Senior Intelligence Analyst

LOCATION **ABU DHABI, UAE**

Summary of Position Forward Defense is looking for a Senior Intelligence Analyst to be a part of the analysis team. The intelligence analysis team primarily is responsible for creating analytical intelligence products, supporting ongoing projects, initiatives, programs and on-demand intelligence requests.

Duties and Responsibilities

- Provide timely intelligence analysis reports and support client deliverables;
- Collaborate internally and externally to develop and enhance analytical products;
- Own and execute ongoing projects, initiatives and respond to on-demand intelligence requests;
- Create, maintain and triage alerts to support the intelligence requirements program;
- Receive, prioritize and respond to Requests for Information (RFI) from clients;
- Analyze raw data sets and extract relevant insight;
- Identify intelligence collection gaps and communicate findings and collection requirements to "on-the-ground" researchers;
- Analyze several disparate data sources to produce analytical products;
- Mentor and train associate and midlevel analysts;
- Initiate, propose, develop and provide intelligence briefings in support of the engagement strategy;
- Initiate, propose, and create processes and standard operating procedures to support team resiliency;
- Identify and communicate opportunities for new tools, products, projects and systems;
- Assess new threat vectors and develop intelligence on threat actor tactics, techniques and ensure end-to-end execution on strategic and tactical projects that can be developed into threat intel products.

Qualifications, skills, knowledge, or experience

- More than five years' experience in an intelligence role, threat intelligence or equivalent;
- Degree in intelligence, cybersecurity, criminology, computer science, information technology, information security, engineering or equivalent work experience; master's degree is a plus;
- Must be an adaptable, inquisitive and self-motivated team player with strong analytical skills, eager to learn and possess the ability to work independently and as part of a team;
- Possess experience working independently and under pressure with minimal supervision;

ISO 9001:2008

51st floor, Addax Tower, Al Reem Island, Abu Dhabi, UAE
info@forwarddefense.com
www.forwarddefense.com

- Display the ability to learn or develop new processes quickly in response to changes in business requirements;
- Experience working/interacting with enterprise environments and teams, such as NOC, SOC, JOC, fraud, CTI, CISO groups, IT security; threat vectors and basic mitigating controls such as IPS, IDS, WAF, etc.; and leverage knowledge to effectively communicate business risk as it relates to the client's cyber threat posture;
- Strong analytical writing and presentation skills;
- Hands-on experience with command line utilities and basic scripting abilities using Bash, Python or Perl is a plus;
- Hands-on experience with databases and structured query language (SQL) and/or no SQL is a plus;
- Strong understanding of cybercrime offerings, malware and intelligence products available in the market;
- Proficient in open source intelligence (OSINT) research and common tool sets;
- Excellent written and verbal skills; fluency in English is required;
- Deep understanding and knowledge of the cybercriminal underground ecosystem; terminology and common hacking tools and methods, such as carding, fraud, exploits, malware, vulnerabilities etc.;
- Experience identifying and evaluating new sources of intelligence and integrating numerous types of cybersecurity data sources into cyber threat analysis products;
- Experience proactively research emerging cyber threats, apply analytical understanding of attacker methodologies and tactics, system vulnerabilities, and key indicators of attacks and exploits
- Good understanding of TCP, IP and other lower level network protocols, as well as common higher-level protocols such as HTTP(s), SMTP, FTP, and SSH;
- Experienced with industry recognized analysis framework and compliance standards, such as Kill
- Chain, Diamond Model, OWASP, NIST, HIPPA, PCI, etc.; and
- Experienced with multiple computing platforms, including Windows, OSX, Linux, Unix.

How to apply: Respond via email to info@forwarddefense.com

ISO 9001:2008

51st floor, Addax Tower, Al Reem Island, Abu Dhabi, UAE
info@forwarddefense.com
www.forwarddefense.com