Our innovative and growing company is looking for a cyber incident response. To join our growing team, please review the list of responsibilities and qualifications.

Responsibilities for cyber incident response

- Assisting phishing team with email analysis and provide responses to customers
- Conduct cyber threat intel research in support of open IR cases
- Work with IR team members to develop and produce the monthly metrics and scorecards
- Perform data analysis in support of weekly cyber threat briefs to InfoSec leadership
- Perform OSINT in support of IR and Phishing team
- Develop scripts to automate the analysis of CTI data
- Perform data analysis and research in support of "Quarterly Review" product
- Perform research on cyber threat and cyber enabled piracy groups
- Build out threat actor/malware/TTP profiles for SharePoint
- Backup the CIRT Director and be the Technical CIRT Commander when needed, and or by rotation

Qualifications for cyber incident response

- The Computing Environment certification can include CompTIA Server+, Microsoft, RedHat, or Solaris professional certifications or training as defined in DoDi 8570.01M
- This position requires you have an Interim DOD Secret or higher
- Work is located in Radford VA
- A minimum 4 years Information Assurance experience in DOD environments
- DoD 8570.01M IAM level II certification (i.e., CISSP)