Example of Threat Intelligence Job Description

Our growing company is looking for a threat intelligence. Please review the list of responsibilities and qualifications. While this is our ideal list, we will consider candidates that do not necessarily have all of the qualifications, but have sufficient experience and talent.

Responsibilities for threat intelligence

- Compose white papers about your research for publication
- Contribute to our well-read blog about any technical topic of interest, including day-to-day work or outside interests, when possible
- Direction, productization, and full lifecycle management of threat intelligence-related products and features
- Executes an intelligence life cycle, including requirements gathering, intelligence collection, analysis, targeted distribution, and feedback to produce relevant, timely, accurate, and actionable intelligence providing the "who, what, when, where, why, how, and importance" of cyber threats including those associated with espionage, hacktivism, cybercrime, malicious software, social engineering, and emerging threats
- Collaborates with internal partners to provide intelligence and reporting which meets business needs
- On behalf of Global Cybersecurity, prepare and deliver regular written and verbal briefings across all levels of the enterprise delivering authorised briefings to external clients when required
- The analyst leads TI activities as a customer surrogate in support of enterprise-level cyber security incidents, provides situational awareness to appropriate personnel through clear and concise communications, and promotes a proactive response to possible threats by staying current with, analyzing, and identifying mitigations for emerging threats to the customer's IT infrastructure

engineers, Cyber Security Operations Center (CSOC) analysts, and customer leadership affected by cyber security events
- Focusing on enterprise-level TI, responsibilities entail developing and operationalizing TI in support of CSOC investigations of suspected intrusions, pro-active management of enterprise information security resources, and the technical evaluation of enterprise networks, systems, and applications against the cyber threat and associated risk of cyber attack
- Provide accurate, complete and timely written documentation for all project phases including ongoing status reports and deliverables detailing technical issues identified and their associated business risks

Qualifications for threat intelligence

- Possess security certifications (CISSP, CCNA, CEH)
- Proven experience performing or leading cyber threat management and intelligence, to including collection and aggregation of threat data, automated or manual analysis, and reporting
- Strong knowledge of a broad array of other systems security technical controls and processes (e.g., identity & access management, system hardening, audit and log file monitoring, DLP, security policies, incident response, intrusion prevention, vulnerability management)
- Working knowledge of relevant financial industry cyber security regulations, standards, and controls frameworks, FFIEC, PCI-DSS, GLBA, ISO 2700x)
- Bachelor Degree in computer sciences, engineering, information security or an equivalent combination of education, training, and experience
- Microsoft Certified Systems Engineer (MCSE) and Information Systems Security Professional (ISSP) certifications expected