Job description

Our value is in our employees – smart, passionate, perceptive and fun people.

Learn and Grow with us! Our innovations and employees impact the growth, success, and direction of our client's mission and our company. We all share a true passion for technology and enjoy working together to protect information systems, develop solutions, share ideas, and exchange knowledge. We celebrate diversity and the unique perspective each team member brings to his/her job, team, and community. We are currently seeking talented and motivated **Incident Responder/Handler/Threat Intelligence** for full or part-time positions.

Essential Functions:

Apply your Incident Response and Handler skills in a growth-based position supported by the best security researchers in the world! You will be part of a consulting team working directly with our clients.

The key responsibilities of the role are as follows:

- Conduct and track in-depth threat research on incidents
- Conduct malware analysis and triage and resolve advanced vector attacks such as botnets and advanced persistent threats (APTs)
- Uses threat intelligence information to understand the techniques, tactics, and procedures used by attackers in the kill chain
- Work with asset owners, infrastructure and support teams, stakeholders, Security Operations, and management teams during high severity incidents to develop and execute high level remediation plans, author incident findings and lessons learned
- Investigate suspicious anomalous activity based on data alerts or data outputs from various toolsets
- Utilize tools and advanced techniques to identify and investigate threats or suspicious activities in the environment
- Contribute to information sharing within Customer's organization
- Provide tuning recommendations to administrators based on findings during investigations or threat information reviews
- Assist continuous improvement of processes and work with Applications teams to improve alerts and rules in the incident monitoring systems
- Understand and apply commonly known security practices and possess a working knowledge of applicable industry controls such as NIST 800-53. Employees will be expected to acknowledge their security responsibilities in writing prior to gaining

access to company systems. Employees will be required to maintain a working knowledge of local security policies and execute general controls as assigned.

Knowledge, Skills, Qualifications and Experience:

Required:

- Bachelor's degree, master's degree preferable.
- 5+ years of experience in Cyber (Information) Security
- 1+ year of experience in 3rd Party compliance and/or governance.
- 5+ years of technical experience across various technologies and architectures including web, networks, infrastructure, manufacturing equipment, mobility, computer applications, and information security.

Desired Qualifications:

- At least one of the following certifications is highly desirable: GIAC Certified Incident Handler (GCIH), Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), Certified in the Governance of Enterprise IT (CGEIT).
- 3+ years of experience in an IT Audit, Enterprise Risk Management (ERM), or Information Security Risk Assessment role.
- 5+ years of experience with enterprise level security networking
- 5 years of incident response, threat management or digital forensics experience
- 5+ years of experience with one or more of the following tools: Helix, Encase, FTK, Wireshark, Reg Ripper, Scalpel, Photo Rec, NMAP, Truecrypt, Notepad++, FTK Imager, SIFT, Volatility
- Familiarity with the following technologies: Active Directory, Virtualization platforms, Microsoft Windows, Unix, Linux, Mac OS X, LDAP, Active Directory, 802.11 wireless, firewalls, routers, network protocols and architecture, databases, VPN/RAS, IDS/IPS
- Understanding of both Risk Based and one or more of the following frameworks: PCI-DSS, Sarbanes Oxley, NERC-CIP, HIPAA, FISMA, ISO, COBIT, NIST, IS0 27000/27001

Education and Certification Requirements:

Bachelor's degree or equivalent experience in a computer science, information systems, engineering, or other related field. Relevant and current industry certifications in information security, cybersecurity and risk management.

CyberSecurity for Hire, LLC is an Equal Opportunity/Affirmative Action employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, national origin, disability or protected veteran status, or any other legally protected basis, in accordance with applicable law.