CYBERSECURITY ANALYST

NATURE OF WORK

This is responsible technical work involving the monitoring, analysis, and defense of the City and County's information systems and networks against cybersecurity threats and vulnerabilities.

Work involves responsibility for monitoring security systems and alerts; analyzing network traffic, system logs, and threat intelligence; investigating security incidents; coordinating containment, mitigation, and remediation efforts; conducting vulnerability assessments; supporting risk management initiatives; developing and maintaining cybersecurity documentation and procedures; ensuring compliance with applicable security standards; and assisting in the implementation of security tools and technologies. Work may involve collaboration with internal IT staff, external vendors, and public safety partners to protect critical infrastructure and sensitive data. General supervision is received from the Information Security Officer.

EXAMPLES OF WORK PERFORMED

Uses cyber defense tools to monitor and analyze system activity, in order to identify any potentially malicious activities.

Analyzes any identifies malicious activity to determine weaknesses exploited, exploitation methods, and effects on system and information.

Identifies deficiencies in the effectiveness of security controls through audits, testing, and exercises.

Provides recommendations to resolve deficiencies in security controls, products, and processes.

Performs tuning and optimization of security platforms, tools, and software.

Ensures application of security patches for commercial products; integrates automated capabilities for updating or patching software; develops processes and procedures for manual updating and patching of software based on current and projected patch timeline requirements.

Works with stakeholders to resolve computer security incidents and vulnerability compliance.

Assists in the development and delivery of cybersecurity awareness training to employees.

Maintains detailed documentation of incidents, investigations, corrective actions, and system changes.

Stays current on emerging cybersecurity threats, vulnerabilities, and industry trends.

Performs related work as required.

DESIRABLE KNOWLEDGE, ABILITIES AND SKILLS

Considerable knowledge of cybersecurity principles, threat detection methodologies, and incident response procedures.

Considerable knowledge of network protocols, operating systems, firewalls, endpoint security systems, and security monitoring tools.

Knowledge of vulnerability assessment tools, penetration testing concepts, and risk management frameworks.

Knowledge of applicable cybersecurity regulations, standards, and best practices.

Ability to analyze complex technical information and identify security risks and vulnerabilities.

Ability to investigate and respond to cybersecurity incidents in a timely and effective manner.

Ability to communicate technical information clearly and effectively both orally and in writing.

Ability to develop and maintain effective working relationships with supervisors, coworkers, vendors, contractors, and the general public.

Ability to exercise independent judgment and initiative in analyzing cybersecurity threats and recommending appropriate corrective actions.

Ability to manage multiple priorities in a fast-paced and high-pressure environment.

MINIMUM QUALIFICATIONS

Graduation from an accredited four-year college or university with major coursework in cybersecurity, computer science, information technology, or a related field and five years of experience in cybersecurity operations, network security, or information security; or any equivalent combination of training and experience that provides the desirable knowledge, abilities and skills.