Stephenson Stellar Corporation

Title: Senior AI/ML Systems Architect **Position ID**: 2026-0020	**Type Position:** Full Time **Annual Salary:** TBD **Level:** PL4
Primary Location: Remote	**Travel Required:** 10% CONUS and HI
Alternate Location: Home office anywhere in USA	**Contact:** Technical: aechevarria@stephensonstellar.org (Axel Echevarria) Human Resource: bmoyer@stephensonstellar.org (Barb Moyer)

Company Background: Stephenson Stellar Corporation (Stellar) is a nonprofit research and development organization focused on assuring our nation remains a global leader in the Space Domain. Our mission is to foster technological innovation and provide secure space-based solutions.

Stellar is an equal opportunity employer, and all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin, age, disability status, protected veteran status, or any other characteristic protected by law.

Additional information at: www.stephensonstellar.org

Job Description: In this position, you will serve as the Senior AI/ML Systems Architect for the Space Systems Protection Directorate (SSPD). This is a hands-on senior technical role responsible for designing, building, and maturing AI-enabled capabilities across SSPD, including internal tools, lab support environments, secure knowledge management, cyber automation, assessment support workflows, research and development prototypes, and mission focused AI solutions. This role is not limited to a single Cyber Test and Evaluation (CT&E) tool. The candidate will help establish the directorate wide AI technical roadmap and translate that roadmap into working, secure, maintainable tools that improve how SSPD performs cybersecurity research, assessment, adversary emulation, vulnerability research, reporting, and internal operations. The candidate will work directly with SSPD leadership, cybersecurity researchers, engineers, assessors, and junior developers to build local, and server hosted AI capabilities suitable for controlled environments. The position requires a builder mindset, strong architecture discipline, practical AI engineering skills, and the ability to guide junior developers through meaningful implementation work. The ideal candidate can move between strategy, software architecture, secure implementation, technical mentorship, and customer-facing explanation without losing focus on mission impact, CUI protection, and operational usefulness. The position responsibilities include: (1) Own and maintain the SSPD AI technical roadmap across internal tools, lab environments, knowledge management, cyber automation, and mission support capabilities; (2) Architect, develop and integrate local and server hosted AI/ML systems, including large language models (LLMs), retrieval augmented generation (RAG), agentic workflows, model evaluation pipelines, and secure tool integrations; (3) Build hands on software prototypes and production-oriented tools while leading junior developers through tasking, code review, technical mentoring, documentation, and disciplined engineering practices; (4) Develop AI-enabled workflows to support CT&E operators, adversary emulation, vulnerability research, cyber assessment preparation, evidence generation, reporting, knowledge base search, task tracking, SOP development, and internal operational automation; (5) Design standalone and disconnected workflows for laptops and lab environments, including synchronization concepts with internal LLM servers for approved model, prompt, playbook, and knowledge base updates; (6) Integrate AI capabilities with approved cybersecurity tools, lab testbeds, emulation and virtualization environments, internal dashboards, document repositories, and reporting workflows; (7) Establish secure AI engineering practices for Controlled Unclassified Information (CUI aware) development, including access control, audit logging, data handling rules, model and prompt version control, approval gates, evaluation criteria, and repeatable deployment patterns; (8) Create technical documentation, CONOPS, SOPs, training material, architecture diagrams, demonstrations, and briefings that make AI capabilities understandable and usable by technical and non-technical stakeholders and (9) Support business development, Independent Research and Development (IRAD) execution, research papers, white papers, customer demonstrations, and proposal efforts related to AI-enabled cybersecurity for space systems

Requirements

Clearance: Ability to obtain and maintain a Top-Secret clearance. Active Secret, Top Secret, or TS/SCI clearance is highly preferred.

Citizenship: Candidate must be a United States citizen.

Education: BS in Computer Science, Computer Engineering, Software Engineering, Artificial Intelligence, Machine Learning, Data Science, Cybersecurity, Electrical Engineering, or a closely related technical field. An advanced degree is preferred but not required when equivalent hands-on experience is demonstrated.

Experience:

- 10 plus years of progressive hands-on experience in software engineering, AI/ML engineering, platform engineering, cybersecurity automation, applied research and development, or related technical domains. At least 5 years should include practical AI/ML, data engineering, automation, or model-enabled software development. Demonstrated experience owning technical roadmaps, leading small technical teams, mentoring junior developers, and delivering working software is required.

Required Skills:

- Strong knowledge of AI/ML systems engineering, including LLM-based applications, RAG architecture, embeddings, vector databases, model evaluation, prompt and context engineering, agentic workflows, and practical model deployment patterns.
- Hands-on software engineering experience in Python and at least one additional language such as TypeScript, JavaScript, Go, C/C++, or Rust.
- Experience building secure, maintainable software services, APIs, command line tools, automation scripts, dashboards, and data pipelines.

- Experience with local or on-prem AI deployments, including open-source LLMs, model serving, GPU-enabled inference, containerization, and offline or restricted-network deployment considerations.
- Understanding of cybersecurity workflows such as vulnerability assessment, penetration testing, adversary emulation, defensive cyber operations, evidence collection, reporting, or security control assessment.
- Ability to integrate AI capabilities with cybersecurity tools, internal data sources, document repositories, lab environments, and operator workflows.
- Familiarity with secure software development practices, DevSecOps, Git based workflows, automated testing, code review, configuration management, and documentation discipline.
- Ability to design AI systems that account for CUI protection, access control, auditability, data provenance, model/prompt versioning, and human approval gates for sensitive workflows.
- Demonstrated ability to translate ambiguous operational needs into executable technical roadmaps, system designs, prototypes, and working tools.
- Demonstrated ability and willingness to train, mentor, and develop junior developers and technical staff in AI engineering, software development, secure implementation, and disciplined delivery practices.
- Strong written and verbal communication skills, including the ability to brief technical concepts to leadership and produce clear technical documentation, SOPs, user guides, and architecture artifacts.

Desired Skills:

- Active Secret, Top Secret, or TS/SCI clearance.
- Experience designing AI-enabled tools for national security, defense, aerospace, cyber operations, mission assurance, or classified/CUI controlled environments.
- Experience with RMF, NIST SP 800-53, NIST SP 800-171, CMMC, CUI handling, or secure development in regulated environments.
- Experience with space systems, ground systems, satellite operations, flight software, embedded Linux, RTOS environments, or cyber testing of mission systems.
- Familiarity with CT&E, adversary emulation, red teaming, penetration testing, vulnerability research, SPARTA, MITRE ATT&CK, threat-informed testing, or mission impact driven cybersecurity assessment.
- Experience integrating AI workflows with QEMU, emulation, simulation, lab automation, HIL/SIL environments, or cyber range infrastructure.
- Experience with knowledge management, document intelligence, secure search, internal assistant development, workflow automation, and AI-enabled reporting.
- Experience developing AI governance practices, model evaluation harnesses, red team testing for AI systems, secure update pipelines, and safety controls for agentic systems.
- Experience supporting proposals, IRADs, research papers, technical demonstrations, customer briefings, or early-stage product/capability development.
- Familiarity with GPU servers, Linux administration, container orchestration, vector search infrastructure, and secure deployment of open-source AI tooling.