CYBERSECURITY ANALYST

NATURE OF WORK

The Cybersecurity Analyst (CSA) is responsible for assisting with the day-to-day operations of securing the City's various information systems. Reporting to the Chief Technology Officer (CTO), the CSA is tasked with providing technical expertise in all areas of network, system, and application security. The CSA works closely with the various teams in the Information Technology Department to ensure that systems and networks are continuously designed, developed, deployed, and managed, emphasizing strong, effective security and risk management controls. The CSA assists the City's vulnerability management program, assists the annual cybersecurity assessments and penetration tests, and researches and reports on emerging threats to help the firm take pre-emptive risk mitigation steps. The CSA effectively correlates and analyzes security events within the context of the City of Mentor's unique environment to proactively detect threats and mitigate attacks before they occur.

EXAMPLES OF ESSENTIAL JOB FUNCTIONS

- Proactively monitor the environment to detect and implement steps to mitigate cyber-attacks before they occur.
- Provides technical expertise guided by the CTO regarding security-related concepts to operational teams within the Information Technology Department and the City Departments.
- Review, investigate, and respond to real-time alerts within the environment.
- Review real-time and historical reports for security and compliance violations.
- Monitor online security-related resources for new and emerging cyber threats.
- Assesses new security technologies to determine potential value for the enterprise.
- Conducts vulnerability assessments of firm systems and networks.
- Manage systems owned by the Information Security Team.

REQUIREMENTS OF WORK

- A four-year college degree or equivalent industry training and certifications.
- Minimum three years of experience in a security analyst or related position.
- Technical knowledge of enterprise-class technologies such as firewalls, routers, switches, wireless access points, VPNs, and desktop and server operating systems.
- Thorough understanding of Microsoft's enterprise technology platform, including Network security controls, Cloud, Azure, Active Directory, SQL, Office365, Windows server, and desktop operating systems.
- Proficiency in Windows PowerShell, Scripting, data management, cybersecurity framework and controls, IDS, IPS, Operating Systems, Incident response, DevOps, Threat Knowledge, and Regulatory Guidelines.
- Working experience with the following technology vendors and products: Palo Alto Networks, Splunk, Rapid7 Nexpose Vulnerability Scanner, Trellix, Crowdstrike, and Zscaler.
- Strong writing skills and ability to articulate security-related concepts to various technical and non-technical staff.
- Working experience creating, implementing, and managing a threat-hunting program within a corporate environment.
- Demonstrated experience implementing and enforcing security and compliance frameworks such as NIST, Cobit, and ISO.
- Be a proficient problem-solver that can work autonomously.

DESIRED QUALIFICATIONS

- One or more of the following certifications: CEH, CISM, CompTIA Security+, CISSP, GSEC
- Experience with managing and securing both on-premises and hosted systems and applications.
- Experience with application and database security

PHYSICAL DEMANDS

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Work is performed mainly in an office setting; hand-eye coordination is necessary to operate computers and various office equipment, requiring the ability and physical mobility to install or remove equipment.

While performing the duties of this job, the employee is frequently required to sit and talk or hear; use hands to finger, handle, or feel objects, tools, or controls; and reach with hands and arms. The employee is occasionally required to walk, lift, and/or move up to 25 pounds. Specific vision abilities required by the job include close vision and the ability to adjust focus.