Class Code: 2089   **Effective Date : 08/17/2022**

THIS CLASSIFICATION INCLUDES PAY INCREASE OPPORTUNITIES - OUTLINED BELOW

PURPOSE OF THE CLASSIFICATION: Under supervision, the purpose of this position is administration of advanced security technologies, automation, and procedures to protect, detect and respond to cybersecurity issues in real-time, performing security initiatives across the company, analyzing threats and escalations from multiple sources, both internal and external, triaging a wide variety of security events, conducting detailed and comprehensive investigation and drive issues to closure, contributing to developing innovative solutions for detection and event handling, and collaborating with security partners and threat intelligence teams to derive indications and warnings of impending threat; and performs other related assigned duties.

ESSENTIAL TASKS:
- Supports Security System Infrastructure and Applications
- Implements and tests endpoint security tools
- Administration of security tools and products
- Conducting scans of networks to find vulnerabilities
- Implementation and testing of new security products and procedures
- Investigating Cyber Incident Response and Recovery activities
- Researching data for Legal and HR investigations
- Works closely with other information technology staff, vendors, and internal customers to optimize and support the security tools and systems
- Cross-trains junior engineers and customers on the use of security products and procedures
- Must report to work on a regular and timely basis

Reasonable accommodations may be made to enable individuals with disabilities to perform the essential tasks.

QUALIFICATIONS:
Training and Experience: Must meet one of the following options or an equivalent combination of training and experience per Personnel Policies and Procedures, Section 128:

1.   (a) Completion of sixty (60) hours from an accredited college or university including coursework in management information systems, computer science, information technology, information systems, or other related fields relevant to the essential tasks listed in this job description; **and,**
        (b) Six (6) years' experience relevant to the essential tasks listed in this job description, preferably experience in enterprise-class systems analysis and/or systems administration**; or,**

2.   (a) Graduation from high school or possession of a General Education Development (GED) certificate; **and**
        (b) Five (5) years experience relevant to the essential tasks listed in this job description; **and,**
        (c) Possession of a current industry accepted certification in two (2) of the following:
                1) Security+; or
                2) Server+; or
                3) Network+; or
                4) Certified Information Systems Security Professional (CISSP); or
                5) Cisco Certified Network Associate (CCNA); or
                6) Cisco Certified Network Professional (CCNP); or
                7) Cisco Certified Internetwork Expert (CCIE); or
                8) Microsoft Azure Certification

PAY INCREASE OPPORTUNITY

Employee will be eligible for the equivalent of a one (1) step increase upon completion of one (1) additional certification, listed in Training and Experience, not previously submitted, as approved by management and one (1) year employment in the position.

Knowledge, Abilities and Skills:

Knowledge of:
- Considerable knowledge of an Enterprise Infrastructure Applications and Systems
- Considerable knowledge of cyber threats and response tactics
- Considerable knowledge of endpoint protection
- Considerable knowledge of identity management, Intermediate knowledge of intrusion detection systems
- Considerable knowledge of intrusion prevention systems
- Considerable troubleshooting methods used with information systems and infrastructure-type applications
- Considerable knowledge of operational characteristics and capabilities of applicable systems management applications
- Considerable knowledge of various enterprise-level solutions
- Considerable knowledge of personal computers and edge devices
- Considerable knowledge of basic-level scripting

Ability to:
- Ability to troubleshoot and analyze fundamental systems/infrastructure applications/issues
- Ability to communicate verbally and in writing with all levels of customers
- Ability to document advanced technical information in a concise and understandable format
- Ability to cross-train customers
- Ability to perform basic scripting

Skill in:
- Skill in communicating effectively, in writing and verbally, to a diverse customer base

Physical Requirements: Physical requirements include arm and hand dexterity enough to use a keyboard and telephone; occasional lifting and carrying up to 50 pounds; may be subject to sitting for extended periods, walking, standing, reaching, bending, kneeling, handling, and twisting; and vision, speech, and hearing sufficient to perform the essential tasks.

Licenses and Certificates:

1. Possession of a valid Oklahoma Class "D" Driver License.
2. Possession of two (2) appropriate professional certifications, as listed under Training and Experience, as approved by management, not previously submitted, within one (1) year of date of hire.

WORKING ENVIRONMENT: The working environment is primarily indoors in an office setting; it may require some travel to various City locations to provide computer-related assistance; and on-call, after-hour support for assigned production systems.

Class Code: 2089

EEO Code: E-02
Group: Clerical and Administrative
Series: Data Processing and Information Services