pillarsystems CORPORATION
"Supporting Our Clients Through Pillars Of Excellence"

Cyber Threat Hunter/Researcher – Mid-Level

Functional Duties	The Cyber Threat Hunter and Researcher will support the customer's overall cyber threat analysis efforts. Perform advanced analysis of adversary tradecraft, malicious code, and Advance Persistent Threat capabilities. Analyze computer, communication, network security events and exploits to determine security vulnerabilities and recommend remedial actions. Conduct forensic, malicious code, and packet-level analyses to develop comprehensive technical reports stepping through complete reverse engineering of incidents. Recommend countermeasures based on the identified techniques, tactics, procedures, and behavior patterns used by adversaries. This role is also responsible for developing alert criteria to improve incident response capabilities; as well as, contributes to development, writing, and reviewing of SOPs. Candidate should possess experience and knowledge of cyber threat and/or intelligence analysis. Candidate should have proven expert written and oral communication skills to include experience with executive-level presentations. Candidate should have knowledge related to the current state of cyber international relations, adversary tactics, and trends. Candidate will possess the ability to work quickly, and a willingness to complete ad hoc, time sensitive assignments.
Qualifications	A Bachelor's Degree in Computer Science, Information Systems, Engineering, Telecommunications, or other related scientific or technical discipline is desired. Four (4) additional years of general experience (as defined below) may be substituted for the degree.
Certifications Desired	GIAC Certified Incident Handler (GCIH), GIAC Certified Forensics Analyst (GCFA), Certified Ethical Hacker (CEH), Encase Certified Examiner (ENCE)
General Experience	3-5 years of experience advanced technical analysis with increasing responsibilities. Demonstrated oral and written communications skills. • Good working knowledge of cyber threat analytics • Previous experience working in cross functional and interdisciplinary project teams to achieve tactical and strategic objectives • Proven ability to document and teach team members how to apply advanced analytic techniques to solve complex problems • Solid understanding of enterprise IT cybersecurity operational environments
Specialized Experience	• Three years of experience in network security with a focus on computer forensics, static code reverse engineering, and advanced (packet) network analysis. Static code reverse engineering experience can be substituted by experience in similar skill in computer forensics, network analysis, mobile device forensics related to malicious code, network flow analysis, or other similar skill • Two years of experience in intelligence or technical analysis with a focus on cyber threat analysis. • Experience analyzing emerging technologies for potential attach vectors and developing mitigation strategies • Ability to evaluate offensive and intelligence-based threat actors based on motivation and common TTPs • Experience with gathering open-source and controlled intelligence to develop predictive understanding of adversarial strategies, priorities, and overlapping interests • Demonstrated expertise in deploying and maintaining open source network security monitoring and assessment tools • Experience writing contract deliverables such as Event Bulletins, Cyber Digests, and Quarterly Summary Reports
Security Clearance	TS (clearable to SCI)

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