Our innovative and growing company is hiring for a cyber incident response. If you are looking for an exciting place to work, please take a look at the list of qualifications below.

Responsibilities for cyber incident response

- Maintain current with new developments in the security industry including alerts, bugs, vulnerabilities and viruses
- Instill and foster a culture of excellence, integrity, and professionalism
- Conduct reviews of threat analysis activities performed by staff members to identify important trends and opportunities for improvement
- Recommend courses of action based on analysis of both existing and emerging threats
- Provide leadership and guidance to both technical teams and business leaders during large incident responses and major cases
- Provide guidance and mentor technical staff on incident handling and serve as an escalation point for analysts and malware specialists
- Respond to and assist with assessments and compliance requests
- Work with colleagues in other technology departments the business and product offices to establish effective, productive business relationships
- Manage your own workload
- Deliver on time and to a high standard

Qualifications for cyber incident response

- Must be able to work on round-the-clock shifts, rotating or fixed
- Proven experience in conducting investigative interviews, including writing memorandums of interviews
- Advanced experience with Python scripting language

professional experience directly related to information security, cyber, or computer network defense
- Possess a good understanding of several common security tools, such as a SIEM, logging and forensics tools
- Demonstrated ability to establish well-defined procedures and appropriate mitigations strategies derived from post incident analysis and lessons learned