Treadstone 71 is working with a UAE client seeking Strategic Intelligence Analysts and Tactical Intelligence Analysts

We are not looking for people that are rooted in indicators of compromise and purely IT related issues. We seek true intelligence professionals who fully understand the lifecycle, structured techniques, collection planning, analysis and analytic writing. This are on location positions in the UAE. Resume and references required. Should you be selected for an interview, we will require analytic writing samples at a minimum.

STRATEGIC ANALYST

- Stay current with "trigger events" (e.g. M&A activity, socio-political issues, executive travel, civil unrest, adversaries, customer issues, and campaigns, etc.) and communicate to other Intel teams
- Assist in the definition of corporate intelligence requirements (both inside and outside of the team, to include key business areas or units) based on changes to business needs, structure, priorities and technology
- Assist in the identification of threat intelligence sources (from a process perspective, acting as a stakeholder for the team)
- Analyze collected strategic intelligence and determine factors such as confidence, relevance, likelihood, and potential impact to COMPANY business services, functions, and products
- Assist the Cyber Intelligence Manager in contextualizing internal intelligence collected from actual security incidents (or c compromises) within COMPANY environment (i.e. mapping threats to business concerns)
- Produce formal intelligence products, based on collection and analysis efforts, tuned to intelligence requirements, different audiences, and can drive risk-reducing courses of action
- Assist the Cyber Intelligence Manager in the dissemination of Intel products, to include threat alerts, reports, briefings, etc.
- Assist/Contribute to situational awareness activities or processes within the organization, and business, providing business context to active or emerging threats
- Conduct intelligence assessments to determine key characteristics of the attack, attribution, and actor motivation, intent, and capability
- Participate in defense and incident response integrated activities
  - Alerts and investigations
- Drive adversary dossier development and adversary organization development, campaign identification and tracking.
- Drive attack vectors awareness, operational impact, defense methods, informational impact while assisting in target definition, actual adversary (skills, maliciousness, motivation), level of automation and rate
- Ingests and/or creates technical, tactical, operational, and strategic intelligence products
- White papers, technical press, peer discussions and data sharing with other organizations
- Authors Periodic and Ad-hoc reports and briefs including:
  - Platform, Adversary, Current Intelligence, Daily Intel Summary, Periodic Intel Summary
- Review and validation of vendor reports

Your experience - qualifications

- Expertise in understanding and applying the intelligence lifecycle.
- In-depth awareness and use of open source intelligence-type tools and methods.
- Expertise in collection methods, intelligence production and analysis, analytic writing, argument mapping, and structured analytic techniques.
    - Training in critical thinking, cyber intelligence, and cyber counterintelligence
- Strong knowledge of threat intelligence platforms.
- Strong analytic tradecraft is necessary, as is the ability to defend analysis in the face of countervailing opinion.
- Exposure to assessing technical intelligence collection and analytic products (e.g. behavioral analysis and reverse engineering outputs) also a plus.
- Strong understanding of the information security threat landscape
- Desired qualifications:
    - Formal intelligence analysis training and/or intelligence application experience

TACTICAL INTELLIGENCE ANALYST

This key analytical position is responsible for the processing, analyzing, and reporting tactical intelligence to provide relevant, accurate, and timely threat intelligence that supports incident response triage activities when necessary while providing tactics, techniques, and procedure reviews of actors and campaigns.

Your manager will help you with:

- Authority to make changes
- Measuring and reporting on key performance indicators.
- Self-education and career progression.
- Career progression into analytics using machine learning as a data science approach to cyber security.
- Coordination with other Intelligence Analysts who focus on emerging threats.
- Application and communication of tactical intelligence concepts to business operations.

Your responsibilities

- Consume and analyze tactical cyber threat Intel (CTI) such as indicators of compromise and tactics, techniques, and procedures.
- Act as a liaison between operators/investigators and the Cyber-Fusion Manager to add context to security investigations.
- Provide timely Intel support to operators/investigators, but also directly assisting and/or executing investigative actions.
- Augment, and in some cases, execute, detection capabilities.
- Provide guidance and suggestion for specific Hunt Mission operations, and assist in their execution when needed.
- Support response efforts from a technical perspective.
- Extract and correlate indicators or artifacts.
- Derive or collect raw intelligence from investigations and open sources, and inject them into the intelligence lifecycle for processing and analysis.

- Assist Cyber Intelligence Manager and Strategic Intelligence Analysts in the production of Intel products
- Assist in determining total infrastructure threat exposure
- Works to minimize TIP false positives
- Validates internal and external data feeds for the TIP
- Examines feeds for credibility, validity, and relevance Internal and External
- Assists in IoC collection and normalisation within the TIP
- Participates in IoC tagging and tag management
- Participates in the triage of intelligence (warning/threat, current)
- Participates in playbook / workspaces / spaces development and use
- Develops and validates templates
- Feeds data into adversary and campaign models
- Validates TIP processes and procedures – assists in authoring
- Ingests data from malware engineers, forensics staff
- Assists with data, information, intelligence source validation

Your experience – qualifications

- Expertise in understanding and applying the intelligence lifecycle.
  - Expertise in collection methods, intelligence production and analysis
- In-depth awareness and use of open source intelligence-type tools and methods.
- Expertise in collection methods, structured analytic techniques, and analysis
- Strong knowledge of threat intelligence platforms.
- Fundamental analytic tradecraft skillset, with experience in the extraction and analysis of tactical intelligence from investigations and OSINT
- Experience working on teams with diverse skillsets and backgrounds
- Experience in a fast-paced, operational environment
- Understanding of the operation and functionality of COMPANY and related technologies
- Strong technical understanding of the information security threat landscape (attack vectors and tools, best practices for securing systems and networks)
- Knowledge and use of Mitre ATT&CK