SECURITY ANALYST

SUMMARY:

The Security Analyst will work closely with the Director IT/Manager Infrastructure to ensure the security of the Firm. Candidate must have excellent communication, problem solving, organization and follow-up skills with the ability to handle multiple assignments simultaneously. Candidate should demonstrate good judgement as well as attention to detail while working well with a team.

ESSENTIAL FUNCTIONS:

- Working knowledge of CompTIA Network+ to ensure skills in configuring networks as well as designing and troubleshooting
- Demonstrated ability to work solo
- Demonstrated knowledge of bug bounties, cross-site scripting, broken authentication, cross-site request forgery, and glassbox scanning.
- Create and analyze security policies and procedures to determine weakness in infrastructure security and complete a thorough audit of existing measures
- Work with the Director of IT, and the Infrastructure Manager to evolve the on-premises, and cloud security strategy
- Anticipate data breaches by ethically hacking into the company's secure systems while determining future flaws and their prevention
- Become a Certified Ethical Hacker to legally utilize tools of malicious hackers to improve company's security posture
- Understand reverse engineering to have a thorough knowledge of malware analyzation and bug patching on various software platforms
- Minimize negative impact of security breach by shifting security measures for future prevention and creating information assurance
- Work with other IT groups to make sure all systems and software are upgraded
- Install and upgrade antivirus software
- Test and evaluate new technology
- Perform penetration testing
- Analyze IT requirements and provide objective advice on the use of IT security requirements
- Design, analyze and implement efficient IT security systems
- Identify potential areas of security risk, develop, and implements corrective action plans for resolution of problematic issues, and provide general guidance on how to avoid or deal with similar situations in the future.
- Provides reports on a regular basis to IT Director to keep current with all security efforts.
- Ensure proper reporting of violations or potential violations to IT Director as appropriate or required.

REQUIRED SKILLS AND EXPERIENCE:

- Degree in Information Systems, preferred
- 3+ years of experience in information security
- Proficient with Microsoft full stack, to include Azure cloud technologies with emphasis on EM+S, Azure ATP, Defender ATP, Azure NSG, and Identity Management
- Proficient in DMARC, DKIM, and SPF
- Ability to create and deploy email attack simulations
- Knowledge of Mimecast Email Security Platform
- Experienced with penetration testing and techniques
- Ability to identify and mitigate network vulnerabilities
- Understanding of web development, HTTP, HTML, and application security
- Understand patch management
- Understanding of Zero Trust / VPN's
- Knowledge of firewalls, antivirus and IDPS concepts to include both on-premises and cloud environments
- Experienced in installing security software and documenting security issues
- Excellent written and oral communication skills

ADDITIONAL QUALIFICATIONS:

- Problem solving and analytical skills
- Project management skills
- Communication skills – written and verbal

WORKING HOURS:

- Work may require more than 40 hours per week to perform the duties of the position which may include nights and/or weekends.
- Be available to resolve critical security related issue 24/7 when needed
- Work may require travel.

WORKING CONDITIONS:

Work is performed in a normal heated or air-conditioned office environment.

The above is intended to describe the general content of and requirements for the performance of this job. It is not to be construed as an exhaustive statement of essential functions, responsibilities or requirements. This job description must not be misconstrued as a promise of employment, nor deemed as an employment contract. EOE. We participate in e-verify.

Revised 06/28/2021