LOUISIANA MILITARY DEPARTMENT

LANG-GOHSEP, Baton Rouge, LA
CTAC Specialist 1, 2, or 3
#50658492

ANNOUNCEMENT NO. 196-2026
OPENING DATE: November 04, 2026
CLOSING DATE: November 11, 2026

***SALARY:**
MT-318 $75,046 - $135,096
MT-319 $80,309 - $144,560
MT-320 $85,925 - $154,690

*Salary indicates typical starting range. Level will be determined by qualifications.

BENEFITS
Retirement: LASERS
Insurance: Medical, Dental, & Vision
Paid Holidays: 10 plus proclaimed
Annual Leave: 96 hours per year with tenure increases
Sick Leave: 96 hours per year with tenure increases

JOB TYPE: Unclassified
Current Classified employees must give up their designation to accept this position.

POSITION DESCRIPTION:

Serves as a Cyber Threat Analytics Center (CTAC) Specialist, responsible for monitoring, detecting, analyzing, and responding to cybersecurity threats across organizational networks and systems. This role supports continuous security operations by identifying suspicious activity, investigating incidents, and coordinating response efforts to protect critical infrastructure and information systems.

Continuously monitor security tools such as SIEM, EDR, IDS/IPS, and firewalls to identify suspicious or anomalous activity. This includes reviewing and triaging alerts, correlating events across multiple data sources, and determining whether activity represents a legitimate threat or a false positive. The analyst maintains real-time situational awareness of the environment and ensures that validated threats are escalated appropriately based on severity and potential impact.

Conduct detailed investigations into suspicious activity and confirmed security incidents. This involves analyzing logs, endpoint data, and network traffic to determine the scope, root cause, and impact of an incident. Coordinate with internal and external customer teams to support containment, eradication, and recovery efforts, while following established incident response procedures and playbooks to ensure a consistent and effective response.

Document all alerts, investigations, and response actions within ticketing systems, ensuring clear and complete case management. Generate incident reports and after-action summaries, contribute to operational metrics, and maintain documentation that supports audits, compliance requirements, and organizational awareness.

Conduct threat hunting activities designed to identify previously undetected threats. This includes leveraging threat intelligence, forming hypotheses, and analyzing available data for indicators of compromise. Assist in tuning detection rules, improving SIEM use cases, and identifying gaps in visibility to strengthen overall detection capabilities.

Participate in training sessions, exercises, and knowledge-sharing activities to stay current on emerging threats and techniques. Collaborate with internal teams and external partners. Provide feedback to enhance SOC processes, tools, and overall effectiveness. Performs all other tasks, special projects, analysis, studies, and plans as directed.

POSITION QUALIFICATIONS:

Minimum Qualifications: Bachelor's degree in Cybersecurity, Information Technology, or related field (or equivalent experience). 1–3 years of experience in cybersecurity, IT operations, or network defense. Familiarity with security monitoring tools (e.g., SIEM platforms, endpoint protection). Basic understanding of networking concepts (TCP/IP, DNS, HTTP/S). Knowledge of common attack techniques and frameworks (e.g., MITRE ATT&CK). Strong analytical and problem-solving skills. Strong verbal and written communication skills. Ability to work with minimal guidance, instruction, or supervision.

Preferred Qualifications: Experience working in a Security Operations Center (SOC) environment. Hands-on experience with modern security platforms, including Google SecOps and CrowdStrike Falcon SIEM. Demonstrated ability to develop, maintain, and optimize incident response playbooks. Experience implementing and managing automation through SOAR (Security Orchestration, Automation, and Response) platforms. Familiarity with log analysis, detection engineering, and security tool integration to enhance visibility and response capabilities. Understanding of cloud security concepts (GCP, AWS, Azure, or similar). Experience supporting critical infrastructure or public sector environments.

Preferred Certifications: CompTIA Cybersecurity Analyst (CySA+), CompTIA Security+, Global Information Assurance Certification (GIAC) credentials such as GSEC, GCIA, or comparable certifications, and Certified SOC Analyst (CSA). Equivalent industry-recognized certifications demonstrating expertise in cybersecurity operations, threat detection, incident response, or security analysis may also be considered..

Key Competencies: Detail-oriented demonstrates sound critical thinking, analytical reasoning, and clear written and verbal communication. The ideal candidate can assess complex information, identify practical solutions, and deliver accurate work under time-sensitive conditions. Success in this role also requires the ability to collaborate effectively with diverse teams, coordinate efforts across stakeholders, and maintain a high standard of performance in a fast-paced environment

GENERAL REQUIREMENTS:

- Must have a valid Driver's License, Social Security Card and Birth Certificate.
- Must be available to report to duty during emergency or disaster situations. Other periodic travel may be required.
- Must meet physical requirements to perform functions of the position.
- Must attend/complete all Louisiana Military Department (LMD) annual training and other training required for the position.
- Must adhere to the Code of Ethics and foster a Sexual Harassment-Free Environment.

CONDITIONS OF EMPLOYMENT: By submitting an application for employment with the Military Department, the applicant agrees to the following conditions of employment:

- All LMD positions require in-office attendance. This is not a remote position.
- Salary is paid by Electronic Funds Transfer (EFT) / Direct Deposit Only. A checking or savings account is is required for employment.
- LMD is a substance abuse and drug free workplace. The selected applicant must pass a pre-employment background investigation and pre-employment drug test. Thereafter, all employees are subject to random drug testing.
- The selected applicant must pass a pre-employment criminal background investigation prior to employment.

APPLICATION PROCEDURES: All Applicants must complete a LANG-LMD-H Form 10 (State Application) and attach a legible copy of their Official Birth Certificate, Driver's License and Social Security Card. Resumes are optional and will not be accepted unless they are submitted with the LANG-LMD-H Form 10 (State Application).

- **State Application:** The LANG-LMD-H Form 10 (State Application) is located at:! http://geauxguard.la.gov/join-us/state-technician-vacancies

Application(s) must be submitted to the appropriate LMD Human Resources point of contact below by the Close Date, no later than 12:00 a.m. CST:

Shanice Allen
7667 Independence Blvd.
Baton Rouge, LA 70806
Email: gohsepemployeerelations@la.gov