pillarsystems CORPORATION
"Supporting Our Clients Through Pillars Of Excellence"

Cyber Threat Analyst

Location	Rosslyn, VA
Security Clearance	TS (clearable to SCI)
Description	Serves as a Cyber Threat and Intelligence Analyst in support of a major federal client. This organization provides services that analyze and produce enhanced cyber security and threat intelligence information to include threats and potential threats to the customer's personnel, information, and information systems; provides timely and relevant intelligence to assist with mitigating cyber threats confronting the Department; supports evaluation, implementation, and operations of tools/technologies used in advanced analysis. Responsible for the delivery of written and oral briefings to stakeholders and community partners across the Foreign Affairs community.
Functional Duties	The Cyber Threat and Intelligence Analyst will support the customer's overall cyber threat analysis efforts. Researches, analyzes, writes, edits, and proofreads technical data for use in documents such as cybersecurity intelligence bulletins, alerts, and briefings. Attends meetings such as those that determine workflow, requirements, and other required documentation as part of contract deliverables. Ensures documentation is accurate, complete, meets editorial and government specifications, and adheres to standards for quality, graphics, coverage, format, and style. Participates in establishing style guidelines and standards for text and illustrations. Contributes to development, writing, and reviewing of SOPs. Creates and utilizes a variety of documentation templates with the goal of standardizing deliverables. Ensures content is developed in an appropriate style for the intended audience to include presentations, bulletins, white papers, memos, policies, briefings, and other products. Acquires subject knowledge by collaborating with analysts and engineers. Assists in coordinating projects from the planning stage, provides additional or missing materials, and edits for content format, flow, and integrity. Researches topics and interview stakeholders to understand communication product requirements; analyzes business problems and helps prescribe communication solutions. Candidate should possess experience with 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.
Qualification	A Bachelor's Degree in Computer Science, Information Systems, Intelligence, English, Communications, History, International Affairs or Studies, or other related technical or liberal art discipline is desired. Four (4) additional years of general experience (as defined below) may be substituted for the degree.
Certifications Desired	CISSP, CISM, Security+

pillarsystems CORPORATION
"Supporting Our Clients Through Pillars Of Excellence"

Cyber Threat Analyst

General Experience	3-5 years of experience in intelligence or technical analysis with increasing responsibilities. Demonstrated oral and written communications skills. • Good working knowledge of cyber threat intelligence analysis • Prior military or intelligence community experience and/or formal analytic training/certification • Strong analytical skills and the ability to effectively research, write, communicate and brief to varying levels of audiences to include at the executive level • Previous experience managing cross functional and interdisciplinary project teams to achieve tactical and strategic objectives.
Specialized Experience	• Three years of experience in intelligence or technical analysis with a focus on cyber threat analysis. • Knowledge of geopolitical issues and events and the use of cyber tools & techniques to influence them • One or more geographic area of expertise, e.g. East Asia and Pacific, South and Central Asia, Near Eastern, European and Eurasian, South American or African areas. • Experience working with data breach analysis • Experience working with open source and social media data platforms to evaluate publically available information for suspicious or malicious activities • Demonstrated expertise in deploying and maintaining tools to facilitate the flow of intelligence analysis and reports. • Experience with All Source production and knowledge of cyber/technical intelligence • Experience writing contract deliverables such as Event Bulletins, Cyber Digests, and Quarterly Summary Reports