(ISO) Cybersecurity Analyst IV

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

The person in this role will lead the new TCOLE Cybersecurity and Network Team to oversee the cybersecurity program and network operations. If you are looking to join a growing IT team in a small State agency that has a big reach and great impact on Texas law enforcement, this is the job for you!

Work involves complex (senior-level) planning of prevention, detection, and remediation of cybersecurity threats and intrusions; cybersecurity policies and monitoring protocols; and leading the development of a security plan; as well as overseeing operation of the TCOLE network infrastructure. Works under minimal supervision, with considerable latitude for the use of initiative and independent judgment. Works both independently and with other staff in performing work of greater complexity.

This position reports in person to the TCOLE Headquarters building at 6300 E Hwy 290, suite 200, Austin, TX 78723.

WORK PERFORMED

Recommends the deployment of cybersecurity and network infrastructure to protect critical infrastructure services.

Conducts research related to cybersecurity trends and technology; and evaluates cybersecurity tools and techniques for potential application.

Conducts research & recommends the delivery of cloud solutions that are appropriate for business and best-fit for need and risk appetite.

Oversees the monitoring of network status to ensure that all systems and devices are working properly.

Oversees risk assessments, cybersecurity and network management initiatives, and monitoring and detection activities.

Performs planning activities to enhance the performance of network resources based on evaluations of system and network requirements and network utility and availability.

Monitors and analyzes cybersecurity and network alerts from tools, network devices, and information systems.

Oversees 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.

Coordinate agency policies for encryption of data transmissions and the definition of firewall configuration to protect confidential information in transit.

Develops information technology disaster recovery and business continuity plans.

Ensures cybersecurity awareness training programs for employees, contractors, and users; and facilitates cyber preparedness exercises.

Performs related work as assigned.

EXPERIENCE AND EDUCATION

Five (5) years of experience in the IT industry performing work in one or more of the following areas:

- Information Security
- Vulnerability Scanning
- Vulnerability Management
- Formal Risk Assessments
- Penetration Testing
- Digital Forensics
- Security Operation Center (SOC) Operations

Graduation from an accredited four-year college or university with major course work in a field

relevant to the assignment is generally preferred. Experience and education may be substituted for one another.

EXPERIENCE AND TRAINING PERFERRED

Have or work towards obtaining Certified Ethical Hacker (CEH) GAIC Certified Incident Handler (GCIH), GCFE Certified Forensic Examiner (GAIC), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), GIAC Security Essentials Certification (GSEC), Certified Incident Handler (GCIH) and/or CyberSec First Responder (CFR) or similar certification, or serve as a SME on a certification creation committee or equivalent.

KNOWLEDGE, SKILLS, AND ABILITIES

- Experience building cybersecurity teams or five (5) years of security team management
- Knowledge of relevant DIR IT Security Services and regulations including Texas Government Code Chapter 2059, Texas Administrative Code § 202, and other related security codes, documentation, standards, and best practices
- 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.
- 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.
- Ability to manage projects to resolve complex issues in diverse and decentralized environments.

OTHER REQUIREMENTS

- Pass a TCOLE background check.

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: Jobs may be found 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. 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: Job Search (taleo.net))

PLEASE NOTE: All applications must contain complete job histories, which includes 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 college transcripts must be furnished to the divisional hiring representative at the time of the interview for positions.

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 criminal background check, prior to being offered employment by the Agency.