TEXAS DEPARTMENT OF LICENSING & REGULATION

Working title: Threat Hunting Associate
Class title: Cybersecurity Analyst I
Posting No.: 1208-26
Opening Date: 12/30/2025
Closing Date: Open Until Filled
Location: EOT Bldg., 920 Colorado St., Austin, TX 78701
Class Code: 0319
FLSA: Computer-exempt
Salary Group/Salary: B23, $90,000.00- $99,657.96/yr.
Division: Information Technology
Number of positions: 1

General Description
Perform moderately complex (journey-level) cybersecurity analysis work, essential for TDLR to fulfill its mission of service to the citizens of Texas. Work involves protecting cybersecurity assets and delivering cybersecurity incident detection, incident response, threat assessment, cyber intelligence, software security, and vulnerability assessment services. Works under general supervision, with moderate latitude for the use of initiative and independent judgment, relying on direction from senior staff to resolve non-standard issues. This position reports to the Chief Information Security Officer. This is a hybrid position and not a 100% teleworking position.

Essential Job Functions
- Analyze cybersecurity threat indicators and their behaviors, and research and implement new security risk and threat mitigation strategies, tools, techniques, and solutions for the prevention, detection, containment, and correction of data security breaches.
- Assist in conducting vulnerability scans of networks and applications to assess effectiveness and identify weaknesses. Assist in identifying and evaluating new cybersecurity technologies to identify and remediate vulnerabilities. Provide input on improving network, server, workstation, and application security.
- Monitor agency systems, reporting anomalous activity or malicious traffic, and perform cybersecurity incident detection, analysis, and prevention. Assist in administration of security tools.
- May assist in the design, automation, management, and deployment of security applications and infrastructure program activities. Implement continuous automated security compliance capabilities.
- May assist in the evaluation of code and applications and in the mitigation of security flaws.
- May assist in the development, implementation, and coordination of business continuity plans (BCP) and disaster recovery (DR) processes.
- Review, develop, and deliver cybersecurity awareness training and advise staff regarding security policies and procedures.
- Research cybersecurity and privacy legislation, regulations, advisories, alerts, and vulnerabilities and applies recommendations as required.
- Monitor IT security related websites, newsgroups, organizations and publications; recommend best practices and improvements to agency IT security standards and procedures; and prepare and deliver reports and presentations on security related matters.
- Demonstrate a spirit of teamwork, offering positive and constructive ideas, encouragement, and support to other members of the staff and team while upholding the agency's core values.
- Keep management appropriately informed of ongoing activity and critical matters affecting the operation and well-being of the agency.
- Comply with Division and/or Agency training requirements, adhere to all TDLR Personnel Policies, and perform related duties as assigned.

Required and Preferred Qualifications
- Graduation from an accredited four-year college or university with major coursework in information technology security, information assurance, computer information systems, computer science, management information systems, or a related field is required. (Experience in information security analysis work or IT security related work, in excess of the required two years, may substitute for college on a year-for-year basis.)
- Two (2) years of experience in information security analysis work or related IT security work is required.

- Willingness to travel up to 5% for work-related purposes is required.
- Certification as a Certified Ethical Hacker (CEH), SANS GIAC Certification, Security+, Certified Cloud Security Professional (CCSP), EC-Council Certified Incident Handler (ECIH), Certified Information Security Manager (CISM), Certified Information System Security Professional (CISSP), or comparative cybersecurity professional certification is preferred.
- Experience with network security systems management is preferred.
- Experience with cybersecurity architecture and data flow documentation is preferred.
- Experience with a Vulnerability Management program is preferred.
- Experience doing web application security scans/assessments is preferred.
- Experience with custom dashboards and/or configurations of SIEM tools is preferred.
- Experience patching Windows based computers, using WSUS, SCCM or other tools, patch management programs is preferred.

Knowledge, Skills, and Abilities

- Knowledge of the limitations and capabilities of computer systems and technology; of operational support of networks, operating systems, Internet technologies, databases, and security infrastructure; and of information security controls, practices, procedures, and regulations.
- Knowledge of concepts and techniques for enterprise risk management, audits, and risk assessments; of security requirements and evaluation mechanism for security of cloud-based services; and, of incident response program practices and procedures.
- Skill in collecting and analyzing complex data; in evaluating information and systems; in drawing logical conclusions; in assessing the effectiveness of internal controls over key information technology risks; in detecting changes in key risks and/or control effectiveness; in using analytical software tools, data analysis methods, and other computer applications; and in technical writing.
- Ability to resolve complex security issues in diverse and decentralized environments.
- Ability to provide excellent customer service.
- Ability to communicate effectively.
- Ability to train others.
- Ability to implement and act as an advocate for security best practices and security awareness; and, to plan, develop, monitor, and maintain information technology security processes and controls.

Physical and Mental Requirements

- Must be able to sit or stand for extended periods of time, work well in stressful situations under strict deadlines, and operate standard office equipment and computer software.

Military Occupational Specialty Codes:

Veterans, Reservists, or Guardsmen with a MOS or additional duties or other related fields pertaining to the minimum experience requirements may meet the minimum qualifications for this position and are encouraged to apply.

Additional Military Crosswalk information can be accessed at:
https://hr.sao.texas.gov/Compensation/MilitaryCrosswalk/MOSC_InformationTechnology.pdf

HOW TO APPLY

State of Texas applications may be submitted electronically through the Texas Workforce Commission's workintexas.com online system by the closing date stated on the job posting. Applications may also be downloaded through TDLR's website https://www.tdlr.texas.gov/careers/ and emailed to jobs@tdlr.texas.gov. For applications submitted via email, please list the job posting title and job posting number in the subject line. Applications submitted via email must be received by 11:59 p.m. on the posting's closing date. When a job posting is listed as "Open Until Filled", it is best to apply as quickly as possible, as the posting may close or be placed on hold at any time with or without prior notification. Applications will NOT be accepted via mail, fax, or hand delivery. Incomplete applications will not be considered. A resume in lieu of application will be rejected. Additionally, an application with "see resume" within the summary of experience is considered incomplete and will be rejected. Applicants are solely responsible for timely delivery of applications by the deadline. All applicants must submit a thoroughly completed application, answering all applicable questions. 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.

SELECTIVE SERVICE REGISTRATION

In accordance with legislation effective September 1, 1999, male candidates aged 18 to 25 are required to show proof of selective service registration (or exemption) prior to an offer of employment. Such proof is not required to be filed with an application but must be provided upon request by the Human Resources office.

E-VERIFY

This employer participates in E-Verify and will provide the Social Security Administration (SSA) and if necessary, the Department of Homeland Security (DHS), with information from each new employee's Form I-9 to confirm work authorization.

TDLR IS AN EQUAL EMPLOYMENT OPPORTUNITY EMPLOYER

In compliance with the Americans with Disabilities Act (ADA), TDLR will provide reasonable accommodation. If you are scheduled for an interview and require reasonable accommodation in the 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.