CI Cyber Threat Technical Analyst

Clearance: TS/SCI
Location: Springfield, VA
Travel: Up to 25% Global TDY

Overall Assignment Description: To produce, per analyst on average, 36 weekly threat reports, eight monthly threat reports, three quarterly threat reports, and one annual threat study for their specific focus or area. In addition, each analyst will average six reports of inquiry (ROI) and or requests for information (RFI) and publish or contribute to nine Intelligence Information Reports (IIR) annually. Finally, each analyst will produce, on average, 48 weekly status reports. CI Cyber Technical Analysts duties are as follows:

Duties may include (on average per FTE):

- Support team members in completing forensics reports, CI Cyber Inquiries, and monthly, quarterly, and annual CI Cyber Threat reports. Support includes, but is not limited to, written and technical analysis that contributes to the understanding of a particular threat or situation.
- Identify, analyze, define, and coordinate user, customer and stakeholder needs and translate them into technical requirements.
- Detect anomalous activity through network data analysis.
- Develop custom scripts/programs for automated cyber analytical tools.
- Record best practices, lessons-learned, processes and procedures, and other pertinent quality topics in appropriate formats.
- Evaluate Intrusion Detection, incident tickets, event and log analysis, security change tracking and other network security systems and devices.
- Provide written reports based on findings.
- Perform work without appreciable direction and exercising considerable latitude in the determination of technical objectives of assignments.
- Participate in special projects as required.
- Assist in the development and delivery of malware threat awareness products and briefings.
- Participate in technical meetings and working groups to address issues related to malware threats and vulnerabilities.
- Collaborate with customers and team members consisting of computer security and CI investigators and forensic analysts and other internal and external organizations to facilitate a premier malware program.
- Thoroughly investigate instances of malicious code to determine attack vector, payload, potential origin, and determine extent of damage and data exfiltration.

- Develop analysis and make recommendations for the purchase of software that will mitigate malware intrusions.
- Identify risks to computer systems and make recommendations for corrective actions.

Skills and Experience:

Required:

- Shall possess at least 7 years of network analysis experience. Shall possess experience with industry network analysis tools, such as Wireshark.
- Shall be a credentialed graduate of an accredited federal or DoD CI training academy (ex. FBI Academy, etc.).
- Shall possess a bachelor's degree.

Desired:

- Possess a bachelor's degree in Computer Science, Engineering or a related technical discipline.
- Possess post-graduate degree in Computer Science, Engineering, or a related technical discipline.
- Experience with malware analysis.