • Continually analyzing available security information, including results of configuration compliance verification, vulnerability scans, database assessments, security and system patch information, threat reporting, OIG reporting, and other intelligence information to update and assess the status of an organization's cyber security posture. • Assisting in the analysis, selection, implementation, and/or development of enterprise security tools. • Interfacing with vendor support teams to keep abreast of developments within products currently in use. • Documenting team processes for use in internal Standard Operating Procedures (SOPs), and other on-the-shelf documentation of processes for future team reference. • Building working relationships to effectively complete the mission, while acknowledging and respecting stakeholder needs and requirements. • Both formulating new and adjusting existing information security metrics for the purpose of analysis and greater enterprise security posture awareness. • Consultation and support to other parties concerning Computer Network Defense (CND), often on an ad hoc basis, as necessary for the mission.

Web: pillarsystems.com | Phone: 703.548.4800 | Fax: 703.548.4806
For more information or inquiries, please contact us at: recruiter@pillarsystems.com

pillarsystems CORPORATION
"Supporting Our Clients Through Pillars Of Excellence"

Senior Vulnerability Analyst

Required Qualifications	• Bachelor's Degree or equivalent years of experience in a relevant field (e.g. Cybersecurity, Information Technology, or Computer Science). • Minimum five (5) years of experience in information security, information technology, or related field. • Proficiency in traditional Blue Team or Red Team network security activities. • Experience developing goals, processes and a methodology for effective cyber security assessments. • Experience performing manual and automated analysis of systems and networks to identify, assess, and mitigate vulnerabilities to strengthen organizational security posture. • Experience performing risk assessments by correlating known vulnerabilities, understanding of the threat environment, and prioritization to mitigate risk to network assets. • Effective written and verbal communications skills to prepare and present security assessment results to stakeholders, and to further build relationships with them. • Proficiency in Splunk, Tanium, and other enterprise-level data analytics tools. • Experience with Windows Desktop, Windows Server and Linux operating systems and system administration – specifically with regard to patching and compliance. • Experience with networking hardware (routers, switches, firewalls) and configurations – specifically with regard to patching and compliance. • A solid understanding of core networking concepts such as DMZs, subnets, VLANs, private IP addressing and NAT. • Active Secret (Minimum) security clearance.
Desired Qualifications	• Security+ and/or Network+ certification. • Certified Ethical Hacker certification. • Certified Information Security Systems Professional (CISSP) certification. • 2+ years of experience familiarity with NIST Special Publication 800-53 and CVE (Common Vulnerabilities and Exposures) standards. • Experience with project management to ensure stakeholders remain on schedule with patching and policy compliance to improve overall network security posture. • Experience in developing and leading remediation/ mitigation activities, and building strategies, status updates, and reports on those activities.

Web: pillarsystems.com | Phone: 703.548.4800 | Fax: 703.548.4806
For more information or inquiries, please contact us at: recruiter@pillarsystems.com