RIPTRONIX

Riptronix LLC
38001 Fleming Farm Lane
Lovettsville, VA 20180
703-999-9528

www.riptronix.com

Riptronix is looking for a customer-focused team player working on-site in a mission-oriented environment. The candidate must be a self-starter, possess good communication skills, and be willing to interface with multiple teams.

We are currently seeking Cyber Threat Analysts toidentify and assess the capabilities and activities of cyber criminals or foreign intelligence entities, and help initialize or support law enforcement and counterintelligence investigations or activities.

Qualifications:

- Must possess an active TS/SCI Clearance with Full-Scope Polygraph
- Independently leverage IC mission cybersecurity analytic tools and capabilities to generate threat intelligence
- Independently create cybersecurity mission specific and tailored tradecraft (e.g. fingerprints, signatures, indicators) as well as automated solutions
- Independently performing software engineering functions that directly align/integrate into IC mission cybersecurity architecture and capabilities including understanding the overall design, data flow, interfaces, and other pertinent details
- Working with cybersecurity analyst teams in more than one mission space
- Experience in the IC mission cybersecurity environment generating threat intelligence reporting (information sharing and dissemination), performing data analysis, implementing best practices in knowledge management, applying machine learning algorithms and techniques, and creating automated solutions
- Work with Capabilities tools that support the cybersecurity mission space
- Work with IC mission cybersecurity analysts on understanding the adversary and developing mission specific TTPs
- Perform log file analysis, including creating threat intelligence reports that indicate findings, mitigations, and confidence
- Perform network and comms. traffic analysis including creating threat intelligence reports that indicate findings, mitigations, and confidence
- Perform analysis across disparate data sets to discover and inform cyber operations
- Perform advanced queries at scale including knowledge of a diverse range of data sources (e.g. IC, partner, and open sources) to enhance/enrich reporting
- Form advanced analytics, network diagrams, and other forms of associated knowledge to further understand the system, network, environment, and adversary

Education/Experience:

Mid-Career:Five (5) years experience with security operations and incident response. Bachelor's OR Master's Degree in Computer Science, Information Systems, or other related field, One or more of the following Certification(s): CISSP, CISA, CISM, GIAC, RHCE.