TEXAS COMMISSION ON LAW ENFORCEMENT

POSITION TITLE: Cybersecurity Analyst II

SALARY: $80,000 - $94,000

DURATION: Full-Time

CLOSING DATE: Until Filled

NUMBER OF OPENINGS: 1

WHAT WE DO

The mission of Texas Commission on Law Enforcement (TCOLE) is to ensure that Texas is served by law enforcement professionals. We are the regulatory body that oversees the licensing and certification of peace officers, jailers, and telecommunicators across the state. The Cybersecurity and Network Operations team will work closely with the IT Operations team and Application Development Team to produce and support modern user-centered services that accelerate and reinforce TCOLE's mission.

GENERAL DESCRIPTION

Performs information security and cybersecurity analysis work involving planning, implementing, and monitoring security measures for the protection of information systems and infrastructure. Work also includes protecting cybersecurity assets and delivering cybersecurity incident detection, incident response, threat assessment, cyber intelligence, software security, and vulnerability assessment services.

EXAMPLES OF WORK PERFORMED

- Performs technical risk assessments and reviews of account permissions, computer data access needs, security violations, programming changes, and new and existing applications and systems, including data center physical security and environment.
- Performs cybersecurity incident detection, analysis, and prevention.
- Performs vulnerability scans of networks and applications to assess effectiveness and identify weaknesses.
- Performs forensic analysis of information systems and portable devices and forensic recovery of data using assessment tools.
- Monitors systems and procedures to protect data systems and databases from unauthorized access.
- Monitors and analyzes cybersecurity alerts from cybersecurity tools, network devices, and information systems.
- Supports the implementation of computer system security plans with agency personnel and outside vendors.
- Develops plans to safeguard computer configuration and data files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Modifies and monitors computer configuration and data files to incorporate new software and virus protection systems, correct errors, or change individual access status.
- Implements continuous automated security compliance capabilities.
- Researches and analyzes cybersecurity threat indicators and their behaviors for the prevention, detection, containment, and correction of data security breaches, and recommends threat mitigation strategies.
- Trains users and promotes security awareness to ensure system security and improve application, server, and network efficiency.
- Performs related work as assigned.

DESCRIPTION

Performs complex (journey-level) information security and cybersecurity analysis work. Works under general supervision, with moderate latitude for the use of initiative and independent judgment. May routinely assist other staff in performing work of greater complexity. Employee may:

- Develop plans to safeguard computer configuration and data files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Coordinate agency policies for encryption of data transmissions and the definition of firewall configuration to protect confidential information in transit.
- Design, develop, modify, test, and integrate database or computer hardware systems to protect against cyber threats.
- Design, automate, manage, and deploy security applications and infrastructure program activities.
- Participate in the development of information technology disaster recovery and business continuity planning.

GENERAL QUALIFICATION GUIDELINES

EXPERIENCE AND EDUCATION

Five years of security specific work experience. Experience and education may be substituted for one another.

- Experience with hybrid Active Directory and Azure environments
- MFA, System certificates, and security tokens
- Microsoft Purview

PREFERRED CERTIFICATIONS:

- MS Azure Security Engineer Associate
- CISSP
- CCSP

KNOWLEDGE, SKILLS, AND ABILITIES

- Knowledge of the limitations and capabilities of computer systems and technology; technology across all mainstream networks, operating systems, and application platforms; operational support of networks, operating systems, Internet technologies, databases, and security applications and infrastructure; cybersecurity and information security controls, practices, procedures, and regulations; incident response program practices and procedures; and information security practices, procedures, and regulations.
- Knowledge of change management best practices
- Knowledge of network and IP fundamentals
- Skill in the use of applicable software and the configuring, deploying, monitoring, and automating of security applications and infrastructure.
- Ability to resolve complex security issues in diverse and decentralized environments; to plan, develop, monitor, and maintain cybersecurity and information technology security processes and controls; and to communicate effectively.
- Ability to communicate effectively using interpersonal skills and appropriate supporting technology.
- Ability to establish and maintain effective and cordial working relationships at all organizational levels, including agency management, direct supervisors, co-workers, internal and external customers.

MILITARY OCCUPATIONAL SPECIALTY CODES can be found at: http://www.hr.sao.texas.gov/CompensationSystem/JobDescriptions

VETERAN'S PREFERENCE: If you choose to claim veteran's employment preference including surviving spouse or orphan of a veteran as outlined by the State of Texas, you must attach a DD214 at the time your application is submitted.

FOR NEW HIRES/REHIRES: Health insurance is available the 1st of the following month after a 60-day waiting period.

TO APPLY: Application may be completed at: Job Search (taleo.net)

APPLICATIONS SUBMITTED THROUGH WORK IN TEXAS: Work In Texas (WIT) applicants must complete the supplemental questions to be considered for the posting. In order to complete the supplemental questions, please go to CAPPS Recruit to register or login and access your profile. Go to CAPPS Recruit to sign in (Link: https://capps.taleo.net/careersection/407/jobsearch.ftl?lang=en).

PLEASE NOTE: All applications must contain complete job histories, which include job title, dates of employment, name of employer, supervisor's name and phone number, and a description of duties performed. If this information is not submitted, your application may be rejected because it is incomplete. Resumes do not take the place of this required information. Candidates may be asked to participate in a skills demonstration and/or presentation. Salary is contingent upon qualifications and is subject to salary administration and budgetary restrictions.

- Complete copies of undergraduate and law school transcripts must be furnished to the divisional hiring representative at the time of the interview.
- If you are scheduled for an interview and require any reasonable accommodation in our interview process, please inform the hiring representative who calls you to schedule your interview. Whenever possible, please give the hiring representative sufficient time to consider and respond to your request. Only applicants scheduled for interviews will be contacted.
- *As an equal opportunity employer, we hire without consideration to race, religion, color, national origin, sex, disability, age, or veteran status, unless an applicant is entitled to the veteran's preference.*
- *This position requires the applicant to meet Agency standards and criteria which may include passing a pre-employment background check, prior to being offered employment by the Agency.*