CYBER SECURITY SPECIALIST

Location*:* Delaware Memorial Bridge, New Castle, DE

$94,039 to $113,300 annualized (Grade H)
(*Position and Salary commensurate with experience and skills*)

Opening Date: March 28, 2024 **Closing Date: Until Filled**

I. POSITION SUMMARY

The Cyber Security Specialist is responsible for preemptively identifying security issues that pose a potential threat or an immediate risk to the Delaware River and Bay Authority's (Authority) business operations, employees, customers, and vendors. The position reports to the Director of ITS and has the responsibility for the creation of a comprehensive data security program for the Authority's system. Responsibilities will include developing security protocols, solutions, analyzing current systems for vulnerabilities, and handling all cyberattacks in an efficient and effective manner. The Cyber Security Specialist is also involved in the management to effectively detect malicious software and hardware that might be present on the network; designing and coordinating penetration testing; carrying out security reviews or/and audits of existing and newly acquired systems; making recommendations on internal controls and security; and executing information security risk assessment annually. The Cyber Security Specialist is responsible for following established safety practices while performing assigned duties to protect self, co-workers, and the public from personal injury and to prevent damage to Authority property. This position is subject to 24 hours on call in the event of a cyber security incident.

II. ESSENTIAL DUTIES AND RESPONSIBILITIES

- Safeguards information system assets by identifying and solving potential and actual security problems.
- Protects systems by defining access privileges, control structures, resources, and proper configuration of security solutions applied in the protection of Authority's assets.
- Implements configuration and maintenance of the Cybersecurity Incident Response Plan to effectively identify and alert upon potential security events.
- Participates in the investigations being performed as part of the Cybersecurity Incident Response Team; documenting, and maintaining accurate, and detailed records of the incident and all activities that were undertaken in response to an incident.
- Implements security improvements by assessing current situation, evaluating trends, and anticipating requirements.
- Determines security violations and inefficiencies by conducting periodic audits.
- Upgrades systems by implementing and maintaining security controls.
- Interfaces with vendor support service groups for contract renewals and to ensure proper escalation as required.
- Ensures that all solutions set up for security and monitoring can effectively monitor and report upon security events happening within the environment by assigning security solution agents to devices and systems.
- Initiates and produces custom scripts needed to make logging and alerting requirements easy and effective.
- Participates in the process of selecting and reviewing information security solutions.

- Assists in the configuration of intrusion detection and prevention solutions based in the host and network servers to effectively identify potential security incidents.
- Updates job knowledge by participating in educational opportunities; reading professional publications; maintaining personal networks; participating in professional organizations.
- Provides the highest level of customer service and professionalism to all internal and external customers.

III. REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES

- Must possess a high ethical and moral character as privileged access to confidential data will be an essential component of the job function.
- Experience in information security, specifically with penetration testing, intrusion detection, incident response or digital forensics.
- Deep knowledge and understanding of the various ways attacks are carried out against a system or network and how to effectively detect them.
- Advanced understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, OSI model, defense-in-depth, and common security elements.
- Experience with vulnerability scanning solutions.
- Possess advanced analytical skills and strong ability to maintain calmness and being diplomatic under highly stressful situations.
- Expert problem-solving skills understanding the importance of timely resolution and follow-through.
- Strong multitasking skills to be able to effectively manage multiple activities, including cross-team dependent activities simultaneously.
- Must be able to organize and prioritize work, be proactive, work independently, be self-directed and self-motivated.
- Strong ability to work effectively in collaboration with other members of a team or/and other professionals with minimal supervision.
- Strong ability to quickly learn new processes and technologies, and to adapt to changes in sequences and timelines.
- Strong communication skills, including written and verbal, to explain highly technical concepts to a non-technical audience, capable of writing basic documentation.
- Ability to provide superior customer service to everyone by responding in a courteous and efficient manner.

IV. REQUIRED EDUCATION AND EXPERIENCE

- Bachelor's degree in Computer Science, Information Security or related field, significant work experience may be substituted for a degree
- Two (2) to five (5) years of related experience in Cyber Security, *preferred*

V. LICENSES, REGISTRATIONS, AND/OR CERTIFICATES

- Valid driver's license
- Certified Information Systems Security Professional (CISSP) or CompTIA Security+ Certification or equivalent

VI. SPECIAL REQUIREMENTS

- Subject to a background investigation and pre-employment physical and drug testing
- The Delaware River and Bay Authority requires all employees to have direct deposit with a financial institution to receive their bi-weekly pay.
- Required to be available for duty at all hours (24x7) as may be required in the event of a cyber security incident.
- Required to travel to all Authority locations as needed.

****

If you are interested in applying for this position, please complete the on-line application at www.drba.net. In addition to the online application, please attach a current resume.

The Delaware River and Bay Authority is an Equal Opportunity Employer