Our innovative and growing company is searching for experienced candidates for the position of threat intelligence. If you are looking for an exciting place to work, please take a look at the list of qualifications below.

Responsibilities for threat intelligence

- Developing, implementing, and supervising the execution of processes to ensure a repeatable, but agile, methodology exists to quickly evaluate and implement effective threat intelligence products and services for a variety of internal, executive, and external stakeholders
- Building and overseeing the implementation of tools and technologies to realize the overarching threat intelligence, partnering heavily with our SunTrust Security Operations Center, Security Engineering, and IT Engineering groups as necessary
- Supervising and mentoring intelligence analysts in ensuring that threat intelligence products and services are consistently delivered with high degrees of quality
- Partnering effectively at all levels of the technology organization and with business partners, where needed, to ensure that new or existing cyber security controls are implemented with limited or ideally no impacts to the user experience
- Knowledge of classes of software vulnerabilities and threats and of database query languages
- Familiarity with industry-standard classification schemes (CVE, CVSS, CWE, CPE, CAPEC)
- Strong understanding of host and network security concepts, such as system hardening, log management, intrusion detection & prevention systems, firewalls
- Proficiency with at least one programming or scripting language, such as

- Verifies that application software/network/system security postures are implemented as stated, documents deviations, and recommends required actions to correct those deviations
- Manages and administers the updating of rules and signatures (e.g., intrusion detection/protection systems, anti-virus, and content blacklists) for specialized cyber defense applications

Qualifications for threat intelligence

- Bachelor's degree and/or equivalent work experience- 5+ years of security, network or operating system related technologies experience – SOC or Threat Intelligence experience also preferred
- Experience in scripting to improve process automation
- Subject matter expert (SME) in one or multiple areas such as SIEM, Proxy or Firewall administration, IDS/IPS, Threat Detection, or Information Risk
- Experience in reviewing and analyzing log files and data correlation
- 7 or more years of experience in information systems security
- Knowledge of computing laws and regulations