



WEBER BASIN WATER CONSERVANCY DISTRICT

CYBER SECURITY ANALYST

Department: Strategic Initiatives/Information Systems
Regular Full-Time (FT40)
Non-exempt / Hourly
Grade 10-11
M-F 8:00 a.m. - 4:30 p.m.

JOB SUMMARY

Under the general guidance and direction of the Information Services Department Manager and Assistant General Manager, conducts assessments with tools and software to identify and remediate any cybersecurity vulnerabilities within the District's IT and OT networks. The duties are of a wide range - from fairly routine to highly technical.

This position is classified as safety sensitive and is subject to random drug testing.

ESSENTIAL JOB FUNCTIONS (Not necessarily a comprehensive list)

- Apply operating system and 3rd party software patching and updates.
- Firmware updates and patching on IT and OT network infrastructure.
- Configuration reviews on network infrastructure
- Use of software and network tools for vulnerability identification and assessments.
- Utilization and configuration of endpoint management and log collection and storage software solutions to secure devices and infrastructure.
- Implementation of the NIST cybersecurity framework.
- Identify unwanted or unknown network traffic via available tools.
- Create monthly reports for review of current vulnerabilities and mitigation efforts.
- Monitor and respond to security alerts from SIEM, IDS/IPS, and other detection platforms; investigate incidents and document findings and remediation steps.
- Administer and maintain identity and access management (IAM) controls, including role-based access, multi-factor authentication (MFA), and privileged account management.
- Evaluate, implement, and manage security for OT/ICS environments, including SCADA systems, PLCs, HMIs, and industrial communication protocols.
- Develop, test, and maintain an incident response plan; participate in tabletop exercises and post-incident reviews to continuously improve response procedures.
- Conduct security awareness training for District staff; promote a culture of cybersecurity best practices across IT and OT teams.
- Assist in maintaining compliance with applicable regulatory requirements and standards.
- Promotes and adheres to the District's core values (collaboration, ownership, mutual respect, professionalism, appreciation, safety and sustainability).

OTHER JOB FUNCTIONS (Not necessarily a comprehensive list.)

- Performs other duties as assigned.

NOTE: These duties are subject to change depending on District needs and the individual in this position may be required to perform other jobs. Any of the herein stated requirements and conditions are subject to approval and/or waiver by the General Manager. The regular work schedule is subject to change depending on the District needs for this position.

MINIMUM QUALIFICATIONS (The education and experience requirements for this job may be satisfied by any acceptable equivalent combination of education and experience.)

Education: Bachelor's or Master's degree (preferred) from accredited college or university in Information Technology/Systems, Computer Science, or Cyber Security.

Experience: Minimum of 2 years of experience in Information Systems, Computer Science or related field. Advanced degrees and certifications may be substituted for experience.

Knowledge: Knowledge of computer network systems and hardware. Knowledge of the NIST Cybersecurity framework is preferred but not required. An understanding of OT (Operational Technology) networks is required. Knowledge of network packet traffic analysis. Knowledge of various cybersecurity tools and software is preferred. Knowledge of network firewall and switch management and configuration is required. Knowledge of the Microsoft Windows operating system is required. Familiarity with the OSI model and an understanding of TCP/UDP protocols is necessary. Knowledge of SIEM platforms, IDS/IPS systems, and log aggregation tools is preferred. Familiarity with identity and access management (IAM) concepts including MFA, role-based access control, and privileged access management is preferred. Familiarity with CISA cybersecurity guidance for water systems is a plus. Understanding of backup, recovery, and business continuity principles as they relate to cybersecurity is desired.

Skills: Ability to effectively communicate with managers, developers, and other staff. Must have excellent problem-solving skills, be able to use critical thinking and the ability to evaluate and resolve complex issues.

Abilities: Ability to operate and use servers, personal computers, firewalls, networks switches, along with software such as databases, spreadsheets, word processing, and email. Ability to analyze and troubleshoot highly technical issues and provide advice and recommendations to staff. Applicants must possess the ability to learn new tools and software applications quickly and incorporate them into their work processes. Ability to communicate effectively orally and in writing, ability to work effectively with other District personnel, public and private agencies and officials, and the general public.

Special Requirements: None

Other Qualifications: Must have and maintain a valid Utah driver's license and an acceptable driving record per District policy.

WORKING CONDITIONS

Work Environment: The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

This position will primarily operate in an office environment. The employee may occasionally work in outside weather conditions for short periods of time and may be exposed to hot or cold temperatures.

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.

While performing the duties of this job, the employee is regularly required to sit for long periods of time, talk, hear, and use hands and fingers to operate a computer keyboard, phone and other office equipment.

Specific vision abilities required include close vision, color vision, depth perception, and the ability to adjust focus. Light to moderate lifting may be required.

HIRING POLICIES

The District provides equal opportunity to all employees and applicants for employment without regard to race, color, national origin, religion, sex, age, disability, sexual orientation or any other category protected by applicable law. Weber Basin Water Conservancy District will not refuse to hire a disabled individual who is capable of performing the essential requirements of the position with reasonable accommodations when they do not create an undue hardship.